Reducing The Challenges To Making Cybersecurity Investments in the Private Sector

Department of Homeland Security Contract #N66001-112-C-0132

FINAL REPORT
June 30, 2015

Robert H. Smith School of Business
and
School of Public Policy

Principal Investigator (PI): Lawrence A. Gordon, Ph.D., EY Alumni Professor of Managerial Accounting and Information Assurance, R. H. Smith School of Business, Affiliate Professor in University of Maryland Institute for Advanced Computer Studies, University of Maryland.

Co-PI: Martin P. Loeb, Ph.D., Deloitte & Touche Faculty Fellow, Professor of Accounting and Information Assurance, Robert H. Smith School of Business, Affiliate Professor in University of Maryland Institute for Advanced Computer Studies, University of Maryland

Co-PI: William Lucyshyn, Director of Research and Senior Research Scholar, Center for Public Policy and Private Enterprise, School of Public Policy, University of Maryland

Research Associate: Lei Zhou, Ph.D., Visiting Assistant Professor, Department of Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland

Table of Contents

Acknowledgments

We gratefully acknowledge the financial support for the research contained in this Report provided by 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. We would like to give special thanks to Dr. Douglas Maughan, Director, Cyber Security Division, DHS Science &Technology (S&T) Directorate, and Dr. Joseph Kielman, Science Advisor and Project Manager with the Cyber Security Division, DHS S&T Directorate, for their continued intellectual support and guidance throughout this research project. We also extend our appreciation to all of the executives who participated in the interviews as part of this research, as well as all of the firms that were kind enough to participate in the questionnaire-based survey portion of this research project. Finally, we would like to thank our co-workers Caroline Dawn Pulliam and Diane Hall for their assistance with the planning, coordination, and administration of this study.

EXECUTIVE SUMMARY

REDUCING THE CHALLENGES TO MAKING CYBERSECURITY INVESTMENTS IN THE PRIVATE SECTOR

The underlying objective of the research project described in this Final Report (hereafter referred to as the Report) was to understand more fully the challenges associated with making cybersecurity investments in the private sector, and to recommend policies for facilitating the appropriate level of such investments. Particular emphasis was given to those firms that own and/or operate assets critical to the national infrastructure. As discussed in Section I of the Report, we began by developing a conceptual/analytical framework for making cybersecurity investments. In other words, since cybersecurity investments compete with other investment opportunities available to firms, they need to be justified in terms of showing that the benefits exceed the costs (i.e., ultimately, cybersecurity investments become a business decision in the private sector). This means that companies in the private sector must be able to "make the business case" for investing in cybersecurity activities in a manner that is consistent with the way companies consider other investment decisions. We gave specific attention to analyzing the following three challenges associated with making cybersecurity investments in the private sector:

- measuring the benefits from cybersecurity investments,
- assessing the risks associated with cybersecurity breaches, and
- quantifying the externalities (i.e., the spillover effects) associated cybersecurity investments.

As part of our analysis, we developed several testable hypotheses related to the above three challenges.

We addressed the issues related to the above three challenges using various complementary research methodologies, beginning with an examination of the relevant existing literature. In a conceptual paper (published in the *Georgetown Journal of International Affairs*), we pointed out that there are systemic problems that make determining the proper levels of cybersecurity investments difficult for profit-oriented corporations and that these problems tend to result in corporations underinvesting in cybersecurity. This journal article also discussed policies that governments could and should adopt in order to foster increased investments in cybersecurity related activities by profit-oriented corporations.

We then developed analytic models for investing in cybersecurity. One of our analytic models, based on input-output analysis, resulted in a paper (forthcoming in the *Journal of Cybersecurity*) that shows that the potential for government incentives/regulations to increase cybersecurity investments by private sector firms is dependent on the following two fundamental issues:

- whether or not firms are using the optimal mix of inputs to cybersecurity, and
- whether or not firms are able, and willing, to increase their budget devoted to cybersecurity.

Several general implications are apparent from our input-output framework. For example, if it were assumed that the total expenditures by firms on cybersecurity activities (i.e. the budget for spending on cybersecurity inputs) are fixed, and that firms are already utilizing the optimal mix of cybersecurity inputs, government incentives/regulations that encourage changes in the resource allocations among cybersecurity inputs would lower the firms' level of cybersecurity. In addition, if it were assumed that the total expenditures by firms on cybersecurity is fixed, but that firms are not able to determine the optimal mix of cybersecurity inputs, government incentives/regulations (e.g., mandatory cybersecurity standards) that encourage changes in resource allocations among cybersecurity inputs could either increase or decrease the level of cybersecurity in firms. In this latter case, the outcome of such incentives/regulations depends on whether the government could properly identify the source of cybersecurity resource misallocations and, in turn, tailor the regulation on inputs to help rectify the misallocation of resources. Finally, it was shown that if it were assumed that the cybersecurity budget of an organization is not fixed (i.e., relax the firm's initial budget constraint), government incentives/regulations that encourage organizations to increase their cybersecurity investments could increase the cybersecurity level of such organizations.

Another one of our analytic models examined the effect of externalities on cybersecurity investment decisions, based on the model used in Gordon and Loeb (2002) and Gordon et al. (2003b). This model examined how the existence of well-recognized externalities changes the maximum a firm should, from a social welfare perspective, invest in cybersecurity activities. The results of this work resulted in a paper published in the *Journal of Information Security.*

A third paper resulting from our analytic models focused on demonstrating how information sharing would likely encourage firms to take a more proactive, as compared to a reactive, approach toward cybersecurity investments. This paper, which is based on a *real options* perspective, is forthcoming in the *Journal of Accounting and Public Policy*. A copy of this paper (as well as the other published or forthcoming papers noted above) is provided in Section II of this Report.

As discussed in Section III of this Report, while developing the above noted analytic models, we concurrently conducted interviews with senior executives involved in cybersecurity investment decisions (e.g., Chief Financial Officers [CFOs], Chief Information Officers [CIOs], Chief Information Security Officers [CISOs]). The key findings derived from these interviews with executives are as follows:

- The portion of the IT budget spent on cybersecurity activities varies from firm to firm, ranging from 3% to 12% of the IT budget.
- The primary benefits derived from cybersecurity activities come from the cost savings (or cost avoidance) associated with preventing and/or managing cybersecurity breaches, as well as reducing the risks of such breaches.
- The expected loss is the dominant means by which the executives expressed the potential risk associated with cybersecurity breaches.
- There is little, if any, consideration given to externalities when making cybersecurity investments.

- Information sharing is potentially very valuable. However, there is a need for some sort of limited liability protection associated with the cybersecurity related information that is shared.
- A vibrant cybersecurity insurance market would (or at least could) be beneficial to the cybersecurity activities of firms.
- There is strong resistance to a greater regulatory environment to improve cybersecurity by the federal government.
- Critical issues that will impact organizations in the near future are mobile devices, bring your own device, supporting multiple platforms, and security associated with the cloud.

We also developed four in-depth case studies of firms that had experienced major cybersecurity breaches, using (heretofore) untapped publically available data. More to the point, what became apparent was that firms that experienced major, well publicized, cybersecurity breaches were often subject to severe scrutiny in public documents (e.g., Congressional Testimony and Corporate Annual 10K and 8K Reports), as well as in the popular press. In fact, as we delved into examining high visibility security breaches, we realized that most of the information we were trying to obtain through the case studies was available via public information. The information provided in these public records and in the popular press included details for specific companies that were made available by the senior executives responsible for the firms' cybersecurity activities. Furthermore, the information provided during Congressional Hearings by executives under oath and information provided to the Securities and Exchange Commission (SEC) on Annual 10K Reports has face reliability and validity. In addition, these high visibility cases resulted in a wealth of other publicly available information (e.g., from company websites, videos, etc.) that could easily be obtained and verified. The companies selected for these case studies are: Target, Neiman Marcus, RSA, and JPMorgan Chase. As discussed in Section III of this Report, the key findings derived from these case studies are as follows:

- Until a firm has a significant cybersecurity breach, the disclosure of the firm's cybersecurity risks and incidences is extremely limited and, most often, of a boilerplate nature.
- Once a significant breach occurs, firms immediately, and significantly, increase their investments in cybersecurity activities (in line with the wait-and-see approach to cybersecurity investments).
- Although major cybersecurity breaches often have a significant negative effect on the annual earnings of firms during the year of the breach, the long-term financial impact of such breaches (e.g., in terms of stock market performance) is usually not significant.
- Major cybersecurity breaches often result in changes among the firm's senior executives.

Based on the information gathered via the literature review, development of the analytical models, interviews with executives, and case studies, we developed a questionnaire for conducting a large scale survey of senior executives (e.g., CFOs, CIOs, CISOs) involved in cybersecurity related activities. The questionnaire-based survey and its findings are discussed in Section IV of this Report. Over the next several months, we will be developing several papers, based on the survey data collected, to submit for publication in various journals and/or for presentation at various conferences. These papers will focus on the key findings from the survey, which are as follows:

- Larger firms are more actively involved in sharing information concerning cybersecurity activities than are smaller firms.
- There is a significant association between the percentage of a firm's IT budget devoted to cybersecurity activities and (1) the degree to which the firm views cybersecurity as part of its internal control system, (2) the size of the firm, and (3) whether or not the firm has recently experienced a major cybersecurity breach.
- Estimating the future dollar value of losses associated with cybersecurity breaches is problematic for all firms.
- Government incentives that are valued the most, in terms of motivating firms to spend more on cybersecurity related activities, are cost sharing, direct grants, and tax incentives.
- Government incentives related to priority government contracting, expediting the security clearance process, providing technical assistance, and information sharing do little to motivate firms to spend more on cybersecurity activities.
- Chief Financial Officers are less optimistic than Chief Information Officers (or Chief Information Security Officers) when it comes to the ability to anticipate cybersecurity breaches and to estimate the costs of such breaches.

Besides the publication of journal articles, dissemination of our research results has taken place via presentations at numerous conferences, forums, meetings and workshops. In addition, the results of the research have been used to develop a significant portion of a new course developed for the undergraduate Honors College at the University of Maryland (UMD) entitled "Accounting and Economic Aspects of Cybersecurity." This course, which is part of UMD's new prestigious ACES (Advanced Cybersecurity Experience for Students) program was offered for the first time in the spring of 2014 and is being offered again in the fall of 2015. In addition, a graduate level version of this course has been developed and will be offered for UMD's Smith Business School students in either 2015 or 2016. A detailed listing of the above activities is provided in Section V of this Report.

In Section VI of this Report, we discuss the possibility of establishing a Cybersecurity Economics Lab (CySEL) to study, and ultimately increase, cybersecurity investments by private sector firms. The proposed CySEL would:

- Conduct economic experiments in a controlled environment to gain insights on the effectiveness of various proposed incentives and regulations to spur investments in cybersecurity by private sector firms,
- Develop and maintain a database on cybersecurity investments and costs (including the costs of cybersecurity breaches) for longitudinal (as well as cross-sectional) economic studies, and
- Provide education and training for CIOs and CISOs, as well as other managers in the private sector, to enhance their ability to compete effectively for scarce internal cybersecurity funding (thereby, providing a boost to cybersecurity investments in the private sector). In other words, CIOs and CISOs need to be able to understand the terminology and business concepts used by those individuals (e.g., CFOs) controlling organizational funds.

In Section VII of this Report, we make and discuss several general recommendations based on the findings from this entire research project. These recommendations are as noted below:

- Improve SOX and the SEC disclosure guidance, as they relate to cybersecurity.
- Develop incentives for firms to increase their level of cybersecurity investments, taking into consideration that incentives related to cost sharing, direct grants, and taxes seem to be the ones judged to be most effective by executives of private sector firms in terms of motivating their firms to increase investments in cybersecurity.
- Encourage the development of a vibrant cybersecurity insurance market.
- Continue to work to improve information sharing related to cybersecurity, with particular emphasis on limiting the liability associated with such sharing.
- Develop risk-based models to help firms estimate the benefits from cybersecurity investments.
- Develop a capability to conduct laboratory-based economic studies concerned with assessing the impact of economic incentives (and possibly regulations) on various cybersecurity-related issues.
- Develop, maintain and analyze, over an extended period of time, a database on cybersecurity investments, the types of major cybersecurity breaches, and the cost of cybersecurity breaches.
- Provide education and training for private sector firms on "making the business case" for cybersecurity investments.

I. INTRODUCTION

This is the Final Report (hereafter referred to as the Report) for our Department of Homeland Security (DHS) contract, N66001-12-C-0132. The period of performance for this effort was from October 2012 through May 2015.

The underlying objective of this research project was to understand more fully the challenges associated with making cybersecurity investments in the private sector, and to recommend policies for facilitating the appropriate level of such investments. Particular emphasis was given to those firms that own and/or operate assets critical to the national infrastructure.[1] In pursuing this objective, we began by developing a conceptual framework for making cybersecurity investments. In other words, since cybersecurity investments compete with other investment opportunities available to firms, they need to be justified in terms of showing that the benefits exceed the costs (i.e., ultimately, cybersecurity investments become a business decision in the private sector). This means that companies in the private sector must be able to "make the business case" for investing in cybersecurity activities in a manner that is consistent with the way they consider other investment decisions.

In developing this framework, specific attention was given to analyzing the following three challenges associated with making cybersecurity investments in the private sector: (a) measuring the benefits from cybersecurity investments, (b) assessing the risks associated with cybersecurity breaches, and (c) quantifying the externalities (i.e., the spillover effects) associated cybersecurity investments. Several testable hypotheses related to the above three challenges were developed.

The research included interviews with executives, in-depth case studies and a questionnaire-based survey to examine the above noted three challenges and the specific hypotheses related to these challenges. In addition, the research included the development of analytic models to examine issues related to cybersecurity investments and incentives related to such investments.

A. Background and Approach

There continues to be growing concern that profit-oriented firms in the private sector may not be investing a sufficient amount in cybersecurity. In addition, it is unclear as to whether or not the funds invested in cybersecurity activities are being allocated in an efficient manner. Since private sector firms own roughly 85% of the United States' critical infrastructure assets, the fact that firms may be underinvesting in cybersecurity and that cybersecurity related funds may not be invested in an inefficient manner, are important concerns for National Security reasons, as well as for firm-level success. The results of this research should prove useful to DHS to help mitigate incomplete and asymmetric information barriers that hamper efficient cybersecurity decision-making.

[1] The assets that are critical to the U.S. national infrastructure are generally considered to be those assets that are vital to the smooth functioning of the economy and defense of the United States. For example, firms in industries related to communications, defense, energy, food, health care, transportation, etc. are considered to own critical infrastructure assets.

Congress' concern with the issues of underinvestment in cybersecurity in the private sector and the inefficient allocation of funds by private firms among cybersecurity activities is highlighted by the testimony requested before the House Committee on Homeland Security's Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology on October 31, 2007.[2] The 2008 report entitled "Securing Cyberspace for the 44th Presidency," published by the Center for Strategic and International Studies (written by Representative Langevin, Representative McCaul, Scott Charney, and Lt. General Harry Raduege), also addressed these concerns.[3] President Obama's establishment of a senior White House position, entitled Cybersecurity Coordinator, is another indication of the concern with, and commitment to, resolving cybersecurity vulnerabilities and threats.[4]

In January 2011, the Center for Strategic and International Studies, published a follow-up to their 2008 report (also written by Representative Langevin, Representative McCaul, Charney, and Raduege as report for the 44th Presidency), titled "Cybersecurity Two Years Later."[5] The report again raised cybersecurity as an issue of utmost national concern and supported regulation in the form of "risk based performance standards" (p.8). The Report also noted, with some surprise, the degree of opposition to government regulation by Internet companies.[6,7]

B. Making the Business Case

The notion of making the business case for cybersecurity investment decisions involves a process that consists of several steps. These steps, which are illustrated in Figure 1, provide a framework for making investment decisions in a rational manner. As shown in Figure 1, the first step in making the business case for cybersecurity investments is concerned with establishing the objective(s) of cybersecurity. The primary objective is to develop models and policies for facilitating the appropriate (i.e., the social welfare maximizing) level of investments in cybersecurity activities by the private sector firms in the U.S. economy, with particular emphasis on firms owning and/or operating assets critical to the national infrastructure.

[2] See: http://homeland.house.gov/Hearings/index.asp?ID=100
[3] See: http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf
[4] See, for example, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1357549,00.html
[5] See: http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf
[6] See page 4 of the Report.
[7] With the apparent likelihood of some government action increasing, Internet companies, concerned about regulatory intrusions and restrictions, recently proposed that the government institute a collection of incentives, including research and development tax credits, to stimulate enhanced cybersecurity. See: http://www.technewsworld.com/story/cyber-security/72064.html?wlc=1308529013

Figure 1. The Business Case for Cybersecurity Investments

Source: Gordon and Loeb, 2006a, pp. 116 and 131.

The second step in making the business case for cybersecurity investments is to identify the cybersecurity opportunities and/or challenges associated with accomplishing the objective(s). In terms of the research reported here, that means identifying the opportunities and/or challenges associated with cybersecurity investments. The third step in making the business case for cybersecurity investment decisions is to develop the necessary data for comparing the various cybersecurity investment alternatives. The fourth step in making the business case is to perform the necessary analysis to compare the alternatives generated. This comparison is usually done with the aid of cost-benefit analysis and results in the allocation of funds to various cybersecurity investment options.[8]

Once funds are allocated to specific cybersecurity investments, the fifth (and final) step in making the business case is to assess the efficacy of the resource allocation decisions (i.e., the

[8] The cybersecurity literature often refers to this analysis as computing the Return on Security Investments (ROSI). For a discussion of why cost-benefit analysis, rather than ROSI, is the preferred method, see Gordon and Loeb (2002b).

control step) with a view toward improving future investment decisions. In terms of the research presented here, that means examining how firms evaluate the success of the cybersecurity investments. As illustrated in Figure 1, the above needs to be thought of as an iterative process, rather than a simple sequential process.

C. Challenges and Hypotheses Related to Cybersecurity Investments

The above process associated with making the business case for cybersecurity investments becomes particularly thorny at the third step, where the data necessary for comparing the benefits and costs of various cybersecurity investment options need to be generated. More to the point, the benefits (B) associated with cybersecurity investments need to be compared to the costs (C) associated with such investments in terms of discounted cash flows. This analysis is usually referred to as cost-benefit analysis, as shown in the fourth step of Figure 1.

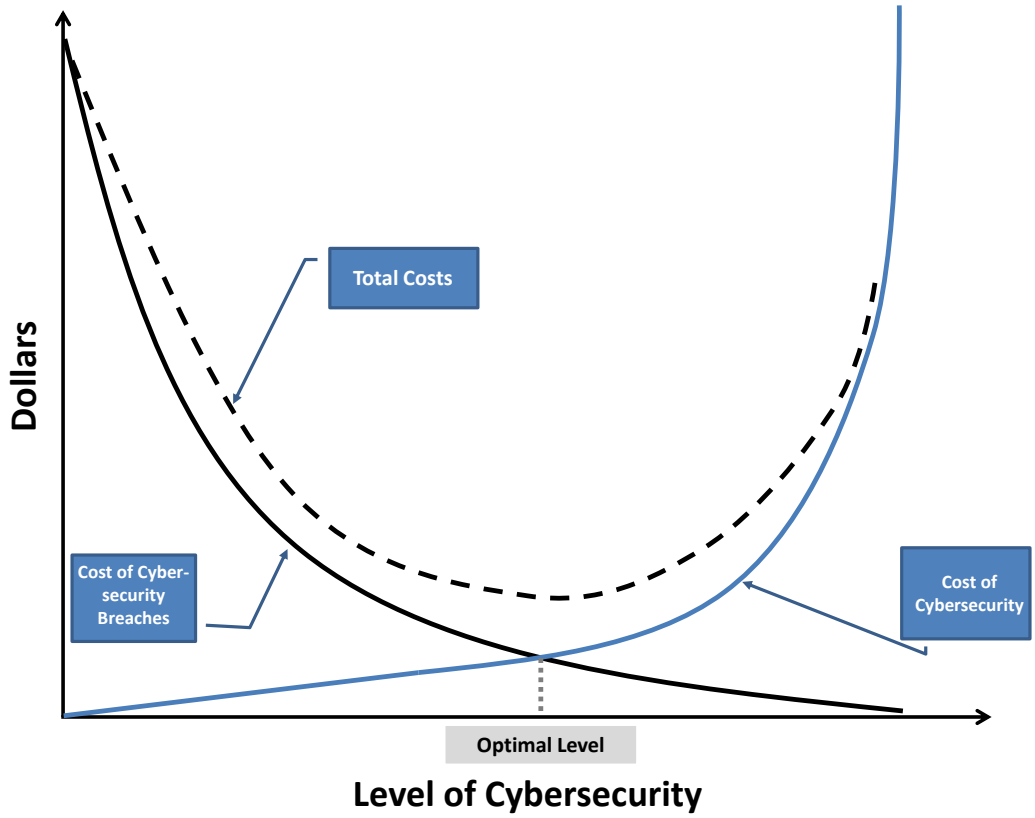
For typical capital investments (e.g., investing in a new product or service to be sold in the open market), the benefits are derived from expected future discounted cash flows associated with the project. The risks associated with these benefits are usually considered by discounting future cash flows by a firm's cost of capital. The difference between the value of the discounted net cash flows and the costs of the project is the net present value (NPV). The basic model for this cost-benefit approach is shown below in Equation 1.[9]

$$NPV = -C_0 + \sum_{t=1}^{n} \frac{B_t - C_t}{(1+k)^t} \qquad \text{Eq. 1}$$

Where NPV=net present value, B=benefits (in terms of cash flows) associated with the investment, and C=costs (in terms of cash flows) associated with the investment, k= the discount rate and usually represents the firm's cost of capital, t=time period t, and n=the number of time periods being considered for the investment.

[9] The use of cost-benefit analysis for efficiently allocating scarce resources (i.e., making the business case) is well established in the capital investment/budgeting literature (e.g., see Gordon and Loeb, 2006).

Figure 2. Selecting the Optimal Level of Cybersecurity



The NPV model gives rise to a simple decision rule for accepting or rejecting additional cybersecurity investments, including the allocation of funds to particular projects. This rule is as follows: accept the security investment if the NPV > 0, reject it if the NPV < 0, and be indifferent if the NPV = 0.

Figure 2 provides a representation of the preceding discussion in terms of appropriate level of total cybersecurity investments. As shown in that figure, the goal is to invest in cybersecurity at a level where the total costs of cybersecurity investments and breaches are at a minimum. If you were to consider the *real options* (a real option is the right to undertake some business decision in the future) associated with cybersecurity investments, the above decision rule would need to be modified.

In making the business case for cybersecurity investments, private sector firms encounter significant added challenges that are not generally faced when making the business case for more traditional capital investments, such as investments related to producing a new product or service to sell in the open marketplace. The added challenges are primarily in regards to the utilization of

cost-benefit analysis. These challenges, as well as testable hypotheses associated with these challenges, are described below.

1. Measuring the Benefits from Cybersecurity Investments

The first special challenge/barrier associated with making the business case for cybersecurity-related investments by firms in the private sector concerns the difficulty in measuring the ex-ante and ex post benefits derived from such investments. These benefits are derived largely from the cost savings associated with potential cybersecurity breaches that are prevented due to the investments.[10] Thus, cybersecurity-related investments generally fall into the capital investment category known as cost savings (or cost avoidance) projects.

In terms of resource allocation decisions, cybersecurity investments need to compete with other organizational investments. In private sector organizations, investments are often classified as revenue generating, cost savings, or compliance (must do) projects (see Gordon, 2004, Chapter 12). A strong bias exists in the private sector firms toward investing in revenue generating projects because of the emphasis by investors on revenue growth of companies. Consequently, making the business case for cost savings projects is particularly difficult relative to revenue generating projects. In revenue generating projects (e.g., investing in a new product line), the ex post benefits can be observed in terms of the new revenues.[11]

In the case of cybersecurity related investments, the benefits from such projects are primarily derived from the costs of security breaches that the projects prevent. Clearly, these costs must be estimated rather than actually observed. In other words, the costs of breaches that are prevented (i.e., never arise) cannot be observed. Furthermore, these cost savings involve implicit costs, as well as explicit costs. The explicit costs are easier to quantify. They relate to the costs of such things as detecting and correcting security breaches. Some of these costs will be of a direct nature, whereas other costs will be indirect in nature. In terms of indirect costs, there are potential national security cost savings associated with cybersecurity breaches that would affect infrastructure assets. The implicit costs relate to the costs associated with potential legal liabilities, and lost sales, accruing to firms as a result of security breaches because additional security investments were not made. For private firms, these costs often significantly exceed the explicit costs. A useful way to look at costs savings is in terms of explicit vs. implicit costs and direct vs. indirect costs, as shown in Figure 3. Of course, estimating the *ex ante* cost savings (which represent the benefits) derived from cybersecurity investments poses a difficult challenge/barrier for investments in cybersecurity by private sector firms.

[10] Although cybersecurity investments can generate new revenues as a result of a firm's ability to develop a competitive edge in terms of cybersecurity, the bulk of the benefits generally derive from preventing cybersecurity breaches.

[11] For must do projects (e.g., pollution abatement investments), the ex post benefits are in terms of the explicit penalties associated with not investing in such projects. These penalties generally can be derived and provides a strong economic incentive to invest in such projects.

Figure 3: Conceptual View of Costs of Security Breaches

	Direct Costs	Indirect Costs
Explicit Costs		
Implicit Costs		

The challenge/barrier associated with estimating the benefits associated with investing in cybersecurity investments also surfaces when trying to evaluate the performance of cybersecurity investments actually made. That is, deriving the *ex post* benefits from actual cybersecurity investments is far more difficult than evaluating the *ex post* benefits from revenue generating projects. The reason for the extra difficulty is due to the fact that the ex post benefits cannot be observed. Thus, the *ex post* benefits must be estimated by computing the difference between estimated costs of security breaches without the additional cybersecurity investments to actual costs of security breaches with the additional cybersecurity investments.

The above discussion led us to consider the first generic hypothesis that underlies the research reported in this Report. This hypothesis is stated below, in the alternative form.

H1: The uncertainties associated with measuring the benefits from cybersecurity have created a situation such that it is more difficult for managers to get funds for cybersecurity investments than for investments related to traditional revenue generating projects.

2. Risk of Cybersecurity Breaches

The second special challenge associated with making the business case for cybersecurity-related investments by firms in the private sector concerns the unusual difficulty in assessing the risk associated with cybersecurity breaches. Cybersecurity risk relates to the probability of breaches materializing as a result of different vulnerabilities and potential threats. The size of the potential loss associated with cybersecurity breaches is another aspect of the risk. Given the highly uncertain nature of such threats, vulnerabilities, and the potential losses associated with cybersecurity breaches, risk analysis pertaining to cybersecurity breaches is as much an art as it is a science. Consequently, the common practice for considering traditional capital investments among private firms of using the cost of capital to discount the future cash flows (i.e., the difference between the Bs and Cs in Equation 1 above) usually is not sufficient to properly consider the risk associated with cybersecurity investments. In a similar vein, estimating the expected loss associated with a security breach does not properly address the issue of risk for cybersecurity investments.

The fact that the risk associated with security breaches is difficult, at best, to specify does not reduce the importance of conducting risk analysis associated with cybersecurity investments. It does, however, present a serious challenge/barrier to those private sector managers proposing cybersecurity investments when competing for funding with more traditional revenue generating investments, such as an investment to initiate a new product line where the firm's cost of capital is often viewed as the appropriate discount rate to use in Equation 1.

The above discussion led us to consider the second generic hypothesis that underlies the research described in this Report. This hypothesis is stated below, in the alternative form.

H2: Most individuals involved in making cybersecurity investments poorly understand the risk associated with cybersecurity investments.

3. Externalities: The Need for Incentives and Regulation

The third special challenge associated with making the business case for cybersecurity-related investments by private sector firms relates to quantifying the externalities (i.e., spillover effects) associated with cybersecurity investments. These externalities result from the fact that cybersecurity investments (and the lack thereof) by one firm have spillover effects, including the free-rider and tragedy of commons effects, on other firms. For example, as one firm invests more in cybersecurity, there are positive spillover effects that will likely reduce the incentives for other firms to invest in cybersecurity. Alternatively, poor cybersecurity by one firm will likely have negative spillover effects on other firms.

Regretfully, there are often no incentives for the culpable firm to invest in cybersecurity to correct the negative spillover effects. Furthermore, measuring these externalities falls largely under the domain of welfare economics, which is tricky, at best, to quantify. The above notwithstanding, there is a growing belief among researchers and policy makers that economic incentives are required in order to get private sector firms to make the requisite investments in cybersecurity. There are also those who believe that economic incentives alone will not resolve the issue of externalities associated with cybersecurity investments. Thus, many argue that additional government regulations are required to achieve the desired goal in terms of private sector investments in cybersecurity. An analogy that is often made, in this latter regard, is in terms of seat belts for automobiles. Not using seat belts in automobiles has negative externalities in terms of the social costs relating to hospital costs associated with injuries to people that are involved in car accidents. Unfortunately, incentives alone did not get most people to buy automobiles with seat belts, let alone buckle-up. Instead, it took government legislation forcing automobile manufacturers to make seat belts a standard automobile requirement, and driving laws to force people to buckle-up.

The above discussion led us to consider the third generic hypothesis that underlies the research reported in the report. This hypothesis is stated below, in the alternative form.

H3: Due to externalities, when firms only consider private profits they tend to under-invest in cybersecurity.

D. Research Design

We addressed issues related to the above three hypotheses using various complementary research methodologies. We began by examining the relevant existing literature. We then developed analytic models for investing in cybersecurity. One of our analytic models resulted in a paper (forthcoming in the *Journal of Cybersecurity*) that shows that the potential for government incentives/regulations to increase cybersecurity investments by private sector firms is dependent on two fundamental issues: (1) whether or not firms are utilizing the optimal mix of inputs to cybersecurity, and (2) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. Another one of our models examined the effect of externalities on cybersecurity investment decisions, based on the models used in Gordon and Loeb (2002) and Gordon et al. (2003b). This model examined how the existence of well-recognized externalities changes the maximum a firm should, from a social welfare perspective, invest in cyber security activities. The results of this work resulted in a paper published in the *Journal of Information Security.* A third paper resulting from our analytic models focused on demonstrating how information sharing would likely encourage firms to take a more proactive, as compared to a reactive, approach toward cybersecurity investments. This paper is forthcoming in the *Journal of Accounting and Public Policy*.

While developing the above noted analytic models, we conducted interviews with senior executives involved in cybersecurity investment decisions (e.g., CFOs, CIOs, CISOs). We also conducted four in-depth case studies of firms that had experienced major cybersecurity breaches, using (heretofore) untapped publically available data. The next stage of our research project focused on designing a questionnaire for conducting a large scale survey of senior executives (e.g., CFOs, CIOs, CISOs) involved in cybersecurity related activities. The questionnaire-based survey represented the final methodology utilized in our research project. The data collected from the survey was used to statistically test the hypotheses underlying the study. Prior to finalizing and mailing the questionnaire-based survey, we conducted a pilot study to assess the survey instruments reliability and validity. The questionnaire was sent to the CFOs and CIOs of approximately 1600 major organizations from a variety of industries (details of the survey methodology follow in the section with the survey results).

E. The Remainder of this Report

The next section of this Report contains the final versions of the papers that have been published or are forthcoming, as a result of the research. The third section of the Report has the results of the interviews with the CIOs and CISOs, as well as the four case studies. The fourth section of this Report provides a description of the survey methodology, the survey results, and a discussion of the results. The fifth section has a summary of other supporting activities. These activities include the participation in meetings and workshops, the presentations made, and the educational courses developed. The sixth section has a plan for a proposed extension of this research. The seventh, and final, section provides some concluding comments.

Section I Selected References

Bodin, L., L. A. Gordon and M. P. Loeb, "Information Security and Risk Management," *Communications of the ACM*, Vol. 51, No. 4, 2008, pp. 64-68.

Bourgeois III, L.J. and K. M. Eisenhardt, "Strategic Decision Processes in High Velocity Environments: Four Cases in the Microcomputer Industry," *Management Science*, Vol. 34, pp. 816-835, 1988.

Campbell, K., L. A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, 11 (2003), pp. 431-448.

Eisenhardt, Kathleen M., "Building Theories from Case Study Research," *Academy of Management Review*, Vol. 14, 1989, pp. 532-550.

Gansler, J. S. and W. Lucyshyn, "Improving the Security of Financial Management Systems: What are We To Do?" *Journal of Accounting and Public Policy*, Vol. 24, No. 1, pp. 1-9.

Gordon, L. A., "Incentives for Improving Cybersecurity in the Private Sector: A Cost- Benefit Perspective," Testimony for the House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, October 31, 2007, http://chsdemocrats.house.gov/SiteDocuments/20071031155020-22632.pdf.

Gordon, L. A., and M. P. Loeb. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, November 2002a, pp. 438-457.

Gordon, L. A., and M. P. Loeb, "Return on Information Security Investments: Myths vs. Reality," *Strategic Finance*, November 2002b, pp. 26-31.

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

Gordon, L. A., M. P. Loeb, and W. Lucyshyn, "Cybersecurity Investments in the Private Sector: The Role of Governments," *Georgetown Journal of International Affairs*, October 2014, pp.79-88.

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

Gordon, L. A., M. P. Loeb, and W. Lucyshyn, "Sharing Information on Computer Systems: An Economic Analysis," *Journal of Accounting and Public Policy*, Vol. 22, No. 6, 2003b, pp. 461-485.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and R. Richardson, "2005 CSI/FBI Computer Crime and Security Survey," *Computer Security Journal*, Summer 2005, pp. 1-25.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and T. Sohail, "The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities," *Journal of Accounting and Public Policy*, 2006, pp. 503-530.

Gordon, L.A., M.P. Loeb and T. Sohail, "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly*, Vol. 34, No 3, 2010, pp. 567-594.

Gordon, L. A., M. P. Loeb and T. Sohail, "A Framework for Using Insurance for Cyber Risk Management," *Communications of the ACM*, Vol. 46, No. 3, March 2003, pp. 81-85.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou, (2015) Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, Vol. 6, No. 1, 2015, pp. 24-30

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou, "The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective," *Journal of Accounting and Public Policy*, forthcoming 2015.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou, "Increasing Cybersecurity Investments in Private Sector Firms," *Journal of Cybersecurity*, forthcoming 2015.

Gordon, L. A., M. P. Loeb and L. Zhou, "The Impact of Cybersecurity Breaches: Has there been a Downward Shift in Costs?" *Journal of Computer Security*, Vol. 19, No. 1, 2011, pp. 33-56.

Yin, Robert K., 1984. Case Study Research: Design and Methods, Sage Publications, Beverly Hills.

II. PUBLISHED AND FORTHCOMING ARTICLES

The articles listed below have either been published or are forthcoming as a direct result of the DHS research contract #N66001-12-C-0132. A complete copy of the articles is also included in this section of the Report.

A. "Cybersecurity Investments in the Private Sector: The Role of Governments" *Georgetown Journal of International Affairs*, October 2014

   This article shows that there are systemic barriers that corporations face in accurately assessing the appropriate levels of cybersecurity investment. The article also discusses the policies that governments could and should adopt in order to foster increased investments in cybersecurity related activities by profit-oriented corporations.

B. "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model" *Journal of Information Security* Vol. 6, No. 1, 2015

   This paper examines how the existence of well-recognized externalities changes the maximum a firm should, from a social welfare perspective, invest in cybersecurity activities. By extending the cybersecurity investment model of Gordon and Loeb (2002) to incorporate externalities, the paper shows that the firm's social optimal investment in cybersecurity increases by no more than 37% of the expected externality loss.

C. "Increasing Cybersecurity Investments in Private Sector Firms" *Journal of Cybersecurity*, forthcoming

   This paper develops an economics-based analytical framework that shows that the potential for government incentives/regulations to increase cybersecurity investments by private sector firms is dependent on: (1) whether or not firms are utilizing the optimal mix of inputs to cybersecurity, and (2) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. The implications of these findings are also discussed in this paper, as well as a formal analysis of these implications.

D. "The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective" *Journal of Accounting and Public Policy*, forthcoming

   Using a *real options* framework, this paper demonstrates how information sharing could reduce the tendency by firms to defer cybersecurity investments. To the extent that information sharing reduces a firm's uncertainty concerning a cybersecurity investment, the paper shows that information sharing may well lead firms to make cybersecurity investments sooner than otherwise would be the case. Moreover, the paper also shows that information sharing may increase the expected expenditures on cybersecurity activities.

A. Cybersecurity Investments in the Private Sector: The Role of Governments

Georgetown Journal of International Affairs, October 2014

by

Lawrence A. Gordon, Martin P. Loeb, & William Lucyshyn

Abstract

Cybersecurity risks have become a major concern to profit-oriented corporate senior managers and Boards of Directors. A key aspect of this concern has to do with deriving the appropriate level of investment in cybersecurity. Unfortunately, there are systemic problems that make determining the proper levels of investment difficult for profit-oriented corporations. These problems tend to result in corporations underinvesting in cybersecurity. This article has two objectives. First, this article will discuss these systemic barriers that corporations face in accurately assessing the appropriate levels of cybersecurity investment. Second, this article will analyze policies that governments could and should adopt in order to foster increased investments in cybersecurity related activities by profit-oriented corporations.

I. Introduction

The Internet has given rise to a burgeoning digital worldwide economy that goes way beyond what most could have imagined a few decades ago. Customers can buy products from firms around the world, and competitors can enter worldwide economic markets without many of the barriers to entry that plague traditional economic markets based on a brick-and-mortar presence. Many refer to this new economic model as a flat world of commerce (e.g., see Friedman, 2006). Unfortunately, as with most phenomena in life, there are both positive and negative features of this new world order of commerce. The introduction of new cybersecurity risks concomitant to conducting business in the cyber domain is one of the most notable of the negative aspects. Although evolving technology will continue to reduce system vulnerabilities for example, cloud technology can shift some of the security burden to the service provider ensuring consistent software with timely security updates—the threats change at even faster rates, identifying and exploiting new vulnerabilities.

Recent high-profile cybersecurity breaches at major multinational retail stores (e.g., Target, Inc.) prompted a February 4, 2014 U. S. Senate Judiciary Committee hearing and gained wide media coverage.[i] The coverage highlighted the cybersecurity risks confronting businesses, as well as the risks to consumers. Regretfully, 100% security is neither feasible nor economically justified even if it were viable. The above notwithstanding, corporate executives need to determine the amount their firms should invest in cybersecurity. Indeed, deciding the appropriate level to invest in cybersecurity related activities has become a critical concern for senior corporate executives. Furthermore, oversight of firms' cybersecurity activities is now on the agenda of corporate Boards of Directors (Yadron, 2014).

This article has two objectives. First, this article will point out the unique problems associated with deriving the appropriate level of cybersecurity investments by profit-oriented corporations. As will become clear, corporate underinvesting in cybersecurity activities is both systemic and not easily resolved. Second, this article will discuss policies that governments

could and should adopt in order to foster increased investments in cybersecurity related activities by profit-oriented corporations.

II. Cybersecurity Investments in Profit-Oriented Corporations

Profit-oriented corporations make all kinds of investments related to their business on a regular basis. Investments in buildings, technology-based equipment, computer software, personnel, and marketing are just some of the areas where executives regularly make investment decisions. Global corporations also typically make decisions regarding activities such as mergers and acquisitions. Investment decisions are generally made on a cost-benefit basis, under the rubric of what corporate executives usually refer to as "making the business case."[ii] A key aspect of the "business case" process is quantifying the benefits associated with the potential investment opportunities. Since most corporate investment opportunities focus on generating new revenues for the firm, the benefits from most investment opportunities are specified in terms of anticipated incremental revenues. These anticipated incremental revenues are translated into cash flows for discounted cash flow (DCF) analyses.[iii] Investment opportunities of this nature are usually referred to as revenue generating investments. Given that financial markets (especially the stock market) focus on revenue growth for firms, senior executives are always searching for new revenue generating investment opportunities.

Revenue generating investment opportunities are not, however, the only type of investment opportunities available to senior executives. Cost savings (or cost avoidance) investments are another category of corporate investment opportunities. Cost savings investment opportunities focus on accomplishing a particular task in a more cost efficient manner than was previously available to the corporation. A classic example of a cost savings corporate investment opportunity is replacing legacy manufacturing equipment with more modern, high-tech, equipment that significantly reduces the labor intensity of the manufacturing process. In such a case, the firm may be able to justify, and verify on an *ex post* basis, the return on the investment based on the cost savings in terms of cash flows (for DCF analyses) resulting from a substantially lower payroll expense.

Cybersecurity investment opportunities are generally a unique class of cost savings investments.[iv] For the most part, investments in cybersecurity activities are directed at avoiding the costs associated with cybersecurity breaches. What makes this class of investments unique is that the cost savings cannot be directly verified on an *ex post* basis. If a cybersecurity investment is successful, the cost savings comes from avoiding the non-observable cybersecurity breach. Thus, the *ex post* cost savings for cybersecurity investment opportunities need to be computed based on the difference between some sort of *ex ante* prediction of what the costs of security breaches would have been without the incremental cybersecurity investment and what the costs of security breaches actually turned out to be.[v] Not surprisingly, this situation makes the business case for cybersecurity investment decisions a much tougher sell to senior management than typical cost savings projects, let alone revenue-generating projects.[vi] As a result, there is a strong tendency for firms to underinvest in cybersecurity activities unless some sort of major security breach occurs **(**see Gordon et al., 2003a).

Another aspect of underinvestment in cybersecurity activities in profit-oriented corporations has to do with *externalities.* Externalities refer to the spillover effects of an activity. In other words, externalities are the costs (or benefits) to firms or individuals that arise from actions taken by another firm or individual that are not borne by the firm or individual taking the

action. In the context of corporations underinvesting in cybersecurity activities, externalities usually refer to the costs associated with weak cybersecurity protection borne by firms other than the initial firm that is underinvesting in cybersecurity activities. More specifically, firms that underinvest in cybersecurity activities only absorb the private costs resulting from a cybersecurity breach. These private costs would include the costs to detect and correct a cybersecurity breach, as well as any decreased revenues due to lost customers. In addition, any costs associated with legal liability incurred by a firm experiencing a cybersecurity breach could be a private cost to the firm. In contrast, the costs borne by supply-chain partners of the firm experiencing a cybersecurity breach, however, are not entirely absorbed by the firm that underinvests in cybersecurity activities. For example, underinvesting in cybersecurity by the initial firm can result in the inadvertent transfer of malware or vulnerabilities to a partnering firm, thereby causing a reduction in the partnering firm's current and future sales and profits. This reduction in the partnering firm's sales and profits are the result of externalities (i.e., spillover effects of the poor cybersecurity by the initial firm). The global reach of most firms, and their supply-chain partners, means that these externalities often extend far beyond national borders.

The combination of cybersecurity investments being unique cost-savings projects, and the externalities associated with cybersecurity breaches, have created a situation whereby corporate underinvesting in cybersecurity activities is both systemic and not easily resolved through free economic markets.

III. Government's Role in Corporate Cybersecurity Investments

The systemic tendency for corporations to underinvest in cybersecurity activities is, in part, the direct result of the extraordinary difficulties of justifying cybersecurity investments based on cost-benefit analysis (i.e., making the business case) relative to other corporate investment opportunities. Furthermore, the fact that corporations are only attuned to the private costs, while ignoring costs associated with externalities, also leads to corporate underinvestment in cybersecurity activities. This underinvestment increases the risk that a cyber-attack may take down an entire critical infrastructure industry (i.e., electric generation), causing critical damage to both a nation's economy and its national defense.

The situation described above demonstrates that there is currently a market failure, wherein a free economic market is unable to generate an efficient allocation of resources. Market failures often result in a situation where government intervention is desirable. In other words, governments are often able to play an important role where free economic markets fail. In this regard, there are several actions available to governments around the world to support a more efficient allocation of corporate resources to cybersecurity activities. The most obvious of these actions are discussed below.

Cybersecurity Regulation

The U.S. government has developed a new Framework (NIST 2014) for improving cybersecurity of the nation's critical infrastructure, which adopts a voluntary risk-based approach. The Framework is intended to be a living document, that is it will evolve over time, and it identifies five functions: identify, protect, detect, respond and recover. The objective is to assist firms in critical infrastructure sectors to identify key cybersecurity risks and issues, and help them assess their ability to respond to cyber-attacks. Ideally, the firms can then evaluate the need for improvements. The European Union, on the other hand, is taking a more broad and

direct approach, for example, by directing common minimum requirement for the Network and Information Security at the national level (European Commission, 2013).

Support for Education on Conducting Cost-Benefit Aspects of Cybersecurity Investments

As discussed, the primary benefits derived from investments in cybersecurity activities are the result of the cost-savings that result from avoiding or minimizing cybersecurity breaches. These savings, however, are not directly observable. Consequently, managers arguing for additional cybersecurity funds need to be able to develop estimates of the cost of cybersecurity breaches to their firm on an *ex ante* basis. The use of econometric models, as well as non-quantitative analyses (e.g., analytic hierarchy process), can be extremely valuable in making these estimates.

Managers arguing for cybersecurity investment funds need to understand how to combine the various risk factors (i.e., threats, vulnerabilities, and potential losses) into a meaningful framework for allocating cybersecurity resources. For example, a threat/vulnerability value grid could be developed to facilitate the handling of the risk associated with potential cybersecurity breaches (Gordon and Loeb, 2011).[vii]

The difficulties associated with estimating the cost savings from cybersecurity investments and considering the various risk factors presents an exceptionally challenging situation for those responsible for securing cybersecurity investment funds. This situation is further complicated by the fact that many managers responsible for implementing their firms' cybersecurity activities and proposing new cybersecurity projects have a background in technology, but little financial management training. Thus, these managers face a relative disadvantage in competing with financially savvy managers for project funding within the firm. Accordingly, governments can play an important role in rectifying this situation by supporting financial management training. Governments can reduce the underinvestment in cybersecurity activities by facilitating the education of cost-benefit analysis for cybersecurity investments. Governments should, in cooperation with universities and/or private sector firms, establish cybersecurity cost-benefit training programs for corporate executives.

Support for Corporate R&D on Cybersecurity

Research and development (R&D) on ways to combat cybersecurity threats are essential to cybersecurity. Corporations' willingness to invest in R&D, however, faces a number of obstacles. First, the payoffs from such investments are highly uncertain and are therefore often discounted heavily. Second, to the extent R&D efforts are successful, there are positive externalities that accrue to firms not making the initial investment (i.e., a large part of successful R&D often becomes a public good).[viii]

Governments can play an important role in the R&D cybersecurity arena, with a particular emphasis on government-corporate and government-academic partnerships. Such partnerships could and should cross national borders in that governments from various countries can join forces to support various research projects. A key concern is transferring the technological advances derived from the R&D into practical use by corporations. Governments can accelerate this process with the judicious use of funds and sponsorship, as has been done by the Department of Homeland Security.[ix]

Subsidies for Corporate Cybersecurity Investments

Governments could provide a direct subsidy (e.g., tax credit) for corporate cybersecurity investments along the lines of subsidies offered for other corporate activities (e.g., investments in energy efficient manufacturing processes). To the extent that such subsidies increase the overall corporate investments in cybersecurity activities, there are obvious benefits to the firms receiving the subsidy, as well as to their corporate partners (i.e., there are positive externalities).

Incentives for Information Sharing

Information is critical to the prevention, detection, and response to cyber-attacks. The relevant information, though, is dispersed among many organizations, including network operators, information systems hardware and software providers, law enforcement, and government intelligence organizations. Consequently, information sharing is critical to effective cybersecurity. "For example, during the denial-of-service attacks that targeted the websites of many leading U.S. banks over the last few years, the Financial Services Information Sharing and Analysis Center brought these banks together to exchange information with each other and with the Federal government" (Daniel, 2014). In the absence of appropriate incentive mechanisms, however, private sector firms often attempt to free ride on the cybersecurity expenditures of other firms, hoping to benefit from information of other firms, but refusing to share their private information (Gordon et al. 2003b). One of the most important steps to improving cybersecurity, particularly on a global scale, is for governments to develop and implement incentives that encourage more effective sharing of information related to cyber threats, vulnerabilities, and best cybersecurity practices.[x]

Support for Transparency of Corporate Cybersecurity Risks

In 2011, the U.S. Securities and Exchange Commission (SEC) came out with its Disclosure Guidelines concerning the importance of firms reporting their cybersecurity risks and cyber incidents on their Annual 10-K Reports (SEC, 2011). Prior to this Disclosure Guidance, a small percentage of the SEC registrants were already providing information on their cybersecurity related activities (see Gordon et al, 2006, 2010). However, since the issuance of the 2011 Disclosure Guidance, nearly all firms are reporting some aspect of cybersecurity risks and/or cyber incidences in their 10K reports (often under Section 1A, titled Risk Factors). The above notwithstanding, much of the information provided tends to be of a boiler-plate nature, often just pointing out the fact that a serious cybersecurity breach could have a negative impact on the firm's business.

The above noted Disclosure Guidance has moved corporations registered with the U.S. SEC toward improved transparency concerning cybersecurity risks and incidences. The movement thus far, however has been modest at best. Accordingly, we agree with the opinion expressed by Senator Rockefeller in his April 9, 2013 letter to the SEC Chairperson, where he noted that the 2011 Disclosure Guidance was an important first step, but "**…** given the growing significance of cybersecurity on investors' and stockholders' decisions, the SEC should elevate this guidance and issue it at the Commission level as well. While the staff guidance has had a positive impact on the information available to investors on these matters, the disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices" (Rockefeller, 2013). The SEC should also suggest that corporations specify the dollar amount of their expenditures on cybersecurity activities (i.e., similar to what is done with capital expenditures). Furthermore, the global nature of corporations (including the

fact that their stakeholders come from all over the world) requires an international movement toward corporate reporting of cybersecurity related activities and risks.

Global Cybersecurity Standards

The global nature of economic markets, combined with the fact that a firm's information and system security is only as strong as its weakest link, means that cybersecurity needs to be treated as a global, rather than national or local, issue. Although efforts do exist to establish global standards for cybersecurity (e.g., see ISO 27001, a standard for an Information Security Management System), these efforts have not been very effective to date. Given that cybersecurity issues are a relatively new issue confronting corporations, the lack of generally accepted and adopted global cybersecurity standards is unsurprising. Nevertheless, the establishment of global cybersecurity standards seems to be a necessary, though not sufficient, condition for eventually winning the cybersecurity battle.

One factor overlooked by most proponents of global cybersecurity standards is that a framework for developing and implementing such standards may already exist. A related situation exists in connection with developing and implementing global accounting standards. Ever since the early 1970's, businesses and governments have discussed the benefits of and need for international accounting. It was not until around the establishment of the International Accounting Standards Board (IASB) in 2001, however, that the movement finally gained momentum. Over 120 countries have adopted the International Financial Reporting Standards (IFRS) that the IASB issues.[xi] The parallels between the benefits of IFRS and the benefits from a potential international cybersecurity standards (ICS), suggest an IASB type framework for the development and establishment of ICS. A good starting place might be the implementation of an International Cybersecurity Standards Board along the lines of the IASB.

Governments, as a major consumer of goods and services, could begin by limiting their purchases to those firms complying with such global standards. As an interim step, governments could enforce such a purchasing rule based on national cybersecurity standards. It should be noted, however, that while cybersecurity standards may go a long way to improve cyber hygiene and offer protection against less sophisticated attacks, they are not without their drawbacks. In particular, standards can take years to develop, coordinate, and implement, but threats and supporting technologies change on a timescale of days, weeks, and months. Moreover, there are situations whereby imposing a standard may result in a firm redirecting cybersecurity funding away from a more productive security activity to a less productive security activity in order to meet the standard, thereby reducing the firm's overall level of cybersecurity.

IV. Concluding Comments

Cybersecurity has become a major concern to profit-oriented corporations. Given the rapid development of the digital and social networking revolution, there can be little doubt that managing cybersecurity risks will play an ever increasing role in managing the overall risks of firms. There are systemic reasons related to how profit-oriented corporations make investment decisions that explain why corporations tend to underinvest in cybersecurity activities. Corporate unwillingness to invest adequately in cybersecurity activities represent a market failure, resulting in significant cyber risks that spill over to other corporate and non-corporate entities. In addition, corporate underinvestment in cybersecurity activities put worldwide economies and the military defense of nations at risk. Governments could and should assume more active roles to facilitate greater corporate focus on cybersecurity related activities.

Endnotes:

[i] For the C-Span.org coverage of the Senate hearing, where Mr. John Mulligan, the Chief Financial Officer and Senior Vice President of Target, Inc., answered questions concerning the cybersecurity breach, see: http://www.c-span.org/video/?317553-1/hearing-cybercrime-privacy.

[ii] Making the business case refers to the process of identifying various opportunities, developing data to support the various opportunities, selecting the most profitable (i.e., highest return) opportunity and allocating resources to that opportunity (see Gordon and Loeb, 2006, Chapter 6).

[iii] DCF analyses are technique excused by economists for the purpose of computing either a net present value or internal rate of return on an investment opportunity (see Gordon and Loeb, 2006, Chapter 2).

[iv] Although it is possible for a cybersecurity investment to generate new revenues for a firm, due to some sort of competitive advantage, this aspect of cybersecurity investments is usually of insignificant consequences relative to the cost savings aspects of cybersecurity investment decisions.

[v] Moreover, cybersecurity breaches are not always detected, thus, making the measurement of the savings from the cybersecurity investment even more troublesome.

[vi] Since financial markets (especially stock markets) tend to focus on revenue growth as a key indicator of corporate growth, revenue-generating projects are clearly preferred over cost-savings projects by most senior executives.

[vii] The Gordon and Loeb (2011) article, in *The Wall Street Journal*, provides a non-mathematical approach to using the Gordon-Loeb Model (see: http://en.wikipedia.org/wiki/Gordon-Loeb_Model) for cybersecurity investments**.** See Gordon and Loeb (2002) for the original technical presentation.

[viii] A public good is a good in which its availability for consumption is unaffected by its consumption by any individual and no individual can be excluded from its consumption.

[ix] The U.S. Department of Homeland Security (DHS) has taken a lead in supporting R&D partnerships with academicians and corporations, as well as in facilitating multinational support for such projects (see http://www.dhs.gov/csd-new-projects).

[x] In a recent policy document, the Justice Department regulators explained that sharing of cyber-threat information differs from the sharing of competitive information, such as pricing data and business plans, and is not a violation of anti-trust laws (Wyatt 2014).

[xi] It is interesting to note that the U.S. is one of the countries that has not yet adopted IFRS, although the U.S. SEC does allow foreign registrants to use IFRS for the purpose of SEC reporting. For an excellent summary of the history of the SAB and IFRS, go to the FASB website at: http://www.fasb.org/jsp/FASB/Page/SectionPage&cid=1176156304264.

References:

Daniel, Michael (2014), "Getting Serious about Information Sharing for Cybersecurity," The White House Blog, April 10, available at http://www.whitehouse.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity

Friedman, T. L. (2006). *The world is flat [updated and expanded]: A brief history of the twenty-first century*. Macmillan.

Gordon, L. A., & Loeb, M. P. (2006). *Managing cybersecurity resources: a cost-benefit analysis* (Vol. 1). New York: McGraw-Hill.

Gordon, Lawrence A., and Martin P. Loeb. "The economics of information security investment." *ACM Transactions on Information and System Security (TISSEC)* 5.4 (2002): 438-457.

Gordon, L. A. and M. P. Loeb, "You May Be Fighting the Wrong Security Battles," *Wall Street Journal*, September 26, 2011 (see: http://online.wsj.com/news/articles/SB10001424053111904900904576554762089179984).

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

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003b). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and 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. *Journal of Accounting and Public Policy*, *25*(5), 503-530.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS quarterly*, *34*(3), 567-594.

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.

National Institute of Standards and Technology. 2014. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. February 12, 2014

Rockefeller, J. D., Letter to Ms. Mary Jo White, SEC Chairperson, April 9, 2013 (see: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51).

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

Wyatt, E. (2014). 2 Regulators Issue Guidelines on Sharing Cyber Security Information. Ney York Times. April 10, 2014. Available at http://bits.blogs.nytimes.com/2014/04/10/2-regulators-issue-guidelines-on-sharing-cyber-security-information/?_php=true&_type=blogs&_r=0

Yadron, D. (2014). Corporate Boards Race to Shore Up Cybersecurity; Directors Grapple With Issues Once Consigned to Tech Experts. Wall Street Journal (Online). Jun 29, 2014

B. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model

By Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Lei Zhou

Journal of Information Security, 2015, 6, **-**
Published Online January 2015 in SciRes. http://www.scirp.org/journal/jis
doi

Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model

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

[1]Robert H. Smith School of Business, University of Maryland, College Park, USA
[2]School of Public Policy, University of Maryland, University of Maryland, College Park, USA
Email: lgordon@rhsmith.umd.edu, mloeb@rhsmith.umd.edu, lucyshyn@umd.edu, lzhou@rhsmith.umd.edu

Received **** 2015

Abstract

Cyber security breaches inflict costs to consumers and businesses. The possibility also exists that a cyber security breach may shut down an entire critical infrastructure industry, putting a nation's whole economy and national defense at risk. Hence, the issue of cyber security investment has risen to the top of the agenda of business and government executives. This paper examines how the existence of well-recognized externalities changes the maximum a firm should, from a social welfare perspective, invest in cyber security activities. By extending the cyber security investment model of Gordon and Loeb [1] to incorporate externalities, we show that the firm's social optimal investment in cyber security increases by no more than 37% of the expected externality loss.

Keywords

Economics of Information Security, Cyber Security Investment

1. Introduction

With economic activity and national defense heavily and increasingly dependent on networked computer systems, cyber security issues continue to draw increasing attention by the media, as well as by executives at the highest levels of government, industry, and nonprofit organizations.[1] A key reason for this increasing attention on cyber security issues by governments around the world is the eminent threat posed by cyber security breaches to a nation's national defense and the nation's economic strength [2].

[1]For purposes of this paper, we use the term *cyber security* to mean the protection of information that is transmitted via any computer network, including the Internet. In addition, for the purpose of this paper, the terms *cyber security* and *information security* are considered to be synonymous.

How to cite this paper: Author 1, Author 2 and Author 3 (2015) Paper Title. *Journal of Information Security*, **6**, **-**.
http://dx.doi.org/10.4236/***.2015.*****

Firms in the private sector of many countries own a large share of critical infrastructure assets.[2] Hence, cyber security breaches in private sector firms could cause a major disruption of a critical infrastructure industry (e.g., delivery of electricity), resulting in massive losses throughout the economy, putting the defense of the nation at risk. Moreover, the cyber security activities of a given firm affect not only the probability of that firm suffering a cyber security breach, but also the probability that other firms (and individuals) suffer cyber security breaches. As one example, consider a firm that is not adequately protected against malware that infects the firm's computer system and, although undetected, use that firm's computer as part of a botnet to attack other firms. Since there is no practical way for a firm to be made liable for the entirety of losses from breaches to other firms caused by the vulnerabilities to its own computer systems, complete reliance on market mechanisms to overcome the externalities problem breaks down (*i.e.*, using the terminology of economics, there are market failures). In fact, it is well known that in the absence of government incentives and/or regulations (hereafter incentives/regulations) firms will under invest in cyber security activities relative to the quantity that maximizes social welfare (e.g., [5]-[8]). Thus, governments have an interest in providing incentives/regulations to firms to invest in cyber security activities at a level that takes into account not only the private losses incurred by firms from breaches of cyber security, but also takes into account the costs of externalities resulting from such beaches.[3,4]

A prelude to developing incentives/regulations that take into consideration the costs of externalities, as well as the private costs, is an understanding of the relationship between the magnitude of externalities and the magnitude of cyber security underinvestment. Thus, the objective of this paper is to investigate the magnitude of underinvestment in cyber security activities by a private sector firm that considers only its private costs and benefits without regard to externalities. This investigation will take place in the context of the influential Gordon-Loeb Model presented in [1], hereafter referred to as GL Model, for deriving the appropriate level of cyber security investment.[5] Earlier work, while recognizing that externalities results in underinvestment, has not sought to characterize the specific degree of underinvestment.

The primary contribution of this paper is to show how the existence of externalities changes the GL rule for the maximum a firm should, from a social welfare perspective, invest in cyber security activities. By analyzing the degree to which ignoring externalities causes underinvestment by firms in the absence of government regulations and incentives, the paper provides a basis for future examinations of potential actions designed to counteract cyber security underinvestment by private sector firms.

The remainder of this paper will proceed as follows. In the next, second, section of the paper we review the influential GL Model for making information security (cyber security) investments, and the subsequent literature dealing with the model. In the third section, we examine the effect of externalities on the optimal level of cyber security investment among private sector firms. We start by analyzing a specific example and then provide a general result characterizing the effect of externalities on the upper bound of a firm's optimal level of cyber security investment. The fourth, and final, section of this paper will present some concluding comments.

2. GL Model Literature

In order to investigate the magnitude of a firm's underinvestment (from a social welfare perspective), we analyze and extend the GL Model. Considering only the firm's private cost and benefits, GL characterized a firm's optimal amount to invest in cyber security activities. In doing so, they defined a security breach function that captured the relationship between the level of cyber security activity expenditures and the probability of a cyber security breach. As such, GL were able to address the fundamental question of particular interest to organizations concerning how much to spend on cyber security activities.[6] GL present a single period economic model to

[2]In the U.S., for example, a figure of 85% has been used in various government reports concerning the portion of U.S. critical infrastructure assets owned by firms in the private sector (e.g., see http://www.dhs.gov/critical-infrastructure-sector-partnerships). The importance of the critical infrastructure in the U.S. is highlighted by [3] and [4].

[3]For example, see [9] and [10].

[4]Although the focus in this paper is on the U.S., the issues addressed in the paper are equally applicable to other countries.

[5]The GL model is widely cited in the cyber security research literature, with more than 700 Google Scholar citations at the time of this writing and having been featured in both *The Wall Street Journal* (see http://www.wsj.com/news/articles/SB10001424053111904900904576554762089179984) and *Financial Times* see http://www.ft.com/cms/s/2/606e0e5a-b345-11e2-b5a5-00144feabdc0.html#axzz2iO8fsZhJ). Böhme [11] writes, "Undoubtedly the most famous security investment model has been proposed by Gordon and Loeb… (p. 11)."

[6]Some other key questions receiving attention in the literature include (1) what is the economic cost of a cyber security breach? (e.g., [12], [13], [14]), (2) what is the effect of information sharing on cyber security? (e.g., [6], [15], [16]), (3) what strategies should be employed to manage cyber security risks? (e.g., [17]), and (4) what is the market value impact of disclosing information security activities on the 10-K Reports file with the Securities and Exchange Commission (e.g., [18]).

examine the problem of a risk-neutral firm selecting the optimal level of expenditures on cyber security activities. The GL Model examines how the firm's optimal level of cyber security expenditures, denoted z^*, varies with two parameters: 1) v, the probability that a cyber security attack will be successful in the absence of any cyber security expenditures, and 2) L^P, the expected loss to the firm if the attack is successful. The model is briefly summarized below.

Denote $S(z,v)$ as the firm's security breach function, defined as the probability that an information security breach occurs and where z is the firm's monetary investments in cyber security and v $(0 \le v \le 1)$ represents firm's the underlying vulnerability to security breaches. GL postulate that the security breach function is twice continuously differentiable and meets the following five regularity conditions: 1) for all $z \ge 0$, $S(z,0) = 0$; 2) for all $v \in (0,1)$, $S(0,v) = v$; 3) for all $v \in (0,1)$ and for all $z \ge 0$ and $\partial S(z,v)/\partial z < 0$; 4) for all $v \in (0,1)$ and for all $z \ge 0$, $\partial^2 S(z,v)/\partial z^2 > 0$ and; 5) for all $v \in (0,1)$, $\lim_{z\to\infty} S(z,v) = 0$. That is, 1) if the firm's information is perfectly invulnerable, then it will remain so for all levels of cyber security investments; 2) if there is no investment in cyber security, the probability of a successful breach will be the underlying vulnerability; 3) increases in cyber security investment will decrease the probability of a successful breach; 4) the security breach function is strictly convex in z, *i.e.*, there are diminishing returns to cyber security investment and; 5) by investing sufficiently in cyber security the probability of a successful breach can be made arbitrarily close to zero.

When making the security investment decision, the firm would choose an investment level (z^*) so that the total expected net benefits from the investment is maximized:

$$\max_z \left[v - S(z,v) \right] L^P - z, \tag{1}$$

and needs to satisfy the following condition:

$$-S_z(z^*, v) L^P = 1. \tag{2}$$

For security breach functions meeting the aforementioned five regularity conditions, GL provide some general results concerning the relation between the optimal level of cyber security investment, z^*, and the prior level of vulnerability, v. The principal result demonstrated by GL, however, is that for a risk-neutral firm, the optimal investment in information security is generally a small fraction of the expected loss of a breach. Specifically, GL show that for the two broad classes of security breach functions satisfying the regularity conditions given below:

$$S^{\mathrm{I}}(z,v) = \frac{v}{(\alpha z + 1)^{\beta}}, \text{ where } \alpha > 0 \text{ and } \beta \ge 1, \tag{3}$$

and

$$S^{\mathrm{II}}(z,v) = v^{\alpha z + 1}, \quad \text{where } \alpha > 0. \tag{4}$$

The optimal investment in information security is always less than or equal to $1/\mathrm{e}$ (approximately, 36.79%) of the expected loss from a security breach (*i.e.*, $z^* \le vL^P/\mathrm{e}$, GL Proposition 3). Beyond the two specified classes of security breach functions (and a third class given in [1], footnote 18), GL conjectured that the $1/\mathrm{e}$ rule holds for all security breach functions satisfying the specified regularity conditions.

Willemson [19] provided a method for constructing a security breach function meeting all the assumptions of GL for which the optimal level of investment could be made to be arbitrarily close to 50% of the expected loss. Furthermore, by relaxing the GL assumption that the security breach function is continuously twice differentiable, [19] demonstrated that security breach functions could be constructed such that the optimal cyber security investment is arbitrarily close to the expected loss.

While the result of [19] appeared to severely limit the generality of the $1/\mathrm{e}$ rule, analysis by [8] and [20] proved that the rule "holds in full generality, thus justifying the intuition" ([20], p.1) of GL. In order to resurrect the $1/\mathrm{e}$ rule, [8] and [20] assumed that security breach function was not just convex but log-convex.[7] Thus, if the security breach function satisfies regularity conditions (1), (2), (3), (4') and (5), where (4') is the conditions that the security breach function is log-convex, then the optimal investment in information security for a risk-neutral firm is always less than or equal to $1/\mathrm{e}$ of the expected loss from a security breach, *i.e.*, $z^* \le vL^P/\mathrm{e}$.

[7] A function f is log-convex if "the composition of the logarithmic function with f, is a convex function" (http://en.wikipedia.org/wiki/Logarithmically_convex_function). A log-convex function is necessarily convex, but a convex function may not be log-convex.

Furthermore, [20] provided some assumptions on the nature of cybersecurity activities that would be sufficient to give rise to the security breach function being log-convex.

3. Modifying the GL Model to Incorporate Externalities

In modeling a firm's selection of the optimal amount to invest in information security, GL only considered the private costs to be borne by a firm that result from an information (cyber) security breach. The private costs of a breach, denoted by L^P in the GL Model, take into account not only items such as the costs of remediation, the cost of lost sales from downtime on sales websites and loss in competitive position through the loss of trade and strategic secrets, but also the loss from potential suits by other firms and customers who were would be hurt by the firm's information security breach. Thus, to the extent that judgments and settlements expected from lawsuits resulting from a breach will account for the losses imposed on others, the externalities (spillover effects) would be fully internalized via the GL Model.[8]

There are good reasons, however, to believe that expected legal judgments and settlements would not fully internalize the externalities associated with an information security breach. For example, suppose a security breach results in malware that allows an attacker to gain complete control over the affected computer. That firm's computer can then be controlled remotely to connect back to a central server, and become part of a network of compromised computers or "botnet" (often just called a "bot"). This network can be used for a variety of malicious purposes, such as conducting a distributed denial of service (DDOS) attack. The DDOS attack may well cause substantial losses to other organizations, yet the contribution of one computer (or one firm's computers) towards the overall loss would be so small that the threat of legal repercussions to the firm owning the compromised computer(s) would be insignificant. Similarly, in addition to the cost of lost sales faced by the firm victimized by a DDOS attack, customers may face non-pecuniary costs in lost time and frustration in attempting to access the attacked firm's website. While the costs to an individual customer may be small and difficult to detect and measure, the aggregate costs to all customers could be substantial. Still, because the individual losses are small, legal action spurred by these losses would not likely be taken on behalf of these customers. In addition, even if legal actions were to occur, where the final responsibility for covering these costs rests is unclear. The extension of the GL Model that follows is an attempt to show the impact of considering these, as well as other, externalities, on the adequacy of cyber security investments.

Let L^E represent the externality (spillover) costs of an information security breach, defined as the total loss to consumers and other firms, not captured within the private loss L^P, from a breach of information security. Let L^{SC} represent the total social costs of an information security breach defined as the sum of the firm's private loss plus the externality costs (*i.e.*, $L^{SC} = L^P + L^E$).

The GL Model can then be easily extended to incorporate the externalities. The social optimal level of investment for the firm, denoted z^{SC}, is the level that maximizes expected benefits net of both the private loss and externality costs:

$$\max_z \left[v - S(z,v)\right] L^{SC} - z, \tag{5}$$

so that z^{SC} satisfies the first-order condition:

$$-S_z\left(z^{SC}, v\right) L^{SC} = 1. \tag{6}$$

By comparing (6) and (2), and assuming $L^E > 0$ and that increasing information security investment decreases the probability of an information security breach, but at a decreasing rate ($S_z(z,v) < 0$ and $S_{zz}(z,v) > 0$, *i.e.*, regularity assumptions 3 and 4), one can see that $z^{SC} > z^*$. That is, the socially optimal amount for the firm to invest in information security is greater than the firm's (private) optimal amount. This is merely a formal demonstration that firms, without additional incentives, will under invest in information security.

In order to examine the possible magnitude of a firm's under investment in information security relative to the amount that maximizes social welfare, we first examine security breach function of the class I type specified by (3). Then, the firm's (private) optimal investment in information security is given by (GL Equation (6)):

$$z^*(v) = \left[\left(v\beta\alpha L^P\right)^{1/\beta+1} - 1\right] \Big/ \alpha. \tag{7}$$

[8]The combination *of externality costs* and *private costs* is what economists refer to as *social costs*.

Now suppose for the firm's initial probability of an information security breach $v = 0.64$, the parameters $\alpha = 0.00001$, $\beta = 1$, and the firm's private loss from an information security breach is $400,000. Then, from (7), the firm's optimal investment in information security is $60,000 (which equals exactly 23.4375 % of its expected private loss). Suppose now that the externality costs were 5% of its private loss, or $20,000, so the total social costs of a breach, L^{SC}, equals $420,000. Using L^{SC}, the socially optimal amount for the firm to invest would be $63,951. Thus, externality costs of 5% results in a 6.18% (=3,951/63,951) under investment in information's security. If externality costs were 100% of the private loss, then the social welfare maximizing investment would be $126,274, so that a firm focusing only on its own private costs would, from a societal perspective, be under investing by 52.48% (=[126,274 – 66,274]/126,274).

The preceding discussion illustrates that in the presence of externalities, social costs diverge from private costs resulting in underinvestment by the firm. **Table 1** provides additional data on how underinvestment percentage changes with externality costs for the specified example.

The following proposition, a generalization of the GL rule, shows how externalities affect the magnitude of a firm's maximum socially optimal investment in cyber security.

Proposition 1: Suppose the security breach probability function satisfies regularity conditions (1), (2), (3), (4') and (5). Denote $\gamma = L^E / L^P$ That is, γ is the ratio of externality losses to private losses for a successful cyber breach, (or 1/100 of the percent externality cost). Then the inequality below characterizes the maximum a risk-neutral firm should invest to protect information set, taking into account externalities as well as private costs:

$$z^{SC}(v) < (1/\mathrm{e})(1+\gamma)vL^P \approx 0.3679(1+\gamma)vL^P. \tag{8}$$

Proof: The maximum socially optimal amount is found by substituting L^{SC} for L^P in the GL model. This yields the rule that the socially optimal investment amount is less than or equal to $1/\mathrm{e}$ of the total social costs:

$$z^{SC}(v) < (1/\mathrm{e})vL^{SC} \approx 0.3679vL^{SC}. \tag{9}$$

The desired result, inequality (8), follows since $L^{SC} = (1+\gamma)\mathrm{L}^P$. Q.E.D.

Notice that for the special case where there are no externalities, $\gamma = 0$, (8) reduces to the GL Model result. **Table 2** shows how the maximums social optimal changes as the magnitude of externalities increases. For example, when the potential external losses due to externalities equal 40% of the potential private losses, the maximum social investment in cyber security is at most 51.5% of the firm's private expected loss. When the externalities are extremely large (e.g., 180% of the private costs of a breach), the social optimal calls for an investment greater than the firm's private expected loss.

Table 1. Relationship between externalities and underinvestment in cybersecurity for security breach probability function $S^I(z, 0.64) = 0.64/(0.00001z + 1)$.

(1)	(2)	(3)	(4)	$(5) = 100\% \times [(4) - (3)]/(4)$
Percent Externality Cost $100\% \times \frac{L^E}{L^P}$	**Private Loss (*i.e.*, costs) from a Successful Cyber Security Breach** (L^P)	**Optimal Cyber security Investment Based on Private Costs**	**Optimal Cyber security Investment Based on Total Social (Private + Externality) Costs**	**Percent Underinvestment by Failing to Consider Externalities**
0%	$400,000	$60,000	$60,000	0%
20%	$400,000	$60,000	$75,271	20.29%
40%	$400,000	$60,000	$89,315	32.82%
60%	$400,000	$60,000	$102,386	41.40%
80%	$400,000	$60,000	$114,663	47.67%
100%	$400,000	$60,000	$126,274	52.48%
120%	$400,000	$60,000	$137,318	56.31%
140%	$400,000	$60,000	$147,871	59.42%
160%	$400,000	$60,000	$157,992	62.02%
180%	$400,000	$60,000	$167,731	64.23%
200%	$400,000	$60,000	$177,128	66.13%

Table 2. Maximum social optimal investment as externalities vary.

Percent Externality Cost (γ)	Maximum Social Optimal Cybersecurity Investment as a Percent of Firm's Expected Private Expected Loss $\left(\frac{1+\gamma}{e}\right)$
0%	36.79%
20%	44.15%
40%	51.50%
60%	58.86%
80%	66.22%
100%	73.58%
120%	80.93%
140%	88.29%
160%	95.65%
180%	103.01%
200%	110.36%

Since most firms in the private sector look only at their private costs of security breaches, it is rational to expect them to under invest in cyber security activities relative to the social optimal. Accordingly, in order to move towards socially optimal levels of cyber security investments, there is a compelling argument for governments (or some other entity focusing on increasing social welfare) to explore a variety of regulations and/or incentives that are designed to get private sector firms to increase their cyber security investments.

4. Concluding Comments

The primary objective of this paper has been to extend the GL Model for deriving the optimal level of investment in cyber security activities. This extension focused on examining the impact of considering the costs associated with the externalities of cyber security breaches (*i.e.*, spill-over effects, of cyber security breaches to other organizations and individuals), in addition to private costs (*i.e.*, the costs to the individual organizations experiencing the cyber security breaches), on a private sector firm's optimal level of cyber security investment level as viewed from a social welfare perspective. For a risk-neutral firm, under specified regularity conditions, we show that the firm's social optimal investment in cyber security increases by no more than 37% of the expected externality loss. Unless private sector firms consider the costs of breaches associated with externalities, in addition to the private costs resulting from breaches, underinvestment in cyber security activities is essentially a given. Thus, cyber security underinvestment poses a serious threat to the national security and to the economic prosperity of a nation. Accordingly, governments around the world are justified in considering regulations and/or incentives designed to increase cyber security investments by private sector firms.

In the U.S. there is a general preference for developing market-based incentive mechanisms rather than new regulations to get private sector firms to increase their investment on cyber security activities. The efficacy of such an approach has, to date, been problematic. Indeed, the problems associated with successfully developing and implementing such incentives have led many in the U.S. to call for regulations requiring private sector firms to invest enough into cyber security activities to cover externalities as well as private sector costs.[9] In other countries, which are more heavily government controlled, regulations requiring private sector firms to increase their investment in cyber security activities to cover externalities (as well as private costs) may well be the clearly preferred method for handling the cyber security underinvestment concern.

Acknowledgements

This research has been supported by the United States Department of Homeland Security (DHS) Science and Technology Directorate, the Netherlands National Cyber Security Centre (NCSC) and Sweden MSB (Myndighetenförsamhällsskyddochberedskap)—Swedish Civil Contingencies Agency.

[9]In recent conversations between two of the authors of this paper and several senior executives from large private sector firms, it was clearly noted that, without a formal regulation concerning the investment level of cyber security activities, externalities were unlikely to be adequately considered by U.S. firms.

References

[1] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information System Security*, **5**, 438-457. http://dx.doi.org/10.1145/581271.581274

[2] U.S. Department of Homeland Security (2013) Executive Order 1636: Improving Critical Infrastructure, Department of Homeland Security Integrated Task Force, Incentives Study. Washington DC.

[3] Presidential Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. *Federal Registrar*, **78**, 11739-11743. https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[4] Presidential Policy Directive/PPD-21 (2013) Critical Infrastructure Security and Resilience. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[5] Varian, H. (2004) System Reliability and Free Riding. In Camp, L. and Lewis, S., Eds., *Economics of Information Security*, Springer US, 1-15. http://dx.doi.org/10.1007/1-4020-8090-5_1

[6] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, **22**, 461-485. http://dx.doi.org/10.1016/j.jaccpubpol.2003.09.001

[7] Kunreuther, H. and Heal, G. (2003) Interdependent Security. *Journal of Risk and Uncertainty*, **26**, 231-249.

[8] Lelarge, M. (2012) Coordination in Network Security Games: A Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications*, **30**, 2210-2219.

[9] Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636. (2013). http://www.treasury.gov/press-center/Documents/Supporting_Analysis_Treasury_Report_to_the_President_on_Cybersecurity_Incentives_FINAL.pdf

[10] U.S. Department of Homeland Security (2013) Executive Order 13636: Improving Critical Infrastructure, Department of Homeland Security Integrated Task Force, Incentives Study Analytic Report. http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

[11] Böhme, R. (2010) Security Metrics and Security Investment Models. In: Echizen, I., Kunihiro, N. and Sasaki, R., Eds., *Advances in Information and Computer Security*, Springer-Verlag, Berlin, Heidelberg, 10-24. http://dx.doi.org/10.1007/978-3-642-16825-3_2

[12] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, **11**, 431-448.

[13] Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, **9**, 69-104.

[14] Gordon, L.A., Loeb, M.P. and Zhou, L. (2011) The Impact of Information Security Breaches: Has There Been a Downward Shift in Cost? *Journal of Computer Security*, **19**, 33-56.

[15] Gal-Or, E. and Ghose, A. (2005) The Economic Incentives for Sharing Security Information. *Information Systems Research*, **16**, 186-208. http://dx.doi.org/10.1287/isre.1050.0053

[16] Hausken, K. (2007) Information Sharing among Firms and Cyber Attacks. *Journal of Accounting and Public Policy*, **26**, 639-688. http://dx.doi.org/10.1016/j.jaccpubpol.2007.10.001

[17] Gansler, J.S. and Lucyshyn, W. (2005) Improving the Security of Financial Management Systems: What Are We to Do? *Journal of Accounting and Public Policy*, **24**, 1-9. http://dx.doi.org/10.1016/j.jaccpubpol.2004.12.001

[18] Gordon, L.A., Loeb, M.P. and Sohail, T. (2010) Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, **34**, 567-594.

[19] Willemson, J. (2006) On the Gordon & Loeb Model for Information Security Investment. The Fifth Workshop on the Economics of Information Security (WEIS), University of Cambridge, 26-28 June. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.9931&rep=rep1&type=pdf

[20] Baryshnikov, Y. (2012) IT Security Investment and Gordon-Loeb's 1/e Rule. 2012 Workshop on Economics and Information Security, Berlin, 25-26 June. http://weis2012.econinfosec.org/papers/Baryshnikov_WEIS2012.pdf

C. Increasing Cybersecurity Investments in Private Sector Firms

Forthcoming in *Journal of Cybersecurity*

By

Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Lei Zhou

Abstract

The primary objective of this paper is to develop an economics-based analytical framework for assessing the impact of government incentives/regulations designed to offset the tendency to underinvest in cybersecurity related activities by private sector firms. The analysis provided in the paper shows that the potential for government incentives/regulations to increase cybersecurity investments by private sector firms is dependent on the following two fundamental issues: (1) whether or not firms are utilizing the optimal mix of inputs to cybersecurity, and (2) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. The implications of these findings are also discussed in this paper, as well as a formal analysis of these implications. In addition, this paper provides a discussion of existing actions by the U.S. federal government that should be more effectively utilized before, or at least in conjunction with, considering new government incentives/regulations for increasing cybersecurity investments by private sector firms.

I. Introduction

The percentage of U.S. critical infrastructure assets owned by private sector firms is usually estimated to be somewhere in the neighborhood of 85%.[1] The way these assets are operated and managed has vastly changed over the last few decades due to the impact of the digital revolution related to computer-based information systems. These changes have increased the efficiency associated with using infrastructure assets. The digital revolution, however, has also created serious risks to the nation's critical infrastructure due to actual and potential cybersecurity breaches.[2] As noted by President Obama in his Executive Order on Cybersecurity of February 12, 2013:

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront (Obama, 2013).

Numerous empirical studies point out the potential negative effects of these breaches on the performance of firms in the private sector (e.g., Gordon et al., 2011). The potential negative effects of cybersecurity risks and incidents on private sector firms have also been recognized by the U.S. Securities and Exchange Commission (SEC), as evidenced by the publication of its Disclosure Guidance (SEC, 2011). In fact, the SEC Disclosure Guidance recommends that firms disclose their cybersecurity risks and incidents in their annual10-K reports.

The cybersecurity risks and incidents confronting private sector firms raise the following fundamental question: How much should a firm in the private sector invest in cybersecurity activities? Answering the above question has been the subject of Congressional Hearings (e.g., Subcommittee of the U.S. House Committee on Homeland Security, 2007), academic research (e.g., Gordon and Loeb, 2002), and discussions among executives (e.g., Boardroom Cyber Watch Survey 2013[3])**.** Unfortunately, there is no simple answer to this question. The above notwithstanding, it is helpful to keep in mind that private sector firms are driven to a large degree by the desire to earn profits. Consequently, cybersecurity investment decisions by private sector firms are largely the result of cost-benefit analysis.[4]

Cost-benefit analysis, however, normally only considers the private costs associated with cybersecurity breaches (i.e., the costs to the firm directly affected by the breaches). The externalities (i.e., spill-over costs to other firms, in both the private and public sectors, as well as to individuals) associated with cybersecurity breaches are generally not factored into the cybersecurity investment decisions by firms in the private sector.[5,6] As Anderson and Moore

---

[1] Although the exact percentage is not known, the 85% figure has been used in various government reports (e.g., see http://www.dhs.gov/critical-infrastructure-sector-partnerships).

[2] The term *cybersecurity* is used in this paper to mean the protection of information that is transmitted via the Internet or any other computer network. The terms *cybersecurity* and *information security* are used interchangeably in this paper.

[3] See http://www.itgovernance.co.uk/what-is-cybersecurity/boardroom-cyber-watch.aspx

[4] In the private sector, cost-benefit analysis usually is based on some form of net present value (NPV) analysis.

[5] The sum of private costs and externalities is what economists refer to as social costs.

(2006) make clear the cybersecurity economics literature recognizes that externalities play a significant role in the underinvestment in cybersecurity. LeLarge (2012, p. 2210), emphasizing the effect of externalities, writes "security investments are always inefficient due to the network externalities."

Holding externalities aside, there is evidence that firms invest in cybersecurity activities at a level below what would be optimal considering private costs alone. A cursory look at some firms that experienced a major cybersecurity breach recently (e.g., Target, Inc., JP Morgan Chase, Inc., and SONY, Inc.) indicates that it took a significant cybersecurity breach for the firms to ramp up their level of cybersecurity investments. Indeed, it is reasonable for the U.S. federal government (hereafter referred to as the *government*) to assume that private sector firms are underinvesting in cybersecurity activities. Beginning with Anderson (2001), the issue of incentive alignment has been a central theme in literature on the economics of cybersecurity. Pym et al. (2013), for example, analyze the need for government intervention in cybersecurity in the context of an economic model of attackers and defenders. One should not be surprised, therefore, to find governments considering various incentives and/or regulations (hereafter referred to as government *incentives/regulations*) that would increase cybersecurity investments by firms in the private sector.[7,8]

The primary objective of this paper is to apply and extend economic production theory to the problem of assessing the impact of government incentives/regulations designed to increase the cybersecurity investments by firms in the private sector.[9] The production theory framework is based on an analysis of the relationships among cybersecurity inputs and outputs. Our input-output analysis provides important insights regarding the impact of various types of government incentives/regulations designed to increase the cybersecurity investments by firms in the private sector.[10] To our knowledge, this is the first study to conduct such an analysis.

The input-output analysis provided in this paper shows that the impact of government incentives/regulations on the cybersecurity investment decisions of firms is dependent on two

---

[6] An example of an externality related to cybersecurity would be a situation where a firm gets a computer virus and spreads that virus to its business partners through the firm's computer interactions with these other firms. The spill-over costs would be the costs incurred by these business partners as a result of receiving the virus. If the spill-over costs could be easily traced to the firm spreading the virus, and the firm could be held liable for these costs, these costs would become part of the private costs of the firm spreading the virus.

[7] The distinction between government *incentives* and *regulations* for purposes of this paper is as follows. A government incentive (e.g., tax incentive for energy efficiency) provides some sort of subsidy to encourage firms to voluntarily take specific actions that are consistent with achieving a desired outcome. In contrast, a government regulation (e.g., the Sarbanes-Oxley Act of 2002) is a law that mandates compliance with the law to achieve a desired outcome.

[8] Pursuant to Presidential Executive Order 13636, the U.S. Department of Homeland Security and the U.S. Treasury Department have recently released reports examining possible incentives/regulations to motivate private firms to increase their investments in cybersecurity. In this regard, see Obama (2013), the U.S. Department of Homeland Security Integrated Task Force, Incentives Study (2013), and the U.S. Treasury Department Report to the President on Cybersecurity Incentives (2013).

[9] While the model we present was motivated and is discussed in the context of cybersecurity, our analysis is more generally applicable to any loss-reducing investment by the firm (e.g., workplace safety or employee-theft prevention).

[10] For purposes of this paper, the terms *investments* and *expenditures* are used interchangeably.

fundamental issues. The two issues are: (1) whether or not firms are utilizing the optimal mix of inputs to cybersecurity (i.e., whether or not firms are accurately conducting and using cost-benefit analysis related to the inputs of cybersecurity investments), and (2) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. An analysis of these two issues results in general implications concerning whether government incentives/regulations will likely result in improvements in cybersecurity investments by private sector firms.

The remainder of this paper proceeds as follows. In the next, second, section of the paper we briefly review the relevant prior literature. The analytical framework for assessing the impact of government incentives/regulations on cybersecurity investments is presented in the third section of the paper. This framework is based on a microeconomic analysis via the inputs and outputs associated with cybersecurity investments. The analysis is initially presented in graphical terms. The third section of this paper also discusses the implications of our graphical analysis, with a focus on how government incentives/regulations could impact firms in the private sector to incorporate externalities, as well as private costs, in their cybersecurity investment decisions. A formal mathematical analysis supporting these implications is also provided in the third section of the paper. The fourth section of this paper provides a few specific examples of existing government incentives/regulations that have the potential for substantially enhancing the current level of investments in cybersecurity activities by private sector firms. The fifth, and final, section of this paper presents some concluding comments concerning the main arguments presented in this paper, as well as recommendations and limitations associated with these arguments. The fifth section of the paper also includes directions for future research in the area.

II. Literature Review

Cybersecurity Breaches

Cybersecurity breaches are a fundamental concern to firms in the private sector of an economy.[11] Estimates of the costs associated with such breaches often are discussed in terms of billions of dollars. Most estimates, however, tend to consider only the explicit costs of such breaches (e.g., the costs of detecting and correcting breaches, as well as any actual loss of physical assets). Once the implicit costs (e.g., potential lost sales, potential liabilities) are considered, the actual losses to firms operating in the private sector could be closer to a trillion dollars. Furthermore, once the national security aspects of the critical infrastructure assets owned by private sector firms are factored into the calculation, the costs of cybersecurity breaches in the private sector are impossible to accurately measure. Although determining the exact dollar costs resulting from cybersecurity breaches is problematic, there is little doubt that the number and sophistication of cybersecurity threats and breaches continue to grow (e.g., Ernst & Young, 2013).

One stream of empirical research on the costs of cybersecurity breaches has to do with the impact of such breaches on the stock market returns of firms that are publicly traded on the

[11] Although outside the scope of this paper, cybersecurity breaches are also a fundamental concern to organizations in the public sector, as well as to individuals.

U.S. stock exchanges (Campbell et al., 2003; Hovav and D'arcy, 2003, 2004; Cavusoglu et al., 2004; Acquisti et al., 2006; Ishiguro et al., 2006; Kannan et al., 2007; Gordon et al., 2011). These studies are of particular relevance to the study contained in this paper for the following three reasons. First, as noted in the introduction to this paper, most of the critical infrastructure assets in the U.S. are owned by firms in the private sector, and the majority of these assets are owned by firms that are publicly traded on the U.S. Stock Exchanges.[12] Second, the impact of cybersecurity breaches on stock market returns implicitly considers such factors as potential lost sales and potential liabilities resulting from the breaches. Thus, the implicit, as well as the explicit, costs of cybersecurity breaches are incorporated into these studies.[13] Third, the findings from these studies show that a particular cybersecurity breach could have a significantly negative impact on a firm, despite the fact that a large portion of these breaches does not have such an effect on firms.

A comprehensive study by Gordon et al. (2011) examined the impact of cybersecurity breaches on the stock market returns of firms publicly traded on the U.S. stock exchanges. Their study shows that, although some cybersecurity breaches do indeed have a statistically significant negative effect on firms, there has been a general downward shift in terms of the impact that cybersecurity breaches are having on firms (when measured in terms of the negative effect on the stock market returns of firms). These latter findings suggest, as pointed out by Gordon et al. (2011), that investors are building up a tolerance for cybersecurity breaches and/or that firms are becoming much more adept at detecting and remediating such breaches prior to the point where such breaches cause critical damage to the firms. The above noted findings concerning the downward trend in the general impact of cybersecurity breaches on firms does not, however, negate the fact that devastating breaches can, and actually do, still occur. If anything, the findings by Gordon et al. (2011) serve to highlight why it is so difficult to incentivize private sector firms to make the appropriate level of investments in cybersecurity activities. That is, the downward trend of the impact of cybersecurity breaches on stock market returns of firms in the private sector highlights the difficulties associated with expecting private sector firms to voluntarily incorporate the cost of externalities of such breaches in their decision-making. Furthermore, since the cybersecurity breaches seem to be having a decreasing effect on the stock market returns of firms experiencing the breaches, a real danger is that the tendency by private sector firms to underestimate the private costs associated with cybersecurity breaches will increase.

Cybersecurity Investments

---

[12] President Obama's February 12, 2013 Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity" defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." As noted on the official website of the Department of Homeland Security (http://www.dhs.gov/critical-infrastructure-sectors), critical infrastructure sectors include: the chemical sector, communications sector, energy sector, financial sector, healthcare and public health sector, transportation systems sector, the defense industrial base sector.

[13] There are other streams of empirical research on the impact of cybersecurity breaches. For example, there are surveys conducted by several professional organizations (e.g., Computer Security Institute, 2011, Ernst & Young, 2013, and PwC, 2014). However, these studies generally do not consider the implicit costs of cybersecurity breaches noted above.

Investments on cybersecurity activities are best viewed in a manner similar to the way other investments are considered by an organization. In the private sector, this essentially means that benefits from investments need to be compared to the costs associated with such investments. In terms of accepting or rejecting an incremental cybersecurity investment opportunity, the basic analysis consists of computing the net present value (NPV). The use of cost-benefit analysis for efficiently allocating scarce resources (i.e., making the business case) is well established in the capital investment literature including the literature on investments in cybersecurity (e.g., see Gordon and Loeb, 2006).

The preceding discussion refers to the way a private sector firm might look at an incremental investment related to cybersecurity.[14] Alternatively, if the firm were trying to optimize the total level of investments in cybersecurity activities, then the firm would want to minimize the sum of the costs of the cybersecurity investments plus the costs of the cybersecurity breaches. A rigorous approach to determining the optimal level of cybersecurity investments is provided by the Gordon-Loeb Model (Gordon and Loeb, 2002). Gordon and Loeb (2002), hereafter denoted as the G-L Model, present an economic model to examine the optimal investment level of information security for a risk-neutral firm. The G-L Model shows that, for two broad classes of cybersecurity breach functions, the optimal investment in information security is always less than or equal to 1/e (approximately, 36.79%) of the expected loss from a security breach. Although G-L Model demonstrated this result for only two (broad) classes of security breach functions, they conjectured that the *1/e* rule is more general. Baryshnikov (2012) proved that the G-L Model rule "holds in full generality." LeLarge (2012) also proved the generality of the G-L Model optimal investment rule.

III. Cybersecurity Inputs and Outputs

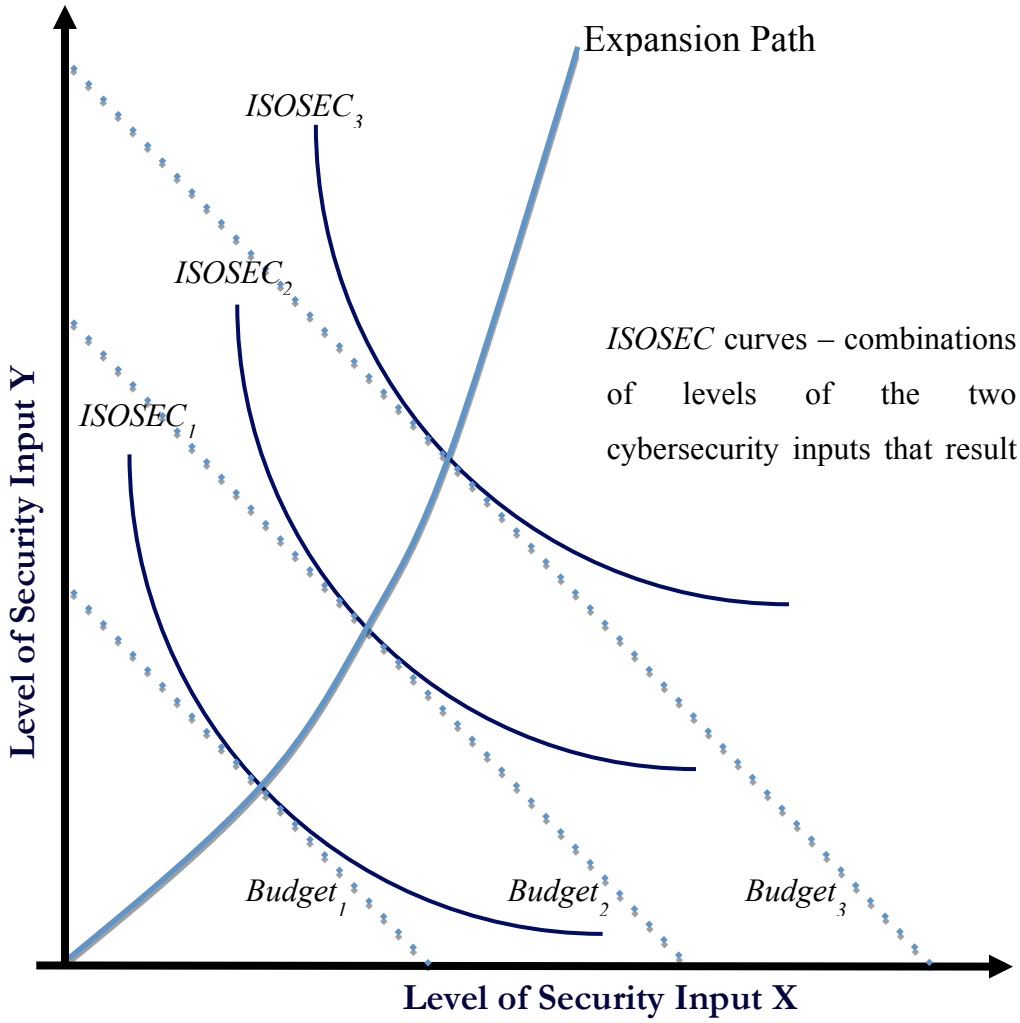
Basic Analysis

As pointed out in Section I, private sector firms will usually underinvest in cybersecurity. Accordingly, it is reasonable for the government to develop incentives/regulations to offset this underinvestment tendency. Ideally, the government would like to provide incentives/regulations to increase cybersecurity investments in private sector firms based on some target level of cybersecurity. Following this logic, the incentives/regulations would be based on the outputs of the firms' inputs (or activities) related to cybersecurity. Under such an approach, the government would let firms decide on the best mix of inputs to use in order to reach the target level of cybersecurity. In reality, however, there is little agreement on how to measure the cybersecurity level of firms. For example, should the number of breaches, or the time it takes to identify and remediate breaches, or the total social costs associated with breaches, be this output measure? Furthermore, even if there were agreement on which metric to use, we are still left with the problem of agreeing on the right way to quantify the metric. As a result of the difficulties associated with defining and measuring the level of cybersecurity, it is common, as well as rational, for the government to consider incentives/regulations based on the inputs to strengthen cybersecurity (e.g., security systems such as intrusion detection/ preventions systems,

[14] Sophisticated models take into consideration such factors as real options (e.g., Dixit and Pindyck, 1994; Gordon et al., 2003; Gordon et al., forthcoming 2015b).

anti-virus software, one time password tokens, improved software, internal control systems,

Figure 1. Cybersecurity Expansion Path



training programs, and security policies and standards).

The relationships between the inputs and outputs of cybersecurity are illustrated in Figure 1. This figure illustrates a case where a firm has three possible levels of cybersecurity represented by the three *ISOSEC* curves *($ISOSEC_3 > ISOSEC_2 > ISOSEC_1$)*. Each *ISOSEC* curve in Figure 1 represents the same level of cybersecurity for different combinations of inputs to cybersecurity. It is assumed, in Figure 1, that the firm has two, and only two, inputs (X and Y) to improve its cybersecurity level. Let x represent the units of input X and let y represent the units of input Y. For simplicity, we assume the measure of X is such that the cost of a unit of X is one dollar and similarly the measure of Y is such that the cost of a unit of Y is one dollar. Thus, one could think of x as the dollar expenditures for input X and y as the dollar expenditures for input Y.

The horizontal axis in Figure 1 measures the amount of one cybersecurity input (e.g., timeliness of patch updating of the firm), denoted as X, for which we assume the government can

get verifiable data. The vertical axis measures the amount of a second cybersecurity input (e.g., software quality) or a composite of all other security inputs, denoted as Y, for which we assume the government cannot attain a verifiable measure. The firm's level of cybersecurity is determined by the level of inputs (x, y). As noted above, each *ISOSEC* curve is the set of all pairs of inputs (x, y) resulting in a given level of cybersecurity, and is assumed to be convex to the origin. The budget, *B*, for expenditures on cybersecurity inputs is the line segment given by the set $\{(x, y)|x \geq 0, y \geq 0, and\ x + y = B\}$. Dotted lines in Figure 1 represents the budget lines for three budget levels, where $B_3 > B_2 > B_1$.

An efficient firm expands its *ex ante* cybersecurity level (i.e., decreases the probability of a cybersecurity breach) by selecting a combination of cybersecurity inputs where the budget line is tangent to an *ISOSEC* curve. The point of tangency is where the marginal benefit (i.e., the marginal increase in the cybersecurity level) of input *X* equals the marginal benefit of input *Y*.[15] At that point, the firm reaches the highest *ISOSEC* for a given budget level. In other words, an efficient firm spends its given budget for cybersecurity activities on the optimal mix of inputs, given the costs of the different outputs. This will map out on the firm's optimal cybersecurity expansion path shown in Figure 1. If a firm were to take into account externalities, this would not change the firm's expansion path.[16]

Now let us look at Figure 2, and assume that the firm initially has a budget for cybersecurity expenditures equal to B_1. If the firm were efficient in its allocation of the cybersecurity budget (B_1) to inputs *X* and *Y* (i.e., the firm knows and uses the optimal mix of *X* and *Y* for a budget level of B_1), it would select the combination of inputs equal to x_1 and y_1. That is, (x_1, y_1) represents the efficient allocation of B_1, in terms of providing the maximum cybersecurity level of $ISOSEC_1$. However, suppose that the government wants to raise the level of cybersecurity achieved by this firm to a target cybersecurity level of $ISOSEC_T$. That is, even if it were assumed that the firm is investing the optimal amount to cover its private costs of cybersecurity breaches, the government could believe the firm is not investing enough to cover the externalities associated with such breaches. Notice that this latter argument is independent of the government's ability to measure the exact level of security.

To raise the firm's cybersecurity level to $ISOSEC_T$, let us assume the government imposes a regulatory constraint on *X* of x_R (recall that the government can get verifiable data on *X*). However, under this scenario we also assume that the firm is not willing (or cannot afford) to raise its budget to B_2. In other words, we assume the firm's budget is fixed at B_1. The firm would solve this constrained optimization problem by setting *X* at the x_R level and setting *Y* at the y_R level shown in Figure 2. As shown in Figure 2, at (x_R, y_R), the cybersecurity level attained would be $ISOSEC_R$, which represents a lower level of cybersecurity than the pre-regulation level of cybersecurity of $ISOSEC_1$. Thus, with the assumption that the firm remains with its initial cybersecurity budget constraint of B_1, the government regulation actually motivates the firm to

---

[15] We have assumed the inputs are measured in a way that one unit of each input cost one dollar. More generally, the point of tangency is where ratio of prices of the cybersecurity inputs equals the marginal rate of technical substitution of the cybersecurity inputs (i.e., the ratio of the marginal benefits of the inputs).

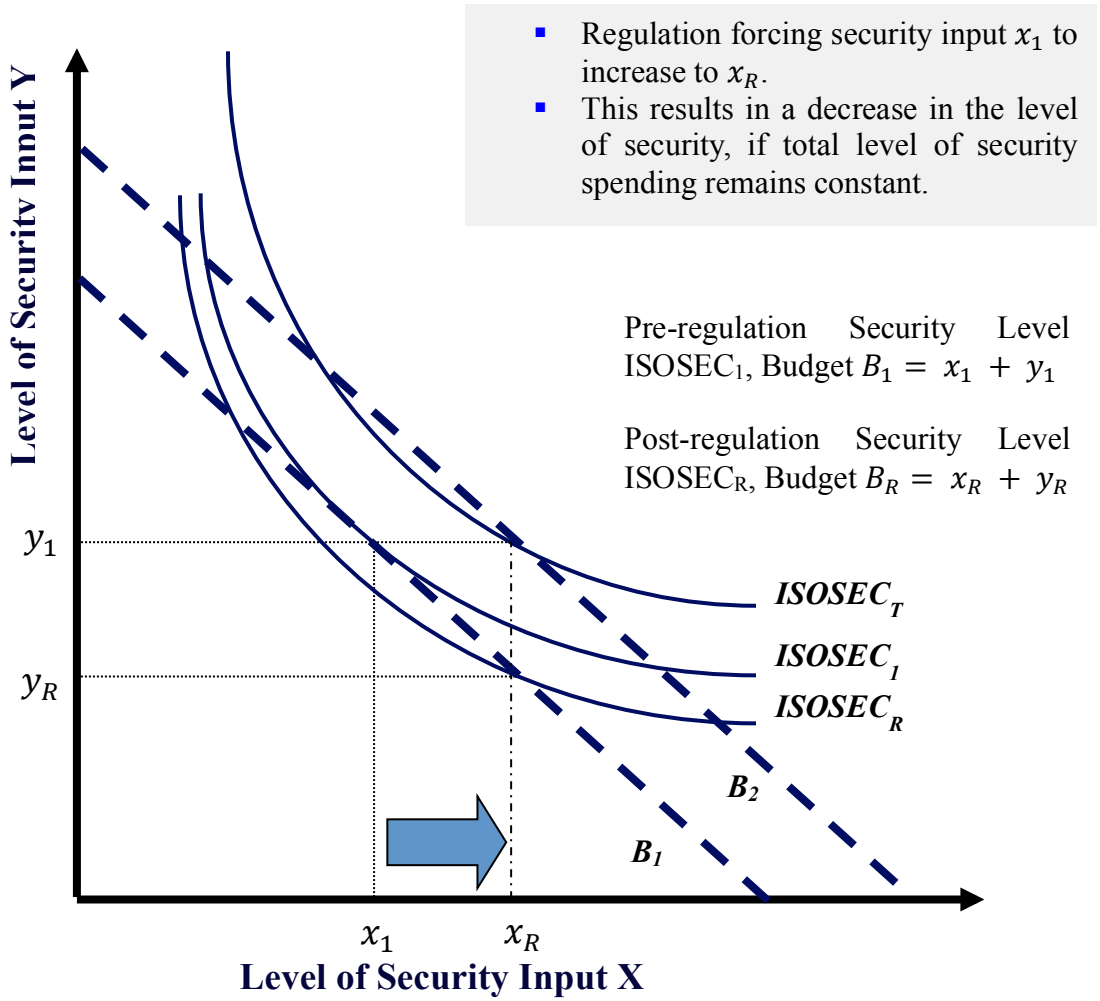
[16] Taking externalities into account, however, would lead the firm to operate at a higher point on the expansion path. This statement is based on the assumption that externalities are only associated with the occurrence of a cybersecurity breach, and implicitly assumes that there are no externalities (e.g., pollution effects) associated with the use of one or more of the inputs (*X* and *Y*).

decrease its level of cybersecurity. In other words, after complying with the regulation on input *X* (i.e., $x \geq x_R$), but not increasing its overall budget for cybersecurity spending (i.e., keeping the budget at B_1), the firm is no longer using its inputs in an efficient manner.

The above analysis illustrates a case where a regulation on an input to cybersecurity lowers the firm's level of cybersecurity. With some minor changes to the analysis, it is easy to illustrate a situation where a regulation on an input to cybersecurity, without any government subsidy, could possibly increase the firm's level of cybersecurity. For example, if the firm were initially allocating its cybersecurity budget of B_1 inefficiently (i.e., the firm does not know the optimal mix of inputs for a given budget level) and spending x_R on *X* and y_R on *Y*, a government regulation that forced the firm to spend y_1 on *Y* could possibly move the firm to spend x_1 on *X* (instead of x_R). In this scenario, the firm's cybersecurity level would move from the $ISOSEC_R$ to the $ISOSEC_1$, given the budget constraint of B_1 (see Figure 2).

Now let us return to the assumption that the firm is able to determine the optimal mix of its cybersecurity inputs. Furthermore, we now assume the firm is willing (and able) to raise its cybersecurity budget to keep its cybersecurity expenditures on *Y* at y_1, after complying with the regulation that the level of input *X* must be at least x_R. At (x_R, y_1), with a budget of B_2, the firm would reach the target cybersecurity level of $ISOSEC_T$ (see Figure 2).

Figure 2. Inappropriate regulatory strategies can cause firms to reduce their overall levels of cybersecurity



Implications

The preceding analysis shows that the potential for government incentives/regulations to increase cybersecurity investments by private sector firms is dependent on the following two fundamental issues: (1) whether or not firms are utilizing the optimal mix of inputs to cybersecurity, and (2) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. Thus, three general implications are apparent from our input-output framework provided above. First, if it were assumed that the total expenditures by firms on cybersecurity activities (i.e. the budget for spending on cybersecurity inputs) are fixed, and that firms are already utilizing the optimal mix of cybersecurity inputs, for different levels of spending on cybersecurity (i.e., firms know the optimal expansion path shown in Figure 1), government incentives/regulations that encourage changes in the resource allocations among cybersecurity inputs would lower the firms' level of cybersecurity.

Second, if it were assumed that the total expenditures by firms on cybersecurity activities (i.e., the budget for spending on cybersecurity inputs) is fixed, but that firms are not able to determine the optimal mix of cybersecurity inputs (i.e., organizations do not know their optimal expansion path shown in Figure 1), government incentives/regulations (e.g., mandatory cybersecurity standards) that encourage changes in resource allocations among cybersecurity inputs could either increase or decrease the level of cybersecurity in firms. In this case, the outcome of such incentives/regulations depends on whether the government could properly identify the source of cybersecurity resource misallocations and, in turn, tailor the regulation on inputs to help rectify the misallocation of resources. If it were assumed that the government could identify the source of cybersecurity resource misallocation, the government incentives/regulations on inputs to cybersecurity could, but not necessarily would, help firms reach a higher level of cybersecurity. The outcome in such a case would depend on whether or not the firm shifted its use of inputs closer to, or further away, from the optimal mix. If the government were not able to identify the aforementioned resource misallocations (which is a more realistic scenario), a more effective approach to having private firms reach a higher level of cybersecurity could be for the government to initiate incentives that would help to educate firms on how to efficiently allocate their resources (e.g., the establishment of training programs that assist firms in applying cost-benefit analysis to cybersecurity activities).

Third, if it were assumed that the cybersecurity budget of an organization is not fixed (i.e., relax the firm's initial budget constraint), government incentives/regulations (e.g., mandatory cybersecurity standards, or tax incentives related to specific cybersecurity inputs) that encourage organizations to increase their cybersecurity investments could increase the cybersecurity level of such organizations. Whether or not the firm knows its optimal mix of inputs, a sufficient condition for an increase in a firm's cybersecurity level is that the incentives/regulations would not cause a lowering of the expenditures on one or more cybersecurity inputs. There exist, however, other sufficient conditions such that even if the regulation on one input results in the lowering of expenditures on other inputs, the overall cybersecurity level would increase. If a lowering of the expenditures on some cybersecurity

inputs were to occur, then the ultimate result on the cybersecurity level of a firm would be dependent on how the input level changes affect the marginal benefits of inputs. [17]

Formal Analysis

The above graphical analysis of the inputs and outputs of cybersecurity, and the discussion of its implications, can be presented in a more formal analysis. Let $S(x, y, v)$ denote the firm's cybersecurity breach function, defined as the probability that an cybersecurity breach occurs, where *x* and *y* are levels of the two cybersecurity inputs *X* and *Y*, and v $(0 < v < 1)$ represents firm's the underlying vulnerability to security breaches, i.e., $v = S(0,0,v)$. Note that the value of the firm's cybersecurity breach function decreases as the firm moves to a higher *ISOSEC* curve (i.e., a decrease in a firm's probability of a cybersecurity breach occurring translates into an increase in the firm's level of cybersecurity). Consistent with Figure 2, we assume that increases in investments in security inputs *X* and *Y* would decrease the probability of cybersecurity breach (*S*) occurring at a decreasing rate, i.e., we assume:

$$S_x = \frac{\partial S(x,y,v)}{\partial x} < 0, \qquad [1]$$

$$S_y = \frac{\partial S(x,y,v)}{\partial y} < 0, \qquad [2]$$

$$S_{xx} = \frac{\partial^2 S(x,y,v)}{\partial x^2} > 0, \qquad [3]$$

$$S_{yy} = \frac{\partial^2 S(x,y,v)}{\partial y^2} > 0. \qquad [4]$$

If a security breach actually occurs, the firm will suffer a private monetary loss *L* and other firms, organizations, and individuals will suffer the externality loss denoted L^E.

Assume the firm is able to determine the optimal mix of cybersecurity inputs (taking into account only its private costs, *L*. When making security investment decisions in the absence of regulation (and considering only private costs), the firm would choose cybersecurity expenditure levels of *X* and *Y* so that its total expected net benefits from the expenditures (i.e., the reduction in the expected private loss from a cybersecurity breach less the costs of the cybersecurity expenditures) is maximized. Letting (x_1, y_1) denote the firm's optimal levels of cybersecurity inputs in the absence of regulation, we have (x_1, y_1) as the solution to the firm's maximization problem[18]:

$$\max_{x,y}[v - S(x, y, v)]\, L - x - y$$

[17] If the actual level of an organization's cybersecurity (i.e., the output of cybersecurity input activities) could be unambiguously measured, then regulation on outputs would likely be the most effective means of addressing externalities.

[18] This optimization assumes that the firm's cost-benefit analysis ignores the costs of externalities. Thus, what is referred to as the firm's optimal level is the firm's (private costs) optimal level, not the social welfare optimal.

Denote $S_1 = S(x_1, y_1, v)$, so that, S_1 represents the optimal cybersecurity level that is obtained in the absence of regulation. In the presence of externalities (i.e., $L^E > 0$), however, the firm's level of cybersecurity, S_1, is below the socially optimal level.[19] We denote the firm's total level of cybersecurity expenditures in the unregulated case as B_1, where $B_1 = x_1 + y_1$.

Suppose the government wishes to have the firm move to a higher cybersecurity level. If the government (i.e., regulator) could measure and verify the level of both cybersecurity inputs (x and y), the government could mandate that higher level of cybersecurity expenditures by imposing large penalties for firms failing to do so. Recall, however, that the government can get verifiable data only on cybersecurity input X. Hence, the government can only require the firm to increase expenditures on input X, and must let the firm decide on the level of cybersecurity input Y. In the following analysis, we will examine the cybersecurity levels under such a government regulation under three different scenarios.

Scenario 1: The firm is able to determine the optimal mix, but is not willing (or able) to increase the total expenditures on cybersecurity inputs (i.e., the cybersecurity budget is fixed at the current level).

For this scenario, the government requires the firm to spend at least x_R on input X, where x_R is greater than the initial unregulated level, x_1 and the firm is assumed to have to choose inputs levels (x^*, y_R) such $x^* + y_R = B_1$ (i.e., the total cybersecurity expenditures remain at the unregulated optimal amount). Formally stated, (x^*, y_R) solves the firm's following maximization problem:

$$\max_{x,y} [v - S(x, y, v)]\, L - x - y$$

$$s.t. \quad x + y = B_1$$

$$x \geq x_R$$

Denote $S_R = S(x^*, y_R, v)$ as the obtained probability that a cybersecurity breach occurs. Our first proposition compares the post-regulation cybersecurity level S_R with the pre-regulation cybersecurity level S_1 and follows directly from the definitions assumptions. A formal proof is presented in Appendix A.

[19] See Gordon et al. (forthcoming, 2015a) for an analysis of the magnitude of a firm's underinvestment caused by ignoring the costs of externalities.

Proposition 1 *Assume the firm is already determining the optimal mix of cybersecurity inputs* (x_1, y_1)*, and will not change its cybersecurity budget* B_1*. Under a regulation that mandates more expenditures on only cybersecurity activity X (*$x \geq x_R > x_1$*), the firm would choose to strictly obey the regulation, but decrease expenditures on activity Y and end up with a higher probability of a cybersecurity breach (recall that a higher probability of a cybersecurity breach occurring results in a lower level of cybersecurity), i.e.,*

$$x^* = x_R > x_1,$$

$$y_R < y_1,$$

and

$$S_R > S_1.$$

<u>Scenario 2</u>: The firm is not able to determine the optimal mix, and the cybersecurity budget is fixed (i.e., the firm is not willing or able to increase its expenditures on cybersecurity inputs).

For this scenario, assume before the regulation takes place, the firm's cybersecurity inputs are (x_0, y_0), which differ from (x_1, y_1), but are subject to the same budget constraint B_1 (i. e., $x_0 + y_0 = B_1$). Suppose the regulator mandates that the firm must increase the cybersecurity expenditures on activity *X* to at least $x_R > x_0$, and the firm chooses to strictly obey the regulation and keep its current budget level the same. Hence, the firm will pick the post regulation input mix as $(x = x_R, y = B_1 - x_R)$. Note that by defining $y_R = B_1 - x_R$, the firm's post regulation input mix would be represented by (x_R, y_R).

The following proposition (a formal proof of which appears in Appendix A) states the intuitive result that when the firm is not able to determine the optimal input mix, a regulation that motivates more efficient resource allocation would induce a lower probability of a cybersecurity breach (i.e., a higher cybersecurity level) without imposing higher total cybersecurity budget:

Proposition 2 *Assume the firm's current cybersecurity input mix* (x_0, y_0) *is different from the optimal mix* (x_1, y_1) *but under the same budget constraint* B_1*. A regulation that requires higher expenditures on x* $(x \geq x_R > x_0)$ *would decrease the firm's probability of a cybersecurity breach (i.e., increase the firm's cybersecurity level) if it moves the input mix towards the optimal mix, and increase the firm's probability of a cybersecurity breach (i.e., decrease the firm's cybersecurity level) if it moves the input mix away from the optimal mix.*

<u>Scenario 3A:</u> The firm may or may not be able to determine the optimal input mix, but responds to the government regulation on a single cybersecurity input without lowering expenditures on other inputs. (Thus, the firm is willing and able to increase it cybersecurity budget).

For this scenario, assume prior to the introduction of the government regulation, the firm's cybersecurity inputs are (x_P, y_P), which may, or may not, differ from the optimal unregulated input mix (x_1, y_1). Let (x_A, y_A) be the firm's input mix, after the regulation. The

government regulation requires the firm to spend at least $x_R > x_P$ on X, so that regulation can be stated as $x_A \geq x_R > x_P$. For this scenario, the firm's cybersecurity level will increase, as will the firm's budget tor cybersecurity inputs. This observation in stated formally in the next proposition and the (straightforward) proof appears in the Appendix A.

Proposition 3 *Assume the firm's current cybersecurity input mix* (x_P, y_p) *and the firm meets the government regulation that* $x_A \geq x_R > x_P$ *without decreasing its expenditures on input Y. Then the firm's cybersecurity level will increase (i.e., the firm's probability of a cybersecurity breach will decrease) and the firm's budget for cybersecurity inputs will also increase.*

<u>Scenario 3B:</u> The firm is able to determine the optimal mix, and is willing (and able) to increase its cybersecurity budget so as to accommodate the government regulation.

We now move to the case where the firm is able to determine the optimal cybersecurity input mix and is willing and able to increase its cybersecurity budget in light of the government regulatory requirement. Note that in this scenario, we have removed the restriction that other cybersecurity inputs will not be lowered.

Before the regulation takes effect, the firm was at its unregulated optimal input mix (x_1, y_1). The regulation begins and mandates the firm to increase its cybersecurity expenditures on input *X* to at least $x_R > x_1$. Denote $(\hat{x}, \hat{y})$ as the firm's optimal levels of cybersecurity inputs under regulation, i.e., $(\hat{x}, \hat{y})$ solves the firm's following optimization problem:

$$\max_{x,y} [v - S(x, y, v)]\, L - x - y$$

$$s.t.\ x \geq x_R,$$

where $x_R > x_1$.

Denote $\hat{S} = S(\hat{x}, \hat{y}, v)$ (i.e., $\hat{S}$ represents the probability that a cybersecurity breach occurs under regulation) and define $\hat{B} = \hat{x} + \hat{y}$ as the total level of cybersecurity expenditures for the regulated case. The constraint $x \geq x_R$ must be binding. [20] Hence we have $\hat{x} = x_R$.

In the next two propositions, we provide two sufficient conditions for the government regulation to result in a decrease in the probability of a cybersecurity breach. The first sufficient condition is that the cybersecurity inputs *X* and *Y* are weakly complementary over the interval $[x_1, x_R]$, in the sense that an increase in *x* will not decrease the marginal benefit of an increase in *y*.[21] Formally, we assume $S_{xy} = \frac{\partial^2 S(x,y,v)}{\partial x \partial y} \leq 0$.

[20] This can be shown by first assuming that $\hat{x} > x_R$. This means that $(\hat{x}, \hat{y})$ is a solution to $\max_{x,y} [v - S(x, y, v)]\, L - x - y$ without the constraint, i.e., $(\hat{x}, \hat{y}) = (x_1, y_1)$, which contradicts the assumption that to $\hat{x} > x_R > x_1$. Hence, $x \geq x_R$ is a binding constraint.

[21] Our use of the term weakly complementary is in the spirit of the discussion on production inputs in Ferguson 1969, p.71.

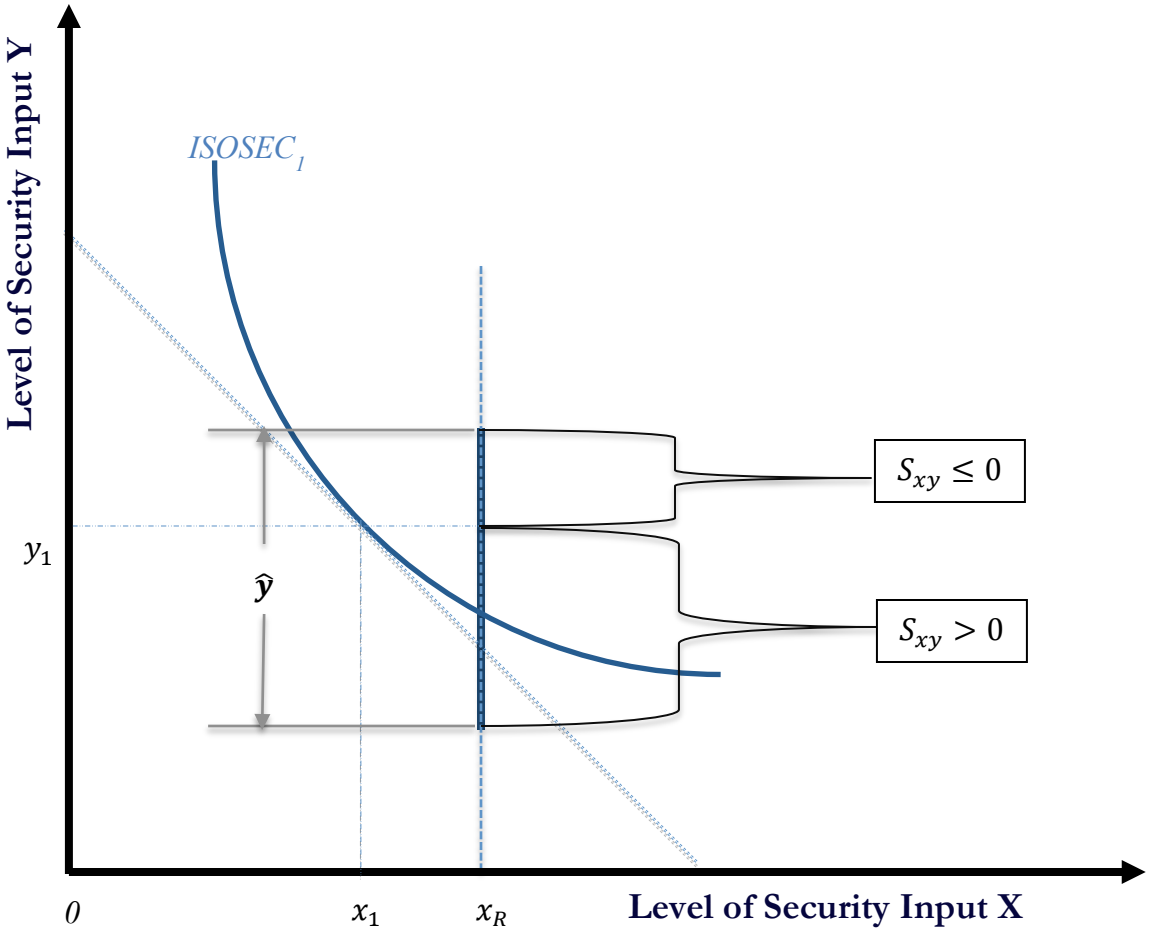
Proposition 4 *If the firm is able to determine the optimal input mix and adjust the cybersecurity expenditure budget and if X and Y are weakly complementary inputs over interval* $[x_1, x_R]$*, then the regulation would result in a lower probability of a cybersecurity breach occurring (i.e., when* $S_{xy} \leq 0$*, we have* $S(\hat{x}, \hat{y}, v) < S(x_1, y_1, v)$*). In addition,* $\hat{x} + \hat{y} > x_1 + y_1$ *(i.e., it is optimal for the firm to increase it cybersecurity budget).* (See Appendix A for the formal proof.)

We now examine the case where *X* and *Y* are not weakly complementary inputs. In that case, $S_{xy} > 0$, and the inputs are said to be *competitive* in the sense that the marginal benefit of input *Y* declines when the input *X* increases. In this case, whether the regulation would induce a lower probability of a cybersecurity breach occurring is ambiguous. The firm is mandated to spend more on input *X*, but would at the same time reduce expenditures on input *Y*,[22] since the marginal benefit from input *Y* is now smaller. As a result, the decrease in the probability of a cybersecurity breach occurring from more spending on input *X* could be partly or even more than offset by the increase in the probability of a breach occurring due to less spending on input *Y*.

Figure 3 illustrates how the optimal post-regulation expenditures $\hat{y}$ varies as the sign of S_{xy} changes. Since $\hat{x} > x_R$ is binding, the optimal post-regulation input mix is always on the vertical solid line at $\hat{x} = x_R$. Comparing with the pre-regulation expenditures on input *Y*, the firm will invest more $\hat{y}$ if $S_{xy} < 0$, invest the same if $S_{xy} = 0$, and invest less if $S_{xy} > 0$. Note that the optimal post-regulation input mix could be either above or below the pre-regulation cybersecurity *ISOSEC* curve.

[22] This can be proved in a similar fashion as Proposition 4.

Figure 3. Optimal Post-Regulation Expenditures on Input *Y*



In our next proposition, the formal proof of which appears in Appendix A, we provide another sufficient condition for the post-regulation probability of a cybersecurity breach occurring to be lower than the pre-regulation probability. The following sufficient condition restates how the optimal *y* changes with changes in *x*.

Proposition 5 *If* $-\frac{s_x}{s_y} < -\frac{s_{xy}}{s_{yy}}$ *over interval* $[x_1, x_R]$, *it follows that*

$$S(\hat{x}, \hat{y}, v) < S(x_1, y_1, v).$$

Figures 4 and 5 summarize our analysis for Scenario 3B, i.e., when the firm is able to determine the optimal input mix and optimally adjusts the cybersecurity expenditure budget in

response to the regulation. A regulation that increases expenditure on activity *X* from x_1 to at least x_R would induce the firm to strictly obey the regulation and set $\hat{x} = x_R$. The post regulation input *Y*, however, may move along the vertical line at $x = x_R$. In Figure 4, the solid vertical line at $\hat{x} = x_R$ represents the region where the regulation will lower the probability of a cybersecurity breach (i.e., increase the cybersecurity level). Any breach probability functions that satisfy our sufficient condition $-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$ would have post-regulation input mix falling into this region.

When *X* and *Y* are weakly complementary inputs, the firm would choose not to decrease input *Y* and the total cybersecurity level would increase. When *X* and *Y* are competitive inputs, the firm would decrease expenditures on input *Y*, but as long as the condition $-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$ holds, the post-regulation cybersecurity level would still be higher. In Figure 5, we combine Figure 3 and 4 to highlight that there is a region where the post-regulation *y* decreases and the probability of a cybersecurity breach also decreases (i.e., we have a higher cybersecurity level). In other words, a regulation may be able to lower the probability of a cybersecurity breach, even though the regulation results in a lowering of other inputs (i.e., input *Y*).

To provide the readers with examples, we consider a generalized version of the two single cybersecurity input breach functions discussed in Gordon and Loeb (2002). These functions are $S^I(x, y, v) = \frac{v}{(\alpha_1 x+1)^{\beta_1}(\alpha_2 y+1)^{\beta_2}}$ for some $\alpha_1, \alpha_2 > 0, \beta_1, \beta_2 \geq 1$, *and* $S^{II}(x, y, v) = v^{(\alpha_1 x+1)(\alpha_2 y+1)}$ for some $\alpha_1, \alpha_2 > 0$.[23] In Appendix A, a straightforward proof is given to show that these functions satisfy Proposition 5. That is, for these generalized functions, the post-regulation optimal expenditures on input *Y* decreases, but the probability of cybersecurity breach decreases.

[23] They include broad classes of functions widely used in economics literature. It can be easily verified that they satisfy conditions [1], [2], [3], [4].

Figure 4. Region for Higher Post-Regulation Cybersecurity Level

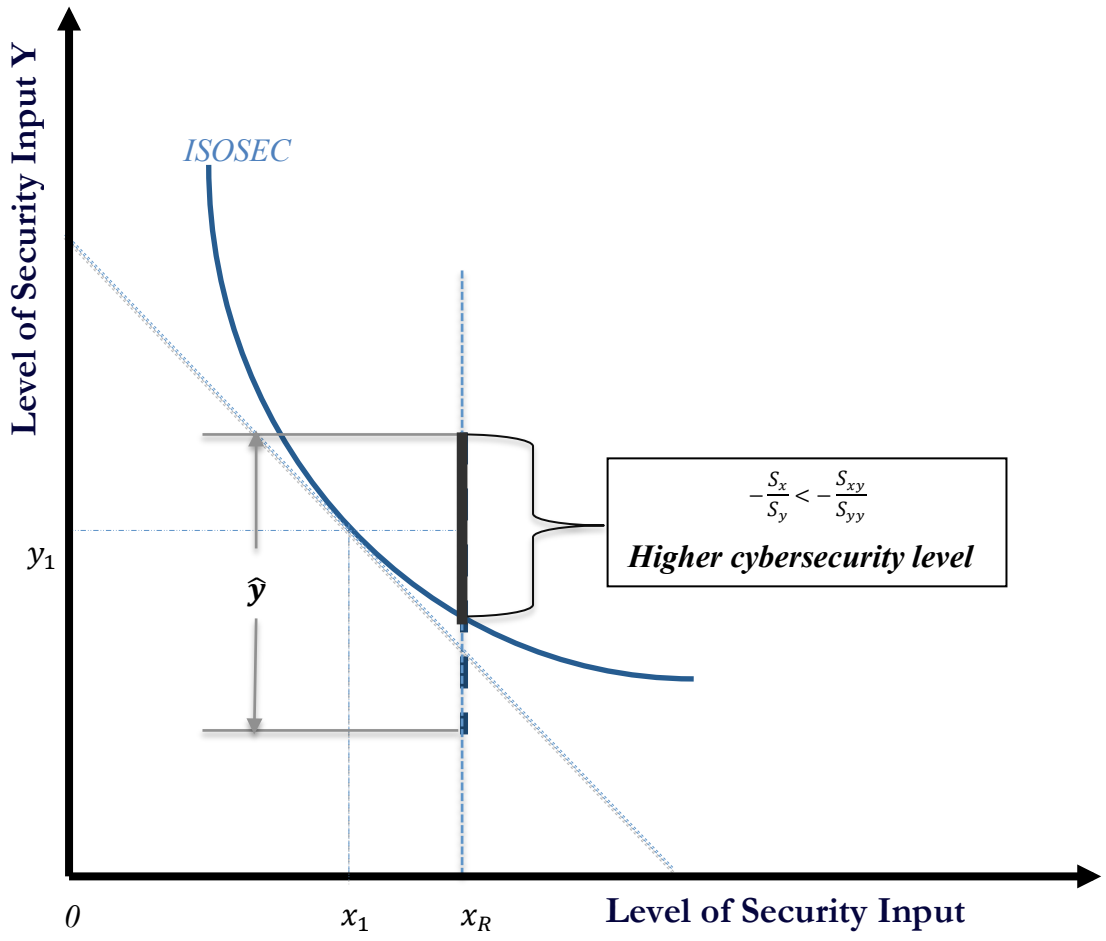


Figure 5. Region Where the Optimal Post-Regulation Expenditures on Input *Y* Decreases and Cybersecurity Level Increases

IV. Existing Government Actions Affecting Cybersecurity Investments

Although there is as an *a priori* argument that firms will likely underinvest in cybersecurity activities, the government has already taken several actions that either have, or have the potential to, significantly offset the tendency by firms to underinvest in cybersecurity. Given the conditional impact of government incentives/regulations on cybersecurity investments by private sector firms, it is strongly recommended that the existing actions be recognized, evaluated, and more effectively utilized before, or at least in conjunction with, considering new government incentives/regulations concerning cybersecurity investments. Two such actions of particular note are the Sarbanes-Oxley Act of 2002 and the 2011 SEC Disclosure Guidance on Cybersecurity Risks and Cyber Incidents.[24]

Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) of 2002 requires firms to have strong internal control systems in place, where internal control systems are defined in terms of reliable financial reports (see Sections 302 and 404 of SOX). In a modern computer-based information system environment, firms cannot produce reliable financial reports results without having secure computer systems. For accelerated filers, SOX (Section 404) requires external auditors to attest to the quality, or lack thereof, of the firm's internal controls of their financial information reporting systems.[25] As indicated in various empirical studies, one category of material weaknesses (MW) in internal control systems identified by managers and auditors has to do with the security of computer based information systems (e.g., Li et al., 2012). More generally, it has been shown that MW in internal control systems have a negative impact on the cost of equity of firms (Asbaugh-Skaife et al., 2009; Gordon and Wilford, 2012).

Presumably, the SOX reporting requirements have been accompanied by an increase in cybersecurity investments. Unfortunately, since firms in the private sector do not disclose the level of expenditures on cybersecurity activities as a separate category on their financial reports filed with the SEC, the presumption about the passage of SOX having a positive impact on the cybersecurity investments of firms has never been verified. Furthermore, since SOX only applies to financial reporting systems[26], its ability to motivate firms to make the appropriate level of cybersecurity investments is limited. The above notwithstanding, the fact that firms are required to report their MW in their 10-K reports filed with the SEC (which include MW related to the security of their computer-based information systems) leads us to conjecture that SOX has motivated corporate executives to increase their expenditures on cybersecurity activities relative to what they would be without SOX. Gordon et al. (2006) provide evidence that is consistent with this conjecture. They show that firms listed on the U.S. Stock Exchanges have significantly

[24] Although these actions pertained only to publicly traded firms, such firms include virtually all of the firms that own an element of the nation's critical infrastructure.
[25] SOX, as modified by the Dodd-Frank Act of 2010, requires only accelerated firms to have external auditors attest to the quality of internal controls. Generally speaking, accelerator firms are large firms, with revenues over $75 million per year (see Gao et al., 2009).
[26] With the increasing use of integrated enterprise systems, an increasing percentage of a firm's IT systems affect the financial reporting systems of firms.

increased their voluntary disclosures of cybersecurity related activities. The fact that these voluntary disclosures are associated with a statistically significant increase in the stock market returns of the disclosing firms (see Gordon et al., 2010) provides additional support for this conjecture.

In our opinion, the potential of SOX to offset the tendency to underinvest in cybersecurity activities by private sector firms has been substantially underutilized by the government. Indeed, to our knowledge this is the first paper to point out the direct link between the financial reporting of MW in IT security and a cybersecurity framework for government incentives related to cybersecurity.

SEC Disclosure Guidance

The SEC Disclosure Guidance on Cybersecurity Risks and Cyber incidences (SEC, 2011) is another government action that is particularly germane to the issue of cybersecurity investments by private sector firms.[27] Unlike SOX, which is focused on the inputs to cybersecurity via its emphasis on computer-based information systems, the SEC Disclosure Guidance focuses on the cybersecurity output in terms of cybersecurity risks and incidents. As stated in the SEC Disclosure Guidance:

> Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition (SEC 2011).

Many firms have reacted to the SEC Disclosure Guidance with an extensive discussion of the cybersecurity risks facing their firms in Item1A of their 10K Annual Reports filed with the SEC. In Appendix B, we present the Risk Factors reported by Lockheed Martin in their 10-K for 2013 as a representative example of a rapidly growing trend by firms to voluntarily report information concerning cybersecurity activities on the 10-K reports. In fact, since the SEC's Disclosure Guidance was published in 2011, one is hard pressed to find a major corporation that does not voluntarily report some sort of information concerning its cybersecurity activities. This trend notwithstanding, we are still only able to conjecture that the increased reporting of cybersecurity related activities are accompanied by an increase in cybersecurity investments. In other words, while it seems reasonable to assume that corporate executives are increasing their level of investments in cybersecurity related activities as a result of the SEC Disclosure Guidance, hard evidence supporting this conjecture does not currently exist.[28] In fact, there have been calls for changing the SEC's Disclosure Guidance on cybersecurity risks and incidences to a more formal regulation that requires firms to disclose more detailed information than currently

[27] Although the SEC Disclosure Guidance related to cybersecurity is technically speaking not a binding requirement, the fact that the disclosure is voluntary will provide a poor defense in the event of a suit by investors.

[28] As noted earlier in the paper, there is scant information on the actual level of investments in cybersecurity activities by firms. The information that does exist is based largely on survey data which is of questionable reliability due to such problems as non-response bias, difficulty in verifying the actual respondent, and difficulty in verifying the amounts reported. Thus, it is difficult, if not impossible, to prove or disprove the accuracy of this statement.

is taking place. A leading advocate of this latter position is Senator Rockefeller. In a letter to the SEC Chairperson (Ms. Mary Jo White) on April 9, 2013, Senator Rockefeller wrote:

> In October 2011, the SEC responded to my request and announced that it was issuing staff guidance on disclosure obligations regarding cybersecurity risks and cyber incidents. I applauded this decision as an important first step in the right direction, and it certainly made a positive impact on disclosures. However, given the growing significance of cybersecurity on investors' and stockholders' decisions, the SEC should elevate this guidance and issue it at the Commission level. While the staff guidance has had a positive impact on the information available to investors on these matters, the disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices.[29]

We agree with the underlying concern raised by Senator Rockefeller in his letter to the Chairperson of the SEC. The "true costs and benefits of companies' cybersecurity practices" have not been identified as a result of the 2011 SEC Disclosure Guidance on Cybersecurity Risks and Cyber Incidences. However, there are steps that the government could take to improve this situation, and in turn potentially improve the level of cybersecurity investments by private sector firms, even without raising the guidance to a Commission level issue. For example, the government (e.g., the SEC) could examine the correlation between the disclosures (or lack thereof) currently taking place and cybersecurity breaches in private sector firms. A study of this sort would create a form of market discipline that could (and likely would) result in increased investments in cybersecurity activities so as to prevent cyber incidences. Of course, if the market discipline turns out to be insufficient, then changing the disclosure guidance to a formal regulation could be a future action by the SEC. If the SEC were to follow Senator Rockefeller's recommendation, our suggestion is that the annual level of cybersecurity expenditures by firms be included in the additional information to be disclosed. In our opinion, disclosing information on the level of capital expenditures would go a long way toward putting market pressure on firms to increase their cybersecurity budget because it would signal to investors, creditors and customers the importance the firms attach to cybersecurity.[30] In addition, if firms were required to disclose their annual cybersecurity expenditures, it would allow the government to more effectively develop incentives/regulations that are designed to increase the budget for cybersecurity activities.

Other Examples of Government Actions Affecting Cybersecurity Investments

Besides SOX and the SEC Disclosure Guidance, there are many industry specific government regulations that are likely to offset the tendency by private sector firms to under-invest in cybersecurity activities. Two such regulations that have presumably had a significant effect on increasing cybersecurity investments in private sector firms are the Gramm-Leach Bliley Act (GLB) of 1999 and the Health Insurance Portability and Accountability Act (HIPAA)

---

[29] See: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51/.

[30] Alternatively, an increase in a firm's annual spending on cybersecurity activities could be interpreted as a signal that the firm is having problems in this area. Thus, not surprisingly, firms have been reluctant to reveal this information.

of 1996. GLB and HIPAA impose stringent privacy and information security rules on financial institutions and health providers, respectively. As a result, both of these Acts provide strong incentives for firms in the private sector to increase their investments in cybersecurity activities. (Harvey and White, 2002). Presumably, the firms affected by these laws are investing enough in cybersecurity to cover the private costs and at least some of the externalities resulting from cybersecurity breaches. Anecdotal evidence provided to the authors, by a variety of firms in both of these industries, confirms this presumption. Unfortunately, we have no way of knowing if this anecdotal evidence is generalizable because private sector firms do not provide public information on the actual expenditure level of investments in cybersecurity activities. However, the significant penalties associated with non-compliance to these Acts suggest that this evidence about increased cybersecurity investments is likely to be true.

The above noted industry-specific regulations only apply to two specific sectors of the nation's critical infrastructure. There are other regulations that apply to a specific subset of firms or sectors. For example, in 2003 California enacted the Notice of Security Breach Act which requires that any company that maintains personal information of California citizens and has a security breach threating the confidentiality of that information must disclose the details of the event.[31] However, unless government agencies were to come up with regulations for each and every sector of the critical infrastructure (a very unlikely scenario), general incentives/ regulations to encourage firms to make the appropriate level of cybersecurity investments are required. The reporting of MW under SOX, and the SEC's guideline on cybersecurity risks and cyber incidences, represent two examples of the types of general incentives/regulations that can help accomplish the goal of increasing cybersecurity investments among a broad array of private sector firms that own U.S. critical infrastructure assets.

V. Concluding Comments

President Obama has recognized the importance of cybersecurity to the U.S. national security (e.g., Obama, 2013). Recognizing the importance of cybersecurity is a necessary first step in resolving the challenges associated with cybersecurity risks and incidents. The next step, however, is to find solutions to these challenges. One such challenge, which has been the focus of this paper, has to do with the tendency by firms in the private sector to underinvest in cybersecurity. Thus, it is appropriate for governments to consider the use of incentives and regulations to offset this tendency. Based on an input-output analysis, this paper has examined the conditions under which incentives/regulations are likely to be most effective in encouraging a more appropriate level of cybersecurity investments by private sector firms.

Two examples of existing U.S. federal government actions affecting cybersecurity investments were also discussed in this paper. These examples are the Sarbanes-Oxley Act of 2002 and the 2011 SEC Disclosure Guidance on Cybersecurity Risks and Incidents. As pointed out in this discussion, the government would be wise to examine existing incentives/regulations before, or at least in conjunction with, initiating new ones. In particular, we believe that even as other incentives/regulations are being considered, a more effective utilization of SOX and the

[31] See the following website: http://oag.ca.gov/ecrime/databreach/reporting.

SEC Disclosure Guidance could go a long way toward resolving the problem associated with underinvestment in cybersecurity activities by a large subset of private sector firms.

It should be noted that private sector firms do not make cybersecurity investments in isolation of other firm-related investment decisions (e.g., new product investments). A limitation of this paper is that we did not consider these other investment decisions in our discussion. In other words, cybersecurity investments need to compete for scarce organizational resources. Thus, no matter how carefully one tries to analyze the impact of government regulations and/or incentives related to cybersecurity investments on private sector firms, the ultimate impact will be determined by a variety of interactive concerns, many of which are unrelated to cybersecurity issues. Accordingly, it is important to monitor the derivative effect of any incentive/regulations directed at improving cybersecurity investments by private sector firms. An important component of such monitoring is the gathering of data on the level of investments in cybersecurity activities by private sector firms visa vie other firm-level investments (e.g., capital investments unrelated to cybersecurity). Unfortunately, at the present time, reliable empirical data on the actual level of cybersecurity investments is unavailable. Thus, one recommendation suggested in this paper is for the U.S. federal government to consider the development of a national database that tracks cybersecurity investments by private sector firms. A database on the level of investments in cybersecurity activities (and their effectiveness) by private sector firms could be maintained by a government agency and/or a research center within a university. The mere collection of such data could (and most likely would) serve to provide an incentive, via the marketplace, for firms to invest more into cybersecurity related activities.

A second recommendation suggested in this paper revolves around the need for firms to determine the optimal mix of their cybersecurity inputs. Whether increasing their cybersecurity budget or keeping it fixed, it is important for firms to understand the process by which they can derive the most efficient allocation of their cybersecurity related resources. To facilitate improved resource allocation decisions among firms, the government could establish a training program on cost-benefit analysis applied to cybersecurity expenditures. This program could be established in conjunction with a university and open to all firms, either at no cost or at a minimal cost to firms. That is, the government could essentially provide a subsidy by covering all, or some part, of the costs associated with the training program as an incentive for firms to increase their cybersecurity level via a more efficient allocation of their cybersecurity resources.

VI. Funding

This work was supported by 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

Acquisti, A., A. Friedman and R. Telang, "Is there a cost to privacy breaches? An event study," in: *Workshop on the Economics of Information Security*, Cambridge, UK, (2006), available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.2942&rep=rep1&type=pdf.

Anderson, Ross. "Why information security is hard-an economic perspective." In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pp. 358-365. IEEE, (2001).

Anderson, Ross, and Tyler Moore. "The economics of information security." *Science* 314, no. 5799 (2006): 610-613.

Ashbaugh-Skaife, Hollis, Daniel W. Collins, and Ryan Lafond. "The effect of SOX internal control deficiencies on firm risk and cost of equity." *Journal of Accounting Research* 47, no. 1 (2009): 1-43.

Baryshnikov, Y., "IT security investment and Gordon-Loeb's 1/e rule," in: *Workshop on Economics and Information Security*, Berlin, German (2012), available at: http://weis2012. econinfosec.org/papers.

Campbell, K., L.A. Gordon, M.P. Loeb and L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security 11, no. 3 (2003): 431-448.

Cavusoglu, H., B. Mishra and S. Raghunathan, "The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers," *International Journal of Electronic Commerce* 9 (2004): 69–104.

Computer Security Institute, "2010/2011 Computer crime and security survey," (2011), available at: http://www.ncxgroup.com/wp-content/uploads/2012/02/CSIsurvey2010.pdf

Dixit, A. K. and R. S. Pindyck, Investment under uncertainty. Princeton University Press, (1994).

Ernst & Young, "Under cyber-attack, EY's global information security survey 2013," (2013), available at http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_ Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf.

Ferguson, C. E., The neoclassical theory of production and distribution, Cambridge University Press, (1969).

Gao, F., J.S. Wu, and J. Zimmerman, "Unintended consequences of granting small firms exemptions from securities regulation: evidence from the Sarbanes-Oxley Act," *Journal of Accounting Research* 47, no. 2 (2009): 459-506.

Gordon, L.A. and M.P. Loeb, "The economics of information security investment," *ACM Transactions on Information System Security* 5, no. 4 (2002): 438-457.

Gordon, L.A. and M.P. Loeb, Managing cybersecurity resources: a cost-benefit analysis, McGraw-Hill, New York, (2006).

Gordon, L.A., M.P. Loeb, and W. Lucyshyn. "Information security expenditures and real options: a wait-and-see approach," *Computer Security Journal* 19, no. 2 (2003): 1-7.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and T. Sohail. "The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities," *Journal of Accounting and Public Policy* 25, no. 5 (2006): 503-530.

Gordon, L.A., M.P. Loeb and T. Sohail, "Market value of voluntary disclosures concerning information security," *MIS Quarterly* 34, no. 3 (2010): 567-594.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model" *Journal of Information Security*, (forthcoming 2015a).

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, "The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective, *Journal of Accounting and Public Policy*, (forthcoming 2015b).

Gordon, L.A., M.P. Loeb and L. Zhou, "The impact of information security breaches: has there been a downward shift in cost?" *Journal of Computer Security* 19, no. 1 (2011): 33-56.

Gordon, L.A. and A. Wilford, "An analysis of multiple consecutive years of material weaknesses in internal control," *The Accounting Review* 87, no. 6 (2012): 2027-2060.

Gramm-Leach-Bliley Act, 1999, Public Law 106-102, see: http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/html/PLAW-106publ102.htm.

Harvey, D.W. and A. White, "The impact of computer security regulation on American companies," *Texas Weslyan Law Review*, (2001-2002): 505-528.

Health Insurance Portability and Accountability Act Of 1996, Public Law 104-191, see: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

Hovav, A. and J. D'arcy, "The impact of denial-of-service attack announcements on the market value of firm," *Risk Management and Insurance Review* 6 (2003): 97–121.

Hovav, A. and J. D'arcy, "The impact of virus attack announcements on the market value of firms," *Information Security Journal: A Global Perspective* 13 (2004): 32–40.

Information Technology Industry Council. "ITI recommendation: Steps to facilitate more effective information sharing to improve cybersecurity," October 2011, available at: http://www.itic.org/dotAsset/8be757cb-88e8-48ce-86a9-0d365db9d016.pdf.

Ishiguro, M., H. Tanaka, K. Matsuura and I. Murase, "The effect of information security incidents on corporate values in the Japanese stock market," in: *Workshop on the Economics of Securing the Information Infrastructure*, Arlington, VA, 2006, available at: http://www.mri. co.jp/PUBLICITY/PAPER/2006/20061023_si304.pdf.

Kannan, A., J. Rees and S. Sridhar, "Market reactions to information security breach announcements: an empirical analysis," *International Journal of Electronic Commerce* 12 (2007): 69–91.

LeLarge, M., "Coordination in network security games: a monotone comparative statics approach," *IEEE Journal on Selected Areas in Communications* 30, no. 11 (2012): 2210-2219.

Li, C., G.F. Peters, V.J. Richardson, and M.W. Watson. "The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports." *MIS Quarterly* 36, no. 1 (2012): 179-204.

Obama, B., The White House, Presidential Executive Order 13636, "Improving critical infrastructure cybersecurity," February 12, 2013, see: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity).

PWC, "The global state of information security survey 2014," (2014), available at: https://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.

Pym, David, Joe Swierzbinski, and Julian Williams. "The need for public policy interventions in information security." *Manuscript at http://homepages.abdn.ac.uk/djpym/pages/InfoSecPubPol.Pdfht. Submitted for publication* (2013).

Sarbanes-Oxley Act of 2002, Public Law 107-204, see: http://www.sec.gov/about/laws/soa2002.pdf.

Securities and Exchange Commission (SEC), "CF Disclosure Guidance: Topic No. 2," (2011), see: **http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm**

U.S. Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636, (2013), available at http://www.treasury.gov/press-center/Documents/__Supporting Analysis Treasury Report to the President on Cybersecurity Incentives_FINAL.pdf.

U.S. Department of Homeland Security, "Executive order 13636: improving critical infrastructure, Department of Homeland Security, Integrated task force, Incentives study," (2013), available at http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-summary-report-cybersecurity-incentives-study_0.pdf

U.S. Department of Homeland Security, "Executive order 13636: improving critical infrastructure, Department of Homeland Security, Integrated task force, Incentives study analytic report**," (2013), available at:** http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

APPENDIX A

Proof of Proposition 1:

First, we prove by contradiction that $x^* = x_R$ (i.e., $x \geq x_R$ is a binding constraint). Assume $x \geq x_R$ is not binding. The firm's problem then becomes $\max_{x,y}[v - S(x,y,v)]\,L - x - y$, subject to $x + y = B_1$. The optimal solution to this problem is (x_1, y_1), which contradicts the regulatory requirement $x \geq x_R > x_1$. Hence, $x \geq x_R$ must be binding, i.e., $x^* = x_R$.

We, therefore have $S(x^*, y_R, v) = S(x_R, y_R, v)$. Given that $x^* + y_R = x_R + y_R = B_1 = x_1 + y_1$ and $x_R > x_1$, it follows that $y_R < y_1$. Thus, we have $S(x_R, y_R, v) > S(x_R, y_1, v)$, so

$S(x^*, y_R, v) > S(x_R, y_1, v)$. Since (x_1, y_1) is the optimal input mix under budget constraint B_1,

it follows that $S(x_R, y_1, v) \geq S(x_1, y_1, v)$. Combining the last two inequalities, we have

$S(x^*, y_R, v) > S(x_1, y_1, v)$. Hence, by the definitions of S_R and S_1, we have $S_R > S_1$. **Q.E.D.**

Proof of Proposition 2:

With fixed budget B_1, the firm's probability of a cybersecurity breach can be rewritten as $S(x, B_1 - x, v)$, which reaches minimum (highest cybersecurity level) at $x = x_1$ with the first order condition $\frac{dS(x,B_1-x,v)}{dx}|_{x=x_1} = 0$ and the second order condition $\frac{dS^2(x,B_1-x,v)}{dx^2} > 0$ satisfied. This implies that $S(x_R, B_1 - x_R, v)$ is decreasing in x_R on interval $[0, x_1]$ and increasing in x_R on interval $[x_1, \infty)$. Hence, regulation requirement $x = x_R$ will decrease the firm's probability of a cybersecurity breach if it moves the input mix towards $(x_1, B_1 - x_1)$, and increase the firm's probability of a cybersecurity breach if it moves the input mix away from $(x_1, B_1 - x_1)$. **Q.E.D.**

Proof of Proposition 3:

After the firm responds to the regulation, it probability of a cybersecurity breach is characterized by $S(x_A, y_A, v)$. Since the firm meets the government regulatory requirement and does not lower it's expenditures on *Y*, we have $x_A \geq x_R > x_P$ and $y_A \geq y_P$. Since the security breach function is assumed to be decreasing in *X* and in *Y* (see equations [2] and [3]), we have $S(x_A, y_A, v) < S(x_P, y_P, v)$. That is, the firm's probability of a cybersecurity breach has decreased, which means its cybersecurity level has increased. Since $x_A > x_P$ and $y_A \geq y_P$, we have $x_A + y_A > x_P + y_P$ (i.e., the firm's cybersecurity budget has increased). **Q.E.D.**

Proof of Proposition 4:

We first show that $\hat{y} \geq y_1$.

The pre-regulation optimal mix (x_1, y_1) must satisfy the following first order conditions:

$$\begin{cases} -S_x(x_1, y_1, v)L = 1 & [A1] \\ -S_y(x_1, y_1, v)L = 1 & [A2] \end{cases}$$

Since $x \geq x_R$ is binding, the post regulation optimization problem is to maximize the following Lagrangian function:

$$\mathcal{L} = [v - S(x, y, v)]L - x - y + \lambda(x - x_R)$$

First-order conditions are:

$$\begin{cases} -S_x(x_R, \hat{y}, v)L = 1 - \lambda & [A3] \\ -S_y(x_R, \hat{y}, v)L = 1 & [A4] \end{cases}$$

From equations [A4] and [A2], we have $S_y(x_R, \hat{y}, v) = S_y(x_1, y_1, v)$. Given $x_R > x_1$, with $S_{xy} \leq 0$, it follows that $S_y(x_R, y_1, v) \leq S_y(x_1, y_1, v) = S_y(x_R, \hat{y}, v)$. Combined with $S_{yy} > 0$, we have $\hat{y} \geq y_1$. Since we also have $\hat{x} = x_R > x_1$, $S_x < 0$, and $S_y < 0$, it follows that $S(\hat{x}, \hat{y}, v) < S(x_1, y_1, v)$. In addition, $\hat{x} + \hat{y} > x_1 + y_1$. **Q.E.D.**

Proof of Proposition 5:

Recall that the unregulated probability of a cybersecurity breach occurring was denoted as $S_1 = S(x_1, y_1, v)$, and now define $\bar{y}$ as the level of input *Y* achieving the same probability of a cybersecurity breach occurring when $x = x_R$, i.e., $S(x_R, \bar{y}, v) = S(x_1, y_1, v)$. In other words, input mixes (x_1, y_1) and $(x_R, \bar{y})$ are on the same *ISOSEC* curve and $\bar{y}(x_R)$ can be described with the slope of

$$\frac{d\bar{y}_R}{dx_R} = -\frac{S_x}{S_y} \quad [A5]$$

Hence, $\bar{y}_R(x_R)$ is decreasing in x_R with the slope of marginal rate of technical substitution (MRTS) of the security breach function.

The firm's optimal post-regulation investment in input $\hat{y}$ can also be viewed as a function of x_R, i.e., $\hat{y}(x_R)$ and can be described by the taking the total differentiation of the first order condition $-S_y(x_R, \hat{y}, v)L = 1$ Eq [A4]):

$$\frac{\partial S_y}{\partial x}dx + \frac{\partial S_y}{\partial y}dy = 0$$

So that:

$$\frac{d\hat{y}}{dx_R} = -\frac{S_{xy}}{S_{yy}}, \quad [A6]$$

when $x_R = x_1$, $\hat{y} = \bar{y}_R = y_1$. This means when the regulation requires the firm to spend at least x_1, the firm will choose the optimal mix (x_1, y_1), and the regulation would not change the probability of a cybersecurity breach (i.e., the cybersecurity level remains the same). When the regulation requires the firm to increase spending on input *X*, imposing $x > x_R > x_1$, the firm needs to spend at least $\bar{y}_R$ to maintain the pre-regulation cybersecurity level. Therefore, by comparing $\hat{y}$ with $\bar{y}_R$, we can draw a conclusion on the regulation induced cybersecurity level. When $S_{xy} \leq 0$, $\hat{y}(x_R)$ is weakly increasing in x_R, the firm would not decrease spending on input *Y*, and the firm will always have a higher post regulation security level (i.e., Proposition 4). When $S_{xy} > 0$, $\hat{y}(x_R)$ is decreasing with the slope of $-\frac{S_{xy}}{S_{yy}}$. If $\hat{y}(x_R)$ is steeper than the *ISOSEC* curve ($-\frac{S_x}{S_y} > -\frac{S_{xy}}{S_{yy}}$), the firm would not invest enough to maintain the same cybersecurity level and the regulation would result in lower cybersecurity level; on the other hand, if $\hat{y}(x_R)$ is flatter than the *ISOSEC* curve ($-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$), the firm would invest more than enough to maintain the same cybersecurity level and the regulation would result in higher cybersecurity level. **Q.E.D.**

Proof that generalized version of security breach probability functions from Gordon and Loeb (2002) satisfying Proposition 5.

I. For $S^I(x, y, v) = \frac{v}{(\alpha_1 x+1)^{\beta_1}(\alpha_2 y+1)^{\beta_2}}$, we calculate the following derivatives:

$$S_x = -\frac{\alpha_1\beta_1 v}{(\alpha_1 x + 1)^{\beta_1+1}(\alpha_2 y + 1)^{\beta_2}}$$

$$S_y = -\frac{\alpha_2\beta_2 v}{(\alpha_1 x + 1)^{\beta_1}(\alpha_2 y + 1)^{\beta_2+1}}$$

$$S_{xy} = \frac{\alpha_1\alpha_2\beta_1\beta_2 v}{(\alpha_1 x + 1)^{\beta_1+1}(\alpha_2 y + 1)^{\beta_2+1}}$$

$$S_{yy} = \frac{\alpha_2^2\beta_2(\beta_2 + 1)v}{(\alpha_1 x + 1)^{\beta_1}(\alpha_2 y + 1)^{\beta_2+2}}$$

$$\frac{S_x}{S_y} = \frac{\alpha_1\beta_1(\alpha_2 y + 1)}{\alpha_2\beta_2(\alpha_1 x + 1)}$$

$$\frac{S_{xy}}{S_{yy}} = \frac{\alpha_1\beta_1(\alpha_2 y + 1)}{\alpha_2(\beta_2 + 1)(\alpha_1 x + 1)}$$

$$-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$$

The above calculations show that for this class of breach function, $-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$, which implies the regulation leads to an improved cybersecurity level.

II. For $S^{II}(x, y, v) = v^{(\alpha_1 x+1)(\alpha_2 y+1)}$, we have:

$$S_x = \alpha_1(\alpha_1 x + 1)(\alpha_2 y + 1)^2 v^{(\alpha_1 x+1)(\alpha_2 y+1)} \ln v$$

$$S_y = \alpha_2(\alpha_1 x + 1)^2(\alpha_2 y + 1) v^{(\alpha_1 x+1)(\alpha_2 y+1)} \ln v$$

$$S_{xy} = \alpha_1\alpha_2(\alpha_1 x + 1)(\alpha_2 y + 1) v^{(\alpha_1 x+1)(\alpha_2 y+1)} \ln v\,[(\alpha_1 x + 1)^2(\alpha_2 y + 1)^2 \ln v + 2]$$

$$S_{yy} = \alpha_2^2(\alpha_1 x + 1)^2 v^{(\alpha_1 x+1)(\alpha_2 y+1)} \ln v\,[(\alpha_1 x + 1)^2(\alpha_2 y + 1)^2 \ln v + 1]$$

$$\frac{S_x}{S_y} = \frac{\alpha_1(\alpha_2 y + 1)}{\alpha_2(\alpha_1 x + 1)}$$

$$\frac{S_{xy}}{S_{yy}} = \frac{\alpha_1(\alpha_2 y + 1)}{\alpha_2(\alpha_1 x + 1)} \cdot \frac{(\alpha_1 x + 1)^2(\alpha_2 y + 1)^2 \ln v + 2}{(\alpha_1 x + 1)^2(\alpha_2 y + 1)^2 \ln v + 1}$$

$$-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}.$$[32]

For this second class of breach function, we also have $-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$, the regulation again leads to a higher cybersecurity level. **Q.E.D.**

[32] When $S_{xy} \leq 0$, $-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$ holds. When $S_{xy} > 0$, it follows that $(\alpha_1 x + 1)^2(\alpha_2 y + 1)^2 \ln v + 2 < 0$. Hence, $\frac{(\alpha_1 x+1)^2(\alpha_2 y+1)^2 \ln v+2}{(\alpha_1 x+1)^2(\alpha_2 y+1)^2 \ln v+1} < 1$, we have $-\frac{S_x}{S_y} < -\frac{S_{xy}}{S_{yy}}$ again.

APPENDIX B

In Lockheed Martin's 10-K Annual Report filed with the SEC, for the fiscal year ending December 31, 2013, under Item 1A: Risk Factors, the following statements concerning cybersecurity related issues are made:

> "**Our business could be negatively affected by cyber or other security threats or other disruptions.**
>
> As a U.S. defense contractor, we face cyber threats, insider threats, threats to the physical security of our facilities and employees, and terrorist acts, as well as the potential for business disruptions associated with information technology failures, natural disasters, or public health crises.
>
> We routinely experience cyber security threats, threats to our information technology infrastructure and unauthorized attempts to gain access to our company sensitive information, as do our customers, suppliers, subcontractors and venture partners. We may experience similar security threats at customer sites that we operate and manage as a contractual requirement.
>
> Prior cyber-attacks directed at us have not had a material impact on our financial results, and we believe our threat detection and mitigation processes and procedures are adequate. The threats we face vary from attacks common to most industries to more advanced and persistent, highly organized adversaries who target us because we protect national security information. If we are unable to protect sensitive information, our customers or governmental authorities could question the adequacy of our threat mitigation and detection processes and procedures. Due to the evolving nature of these security threats, however, the impact of any future incident cannot be predicted.
>
> Although we work cooperatively with our customers, suppliers, subcontractors, venture partners, and acquisitions to seek to minimize the impact of cyber threats, other security threats or business disruptions, we must rely on the safeguards put in place by these entities, which may affect the security of our information. These entities have varying levels of cyber security expertise and safeguards and their relationships with government contractors, such as Lockheed Martin, may increase the likelihood that they are targeted by the same cyber threats we face.
>
> The costs related to cyber or other security threats or disruptions may not be fully insured or indemnified by other means. Additionally, some cyber technologies we develop, particularly those related to homeland security, may raise potential liabilities related to intellectual property and civil liberties, including privacy concerns, which may not be fully insured or indemnified by other means. Occurrence of any of these events could adversely affect our internal operations, the services we provide to our customers, our future financial results, our reputation or our stock price; or such events could result in the loss of competitive advantages derived from our research and development efforts or other intellectual property, early obsolescence of our products and services, or contractual penalties.
>
> (See: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/2013-Annual-Report.pdf, p. 16).

D. The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective

Forthcoming in *Journal of Accounting and Public Policy*

By

Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Lei Zhou

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.

The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective

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 (SEC, 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

[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.

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, 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 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] 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 found "45 percent 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.

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

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 (2003) show that information sharing related to computer security activities may also positively affect the demand for a firm's products. Both Gordon and Loeb (2003b) and Gal-Or and Ghose (2003) 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 and Loeb (2003b) and Gal-Or and Ghose (2003), 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

---

[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).

[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).

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), Kaimen 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.

[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 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 Segal, 1986; Dixit and Pindyck, 1994). Furthermore, there have been several papers addressing the application of real options to 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

[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.

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] 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.,

[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.

[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.

$(11 \times \$200{,}000 - \$1{,}000{,}000) \times .5)$, 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 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. However, we now 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

[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., $11 \times \$40{,}000$), 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).

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.

Figure 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 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 Figure 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 Figure 2). Hence, the expected magnitude of the firm's cybersecurity investment is greater with information sharing than without information sharing ($1,500,000

[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.

+.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. See: 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. Information Systems Research, 10 (1), 70-86.

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

Benaroch, M., Shah, S., Jeffery, M., 2006. On the valuation of multi-stage IT investments embedding nested real options. Journal of Management Information Systems, 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. See: 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. The Economics of Information Security and Privacy, Springer, 25-47.

Department of Homeland Security (DHS), Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise, November 2011, see: 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. Information Systems Research, 15 (2), 132-154.

Fried, D., 1984. Incentives for information production and disclosure in a duopolistic environment. The Quarterly Journal of Economics, 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. Information Systems Research, 16 (2), 186-208.

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

Gordon, L.A., Loeb, M.P., 2002. The economics of information security investment. ACM Transactions on Information and System 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. Computer Security Journal, 19 (2), 1-7.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., 2003b. Sharing information on computer systems security: An economic analysis. Journal of Accounting and 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. Journal of Accounting and 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? Journal of Computer Security, 19 (1), 33-56.

Herath, H.S., Herath T.C., 2008. Investments in information security: A real options perspective with Bayesian postaudit. Journal of Management Information Systems, 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. The American Economic Review, 82 (5), 1293-1306.

Kirby, A., 1988. Trade associations as information exchange mechanisms. RAND Journal of Economics, 29 (1), 138–146.

Mathews, C.M., 2013. Companies not budgeting enough for cybersecurity, study says. The Wall Street Journal Risk & Compliance Journal. April 12, 2013. See: http://blogs.wsj.com /riskandcompliance/2013/04/12/companies-not-budgeting-enough-for-cybersecurity-study-says/

McDonald, R., Siegel, D., 1986. The value of waiting to invest. Quarterly Journal of Economics. 101 (4), 707-727.

Novshek, W., Sonnenschein, H., 1982. Fulfilled expectations Cournot duopoly with information acquisition and release. The Bell Journal of Economics, 13, 214-218.

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

Sarbanes-Oxley Act of 2002, see: 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. 122-137.

Shapiro, C., 1986. Exchange of cost information in oligopoly. The Review of Economic Studies, 53 (3), 433–446.

Target Corporation Annual Report (Form 10-K) for the fiscal year ended February 1, 2014. Available file://localhost/at 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, 211-228.

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

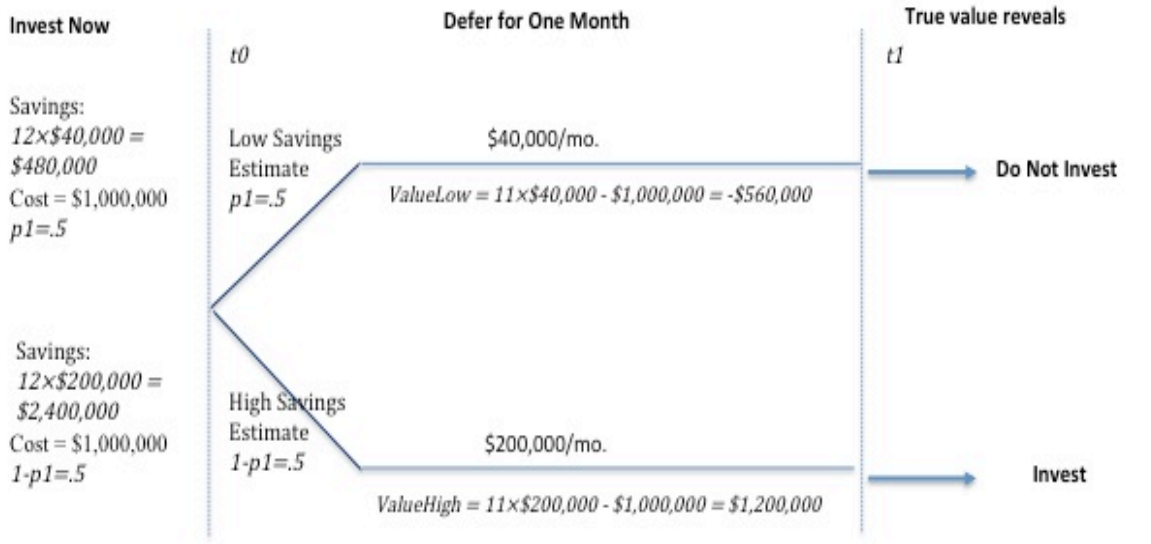
U.S. Security and Exchange Commission Division of Corporation Finance. 2011. CF Disclosure Guidance: Topic No. 2 Cyber Security. See: http://www.sec.gov/divisions/corpfin/guidance/ cfguidance-topic2.htm

Varian, Hal, System Reliability and Free Riding, *Workshop on the Economics of Information Security*, 2002 May 16-17, Berkeley, CA, See: 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 Journal of Economics, 21 (3), 409–430.

Ziv, A., 1993. Information sharing in oligopoly: The truth-telling problem. RAND Journal of Economics, 24 (3), 455–465.

Figure 1 Strategy 1: Ignore information sharing and defer the investment*



EV from investing now
$480,000×.5 +$2,400,000×.5 - $1,000,000 = $440,000

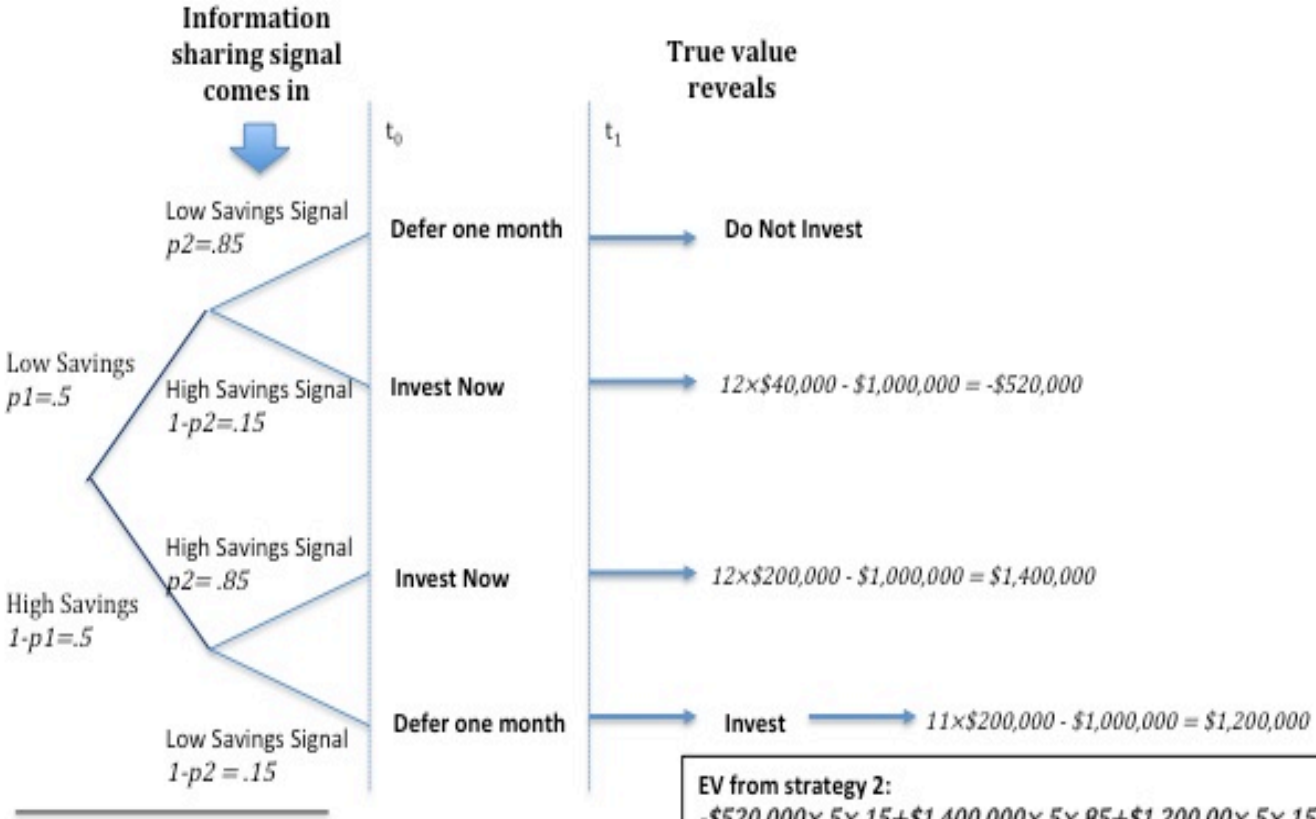
EV from strategy 1:
$1,200,000×.5=$600,000

Ex ante probability to invest: 50%

EV = expected value
p 1 = prior belief probability of cost savings to be low

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

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



EV = expected value
p1 = prior belief probability of cost savings to be low
p2 = information sharing signal accuracy

Critical accuracy of the information sharing signal:
$600,000=-$520,000×.5×1-x+$1,400,000×.5×x+
$1,200,000×.5×1-x
x≈.722

EV from strategy 2:
-$520,000×.5×.15+$1,400,000×.5×.85+$1,200,00×.5×.15
=$646,000
Ex ante probability to invest with information sharing:
.5×.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.

III. INTERVIEWS WITH EXECUTIVES AND CASE STUDIES

A summary of the case studies contained in this section of the Report will be developed into a separate article for publication in a journal. In this regard, the Editor of the *Georgetown Journal of International Affairs* has invited us to submit the article for the journal's 2016 special issue on Cybersecurity.

A. Introduction

There were two fundamental objectives of the case studies portion of our DHS proposal. The first objective was to gather information that would allow us to assess the validity of the basic hypotheses in the proposal. Based on the information provided from the case studies, we would either retain our original three main hypotheses or make the necessary changes based on the information gleaned from the case studies. The second objective of the case studies portion of our DHS proposal was to help us design the instrument that would be used for a large-scale survey of corporations in the private sector operating in critical infrastructure industries.

In pursuing the two objectives specified above, we initially met with eight senior executives in charge of cybersecurity within their firms (representing the telecommunications, power utilities, and financial sectors). The goal of these meetings was to identify and recruit three or four firms to participate in the case studies portion of our research project. All of the executives we met agreed that our project was important. Furthermore, they were all willing to have a general conversation with us about the cybersecurity issues under investigation. In terms of specific details concerning their firms, however, it quickly became clear (with all of these individuals) that the executives were guarded in terms of the information provided, and that each executive did not want the company's name associated with any of the information provided. Moreover, they were reluctant to provide specific details, even though we assured anonymity. A summary of the findings from meeting with the executives is provided below.

Given the experience described above, we decided to also pursue a second approach for gathering the information associated with achieving the two objectives of the case studies. Our second approach is to develop case studies of firms that experienced major cybersecurity breaches that resulted in the public release of the type of information we were seeking for this research project. This idea originated as a result of the February 4, 2014 Senate Hearings concerning the cybersecurity breaches at Target, Inc. and Neiman Marcus, Inc. More to the point, what became apparent was that firms that experienced major, well publicized, cybersecurity breaches were often subject to severe scrutiny in public documents (e.g., Congressional Testimony and Corporate Annual 10K and 8K Reports), as well as in the popular press. In fact, as we delved into examining high visibility security breaches, we realized that most of the information we were trying to obtain though the case studies was available via public information. The information provided in these public records and in the popular press was being gathered in such a way that the details for specific companies were made available by the senior executives responsible for the firms' cybersecurity activities. Furthermore, the information provided during Congressional Hearings by executives under oath and information provided to the SEC on Annual 10K Reports has face reliability and validity. In addition, these high visibility cases resulted in a wealth of other publicly available information (e.g., from company

websites, videos, etc.) that could easily be obtained and verified. In light of the above, we decided to supplement the information derived from our discussions with the executives with case studies of four companies that recently (i.e., within the past couple of years) experienced highly visible cybersecurity breaches. The companies selected these case studies are: Target, Neiman Marcus, RSA, and JPMorgan Chase. The case studies for each of our companies followed a template that focused on answering the following questions:

1. What cybersecurity procedures were in place prior to the actual breach?

2. How did the firm identify the cybersecurity breach?

3. What is the estimate of the ultimate cost, in terms of both private costs and externalities, of the cybersecurity breach to the firm and how is that cost derived?

4. Is there a concerted strategy towards cybersecurity investments in your firm, and, if so, how much does the firm annually invest in cybersecurity activities?

5. Did your firm consider the risks associated with potential cybersecurity breaches, and if so, how?

6. What, if any, cybersecurity insurance did the company have in place prior to the breach?

7. What sort of cybersecurity related information sharing arrangements did the firm have in place prior to the breach?

8. How did the firm respond to the cybersecurity breach (include any changes in the firm's procedures and policies toward cybersecurity as a result of the breach)?

9. How did the cybersecurity breach affect the firm's disclosure in financial reports and public announcement?

The case studies, addressing the questions posed above, are also included in this Report. As will be seen, the information gleaned from these case studies, as well as the information obtained from the meetings with the executives, reaffirmed the importance of the original hypotheses contained in our research proposal. However, the information obtained did suggest the appropriateness of gathering additional information (i.e., additional to what we had originally planned) in our large survey. In particular, based on the four case studies, and the discussions with the executives, it became clear that our survey should gather information related to the types of incentives the federal government could (or should) provide to facilitate the appropriate level of cybersecurity activities in firms within the private sector. Furthermore, the issue of cybersecurity insurance surfaced as an issue that we should include in our survey.

B. Summary of Meetings with Executives

As noted above, we met with eight executives in charge of cybersecurity within a variety of firms. These meetings were informative, despite the fact that the executives were extremely guarded in the terms of the information provided. A summary of the information gleaned from these meetings is provided below.

Portion of IT Budget Spent on Cybersecurity Activities

The portion of IT budget spent on cybersecurity activities varied from firm to firm. Some of the executives provided actual percentages (ranging from 3% to 12%) of the IT budget devoted to cybersecurity activities, whereas others were reluctant to provide a specific percentage. Much of the variation concerning the portion of the IT budget spent on cybersecurity seems due to the way cybersecurity expenditures are defined. Some firms only considered dedicated security expenditures, while others counted all of the indirect security costs throughout their operation. The executives made it clear that what qualifies as an expenditure on cybersecurity activities vs. expenditures on general IT activities is fuzzy, at best.

There was only limited agreement on how to account for the indirect costs associated with cybersecurity activities (e.g., costs associated with certain hardware, salaries of some employees, etc.) as contracted with the direct costs of cybersecurity activities (e.g., malware software, intrusion prevention and detection systems, firewalls, etc.) Nevertheless, there seems to be general agreement that expenditures on cybersecurity activities are increasing in an absolute sense, and as a proportion of the firm's IT budget, over the past few years. Furthermore, there was also a general belief that the cybersecurity expenditure trend noted above would continue during the foreseeable future.

One point that became clear was that some executives responsible for their firms' cybersecurity activities had cultivated sufficient trust and respect so that their proposed projects for enhancing cybersecurity were usually successful in securing (internal) funding. However, there was no clear consensus on the type of analysis that was used to obtain their security spending. One other point noted by virtually all of the executives was that it is common to receive a large infusion of funds for cybersecurity activities following a cybersecurity breach within the firm.

Deriving Expected Benefits from Cybersecurity Activities

There was general agreement among the executives interviewed that the major benefits derived from cybersecurity activities come from the cost savings (or cost avoidance) associated with preventing and/or managing cybersecurity breaches, as well as reducing the risks of such breaches. In other words, reducing the expected loss associated with cybersecurity breaches is the dominant benefit derived from cybersecurity activities, according to the executives interviewed.[1]

A few of the executives noted that supporting compliance and audit findings represent additional benefits derived from cybersecurity activities. In addition, a few executives mentioned that having a strong cybersecurity program, related to their competitors, could generate new revenues for their firm. That is, in limited situations, a strong cybersecurity program could provide a firm with a short-run competitive advantage. In the long run, it was felt that all firms would need to have strong cybersecurity programs.

[1] The *expected loss* is the sum of the estimated dollar amounts of various losses due to potential cybersecurity breaches multiplied by the probabilities that such breaches would occur (or what many call the *mean* of the potential losses).

Although all the executives expressed the view that their firms derived benefits from investing in cybersecurity activities, they also pointed out the difficulties in quantifying these benefits. Thus, it was noted that qualitative justification often dominates the cybersecurity investment decision process. As one executive put it, "…we tend to ask a series of questions in deciding whether or not to invest more into cybersecurity activities." Examples of the types of questions are: "How will the investment reduce the risks of cybersecurity breaches? How will the investment improve compliance? How will the investment resolve problems identified by the firm's auditors?"

Estimating Potential Risks Associated with Cybersecurity Breaches

Although not necessarily expressed in mathematical terms, the expected loss was the dominant means by which the executives expressed the potential risk. One executive did mention, however, that it was the "big breach" (i.e., a major, catastrophic, breach) that worried him the most.

Consideration of Externalities

Generally speaking, there seems to be very little, if any, consideration given to externalities that result from making cybersecurity investments.[2] In other words, firms tend to ignore the impact that their cybersecurity breaches and cybersecurity investments have on other firms, unless they are responsible for some part of the damages resulting from the breach (i.e., unless there are some indirect private costs, which technically means these costs are not externalities).

Information Sharing

All of the executives pointed out that their firms are actively involved in some sort of information sharing related to cybersecurity. Some of the firms are members of an industry ISAC (Information Sharing and Analysis Center), whereas other firms are involved in other types of information sharing arrangements (e.g., via CERT [Computer Emergency Response Team] or law enforcement agencies). However, the degree to which information sharing was perceived as beneficial was highly variable. This latter fact notwithstanding, there was a general agreement that improved and more open information sharing would be helpful in preventing and quickly responding to future cybersecurity breaches, even as they admitted that their firms may be reluctant to share sensitive data regarding breaches. A point that was raised, in this latter regard, was the need for some sort of limited liability protection associated with the information shared.

Regulation and/or Incentives

There was virtually unanimous resistance to a greater regulatory environment to improve cybersecurity by the federal government. This view was based, on large part, in the belief that such regulation would not be successful for a variety of reasons. Most prominent among these reasons was the speed with which the technology and threats evolve. The executives were,

[2] Externalities are the spillover costs (or benefits) to firms that derive from actions of other firms, such that the firms initiating the actions are not affected by the costs (or benefits).

however, in favor of increased government incentives. That said, the discussions on incentives did not provide a consensus as to types of government incentives that would be most effective.

Cybersecurity Insurance

Some of the firms represented by the executives have cybersecurity insurance, whereas others do not have such insurance. Two common concerns with the insurance policies available for cybersecurity breaches are the high deductibles and low coverage ceilings associated with the policies.

Critical Issues that Could Impact Organizations in the Near Future

The executives were asked to indicate some of the critical issues that could have a significant impact on their firms in the near future (i.e., next two years). Below is a list of the key issues mentioned by these individuals:

- Mobile Devices
- BYOD (Bring Your Own Device)
- Supporting Multiple Platforms
- Security Associated with Cloud Computing
- Better Coordination (including information sharing within and between organizations in the private and public sector)
- Cybersecurity Insurance

C. Case Studies

1. Target

Background: Target Corporation, with its bull's eye logo, is one of the best-known corporations in the United States. The company operates nearly 1,800 retail stores in the United States and over 100 in Canada,[3] offering a wide variety of clothing, household items, groceries and pharmacy items. The company's subsidiary, Financial and Retail Services, issues Target's credit cards and Target Debit Cards. Target, which is headquartered in Minneapolis, was ranked as the 34th largest firm in the 2014 Forbes 500 list based on revenue.[4] The company employs over 360,000 employees, and is the second largest merchandise retailer in America[5]. In its latest fiscal year (ending February 1, 2014), the firm earned nearly $ 2 billion on sales of $72.6 billion. However, in the previous fiscal year, the firm earned nearly $3 billion on sales of less than $72 billion. (see Appendix to this case study).

On December 18, 2013, Target Corporation publicly announced a massive cybersecurity breach involving the theft of records of about 40 million debit and credit cards used at Target Stores from November 27, 2013 to December 15, 2003.[6] Within a month the company confirmed that another 70 million records were compromised. Investigation of the breach[7] indicated that Target was attacked using credentials of a Fazio Mechanical Service that sold refrigeration services to Target. The cybersecurity breach at Target took place despite the fact that the company had employed standard security defenses (e.g., virus protection and intrusion detection systems). The attackers are believed to have acquired the credentials of Fazio by means of phishing attacks. With the use of the Fazio credentials, the attackers were able to penetrate Targets' systems and uploaded RAM Scraping malware to Target's Point-of-Sales terminals. This malware takes the data when the cards are swiped from an infected terminal. Using data exfiltration malware that the attackers also inserted in the system, the stolen data was sent to the attackers. Attackers sold the stolen information on the black market and then the buyers produce counterfeit cards by encoding the stolen information onto the new cards magnetic strips. If sufficient information were stolen, the purchasers of stolen data could commit identity theft, taking out loans with the false identity.

Target responded to the cybersecurity breach in a number of ways.[8] These included the actions of notifying payment processors and card networks of the breach, removal of malware from the system, communications to customers via multiple forms (e.g., emails, social media, mass

---

[3] See "Corporate Fact Sheet" at http://pressroom.target.com/corporate, accessed September 9, 2014.
[4] See http://fortune.com/fortune500/target-corporation-36 accessed September 9, 2014.
[5] See "Corporate Fact Sheet" at http://pressroom.target.com/corporate, accessed September 9, 2014.
[6] See the press release at: http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores, accessed September 9, 2014. The announcement may be better characterized as an acknowledgement, since a security blog, Krebs on Security, announced the breach on December 18, 2013. See http://krebsonsecurity.com/2013/12/ sources-target-investigating-data-breach/.
[7] See for example, "'Kill Chain' Analysis of the 2013 Target Data Breach," the U.S. Senate Committee on Commerce, Science, and Transportation Majority Staff Report for Chairman Rockefeller, March 26, 2014.
[8] The subsequent discussion is based on the February 4, 2014 Written Testimony of Target Executive Vice President and Chief Financial Officer John Mulligan before the Senate Committee on the Judiciary Hearing on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime.

communication outlets) letting them know they would not be liable for fraudulent charges to their accounts, providing free enrollment in a credit monitoring service, and offering customers at 10% discount for purchases at Target (excluding online purchases) on the weekend before Christmas. In addition, the company increased fraud detection on the debit and credit cards that the firm issued, reissuing credit or debit cards at request, accelerating investment in chip-enabled technologies, initiated and contributed $5 million to promote cybersecurity awareness and education. As a result of the attack, Target joined the Financial Sector- Information Sharing and Analysis Center (FS-ISAC). Moreover, Target helped to initiate an information sharing organization for the retail industry, called Retail Cyber Intelligence Sharing Center (R-CISC).[9]

Questions and Answers for Target Corporation:

a. What cybersecurity procedures were in place prior to the actual breach?

"Prior to the data breach, we had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools. We performed internal and external validation and benchmarking assessments. And in September 2013, our systems were certified compliant with the Payment Card Industry Data Security Standards, meaning that we met approximately 300 independent requirements of the assessment."

-- Mr. John J. Mulligan, VP and CFO of Target Corporation, March 26, 2014 Congressional Hearing on Consumer Data Privacy

b. How did the firm identify the cybersecurity breach?

"On the evening of December 12 (2013), we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores…"

-- Mr. John J. Mulligan, VP and CFO of Target Corporation, February 04, 2014 Congressional Hearing on Cybercrime and Privacy

c. What is the estimate of the ultimate cost, in terms of both private costs and externalities, of the cybersecurity breach to the firm and how is that cost derived?

"We experienced weaker than expected U.S. Segment sales following the announcement of the Data Breach and are unable to determine whether there will be a long-term impact to our relationship with our guests and whether we will need to engage in significant promotional or other activities to regain their trust."

"The data breach we experienced in 2013 has resulted in government inquiries and private litigation, and if our efforts to protect the security of information about our guests and team members are unsuccessful, future issues may result in additional costly government enforcement actions and private litigation and our sales and reputation could suffer."

[9] R-CISC was launched on May 14, 2014. See http://www.rila.org/news/topnews/Pages/RetailersLaunchComprehensive CyberIntelligenceSharingCenter.aspx.

"We are currently facing more than 80 civil lawsuits filed on behalf of guests, payment card issuing banks and shareholders. In addition, state and federal agencies, including State Attorneys General, the Federal Trade Commission and the SEC, are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. Those claims and investigations may have an adverse effect on how we operate our business and our results of operations."

-- Target Corporation, March 14, 2014 10-K

"In second quarter 2014, the Company expects to record gross breach-related expenses of $148 million, partially offset by the recognition of a $38 million insurance receivable. Expenses for the quarter include an increase to the accrual for estimated probable losses for what the Company believes to be the vast majority of actual and potential breach-related claims, including claims by payment card networks. Given the varying stages of claims and related proceedings, and the inherent uncertainty surrounding them, the Company's estimates involve significant judgment and are based on currently available information, historical precedents and an assessment of the validity of certain claims. These estimates may change as new information becomes available and, although the Company does not believe it is probable, it is reasonably possible that the Company may incur a material loss in excess of the amount accrued. The Company is unable to estimate the amount of such reasonably possible excess loss exposure at this time. The accrual does not reflect future breach-related legal, consulting or administrative fees, which are expensed as incurred and not expected to be material in any individual period."

-- Target Corporation, August 5, 2014 8-K

The $148 million mentioned in Target Corporation's August 5, 2014 8-K Form filed with the SEC does not include an estimate of lost profits due to lost sales (to date and in the future). In addition, the externality costs were not taken into account in the corporation's estimate of $148 million as the costs due to the breach.

Target's sales in 2011, 2012, and 2013, were 68.466, 71.960, and 72.596 million dollars, respectively. As indicated by the above numbers, sales grew at roughly a 5% rate in 2012 relative to 2011. However, sales grew at less than 1% in 2013 (i.e., during 2013, the time frame when the cybersecurity breach occurred). Although many factors may have contributed to low sales growth in 2013, the announcement of the cybersecurity breach during the 2013 holiday season clearly contributed to this situation. In fact, as indicated above, Target itself acknowledged (in its 10-K Report covering the time period when the breach occurred) the fact that the cybersecurity breach resulted in weaker than expected sale. The company's net earnings for the same years (i.e., 2011, 2012, and 2013) were 2.929, 2.999 and 1.971 million dollars, respectively. Thus, net earnings dropped by slightly more than 1 billion dollars during the 2013 time frame. This reduction in net earnings was likely due to several factors, including the company's failed investment in Canadian stores (see: http://www.wsj.com/articles/target-to-exit-canada-1421328919). However, the data breach, with its associated costs, undoubtedly contributed to this decline in net earnings.

d. Is there a concerted strategy towards cybersecurity investments in your firm, and, if so, how much does the firm annually invest in cybersecurity activities?

"For many years Target has invested significant capital and resources in security technology, personnel and processes. We had in place multiple layers of protection, including firewalls, malware detection, intrusion detection and prevention capabilities and data loss prevention tools."

"Over the past several years, we have invested hundreds of millions of dollars in several areas in technology to prevent data loss. This includes segmentation, malware detection, intruder detection and prevention, data loss prevention tools, multiple layers of firewalls."

--Mr. John J. Mulligan, VP and CFO of Target Corporation, February 04, 2014 Congressional Hearing on Cybercrime and Privacy, Panel Discussion

e. Does your firm consider the risks associated with potential cybersecurity breaches, and, if so, how?

Although Target does consider the risks, there's no specificity on how they consider it. Furthermore, there's no clear indication of how they use the risk to determine the level of investments in cybersecurity activities.

"If our efforts to protect the security of personal information about our guests and team members are unsuccessful, we could be subject to costly government enforcement actions and private litigation and our reputation could suffer.

The nature of our business involves the receipt and storage of personal information about our guests and team members. We have a program in place to detect and respond to data security incidents. To date, all incidents we have experienced have been insignificant. If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of RED cards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges increase our labor costs and affect how we operate our business."

-- Target Corporation, 10-K, for the fiscal year ended February 2, 2013 (i.e., in the fiscal year prior to the breach)

"The data breach we experienced in 2013 has resulted in government inquiries and private litigation, and if our efforts to protect the security of information about our guests and team members are unsuccessful, future issues may result in additional costly government enforcement actions and private litigation and our sales and reputation could suffer. The nature of our business involves the receipt and storage of information about our guests and team members. We have a program in place to detect and respond to data security incidents. However, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems

change frequently and may be difficult to detect for long periods of time, we may be unable to anticipate these techniques or implement adequate preventive measures. In addition, hardware, software or applications we develop or procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise information security. Unauthorized parties may also attempt to gain access to our systems or facilities through fraud, trickery or other forms of deceiving our team members, contractors and temporary staff. Until the fourth quarter of 2013, all incidents we experienced were insignificant. The Data Breach we experienced was significant and went undetected for several weeks. We experienced weaker than expected U.S. Segment sales immediately following the announcement of the Data Breach, and we are currently facing more than 80 civil lawsuits filed on behalf of guests, payment card issuing banks and shareholders. In addition, state and federal agencies, including State Attorneys General, the Federal Trade Commission and the SEC, are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. Those claims and investigations may have an adverse effect on how we operate our business and our results of operations.

"If we experience additional significant data security breaches or fail to detect and appropriately respond to significant data security breaches, we could be exposed to additional government enforcement actions and private litigation. In addition, our guests could further lose confidence in our ability to protect their information, which could cause them to discontinue using our RED cards or pharmacy services, or stop shopping with us altogether."

-- Target Corporation, 10-K, for the fiscal year ended February 1, 2014 (i.e., in the fiscal of the breach)

f. What, if any, cybersecurity insurance did the company have in place prior to the breach?

"To limit our exposure to Data Breach losses, we maintain $100 million of network-security insurance coverage, above a $10 million deductible. This coverage and certain other insurance coverage may reduce our exposure. We will pursue recoveries to the maximum extent available under the policies. As of February 1, 2014, we have recorded a $44 million receivable for costs we believe are reimbursable and probable of recovery under our insurance coverage, which partially offsets the $61 million of expense relating to the Data Breach."

-- Target Corporation, 10-K, for the fiscal year ended February 1, 2014 (i.e., in the fiscal of the breach)

g. What sort of cybersecurity related information sharing arrangements did the firm have in place prior to the breach?

Seems none prior to the breach.

As a result of the breach, "Target became the first retailer to join the Financial Services Information Sharing and Analysis Center (FS-ISAC), an initiative developed by the financial services industry to help facilitate the detection, prevention, and response to cyber-attacks and fraud activity."

-- Mr. John J. Mulligan, VP and CFO of Target, March 26, 2014 Congressional Hearing on Consumer Data Privacy

In addition, Target was among the firms that initiated a new information sharing organization called Retail Cyber Intelligence Sharing Center (R-CISC). (See: http://www.rila.org/rcisc/Home/Pages /default.aspx)

h. How did the firm respond to the cybersecurity breach (include any changes in the firm's procedures and policies toward cybersecurity as a result of the breach)?

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

-- Target Corporation, 10 K, for the fiscal year ended February 1, 2014 (i.e., in the fiscal of the breach)

In his written testimony to the Senate Committee on the Judiciary Hearing on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime given on February 4, 2014, John J. Mulligan, VP and CFO of Target reported that Target took the following actions subsequent to the breach: (a) notifying payment processors and card networks of the breach; (b) removal of malware from the system; (c) communications to customers via multiple forms (e.g., emails, social media, mass communication outlets) letting them know they would not be liable for fraudulent charges to their accounts, and providing free enrollment in a credit monitoring service. Moreover, in his December 2013 press releases, (then) CEO Gregg Steinhafel offered customers at 10% discount for purchases at Target (excluding online purchases) on the weekend before Christmas.[10]

i. How did the cybersecurity breach affect the firm's disclosure in financial reports and public announcement?

There has been a significant change in the firm's 10-K (annual report) filed for SEC as a result of the cybersecurity breach. These changes include: a discussion of the data breach in part I, item 1, general discussion portion of the 10-K; item 1(a) risk factor discussion of the 10-K; part II, item 7, management's discussion and analysis of financial condition and results of operations; item 8 financial statements and supplementary data, notes to consolidated financial statements 17 commitment and contingencies.

In addition, the breach resulted in an 8-K filing on August 5, 2014 with a section called "Update on expenses related to the data breach".

Additional Issues: It is worth noting that the cybersecurity breach also seemed to have caused, or at least contributed to, personnel changes within the company**.** More to the point, within a few months of the breach becoming public, the firm's Chief Information Officer decided to retire (see: http://www.nytimes.com/2014/03/06/business/targets-chief-information-officer-resigns.

[10] See, http://pressroom.target.com/news/a-message-from-ceo-gregg-steinhafel-about-targets-payment-card-issues

html?_r=0). In addition, a couple of months later, the firm's Chief Executive Officer stepped down from his position (see: http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/). Of course, there were likely many factors contributing to these personnel changes. However, the cybersecurity breach experienced by the company likely played a significant part in bringing about these personnel changes.

Appendix

Target's Stock Prices[11]

[11] Taken from Yahoo! Finance

Target's Income Statement[12]

Consolidated Statements of Operations

(millions, except per share data)	2013	2012	2011
Sales	**$ 72,596**	$	$
Credit card revenues	**—**	1,341	1,399
Total revenues	**72,596**	73,301	69,865
Cost of sales	**51,160**	50,568	47,860
Selling, general and administrative expenses	**15,375**	14,914	14,106
Credit card expenses	**—**	467	446
Depreciation and amortization	**2,223**	2,142	2,131
Gain on receivables transaction	**(391)**	(161)	—
Earnings before interest expense and income taxes	**4,229**	5,371	5,322
Net interest expense	**1,126**	762	866
Earnings before income taxes	**3,103**	4,609	4,456
Provision for income taxes	**1,132**	1,610	1,527
Net earnings	**$ 1,971**	$	$
Basic earnings per share	**$ 3.10**	$	$
Diluted earnings per share	**$ 3.07**	$	$
Weighted average common shares outstanding			
Basic	**635.1**	656.7	679.1
Dilutive effect of share-based awards *(a)*	**6.7**	6.6	4.8
Diluted	**641.8**	663.3	683.9

(a) Excludes 2.3 million, 5.0 million and 15.5 million share-based awards for 2013, 2012 and 2011, respectively, because their effects were antidilutive.

See accompanying Notes to Consolidated Financial Statements.

Consolidated Statements of Comprehensive Income

(millions)	2013	2012	2011
Net earnings	**$ 1,971**	$	$ 2,929
Other comprehensive income/(loss), net of tax			
Pension and other benefit liabilities, net of provision/(benefit) for taxes of **$71,** $58 and	**110**	92	(83)
Currency translation adjustment and cash flow hedges, net of provision/(benefit) for	**(425)**	13	(17)
Other comprehensive income/(loss)	**(315)**	105	(100)
Comprehensive income	**$ 1,656**	$	$ 2,829

[12] Taken from Target 2014 10-K.

2. Neiman Marcus Corp.

Background: Neiman Marcus Group is a luxury, multi-branded, omni-channel fashion retailer headquartered in Dallas, Texas. The Company operates forty-one Neiman Marcus Stores across the United States and two Bergdorf Goodman stores in Manhattan. The Company also operates thirty Last Call clearance centers and twelve Last Call Studios as well as six CUSP stores. These store operations total more than 6.8 million gross square feet. The Company conducts direct to consumer operations under the Neiman Marcus, Bergdorf Goodman, Last Call, Horchow, CUSP and mytheresa brand names.[13] As of September 19, 2014, Neiman Marcus Group had approximately 16,500 employees.[14] The company ranked 527th in the Fortune 500 for 2014. In the fiscal year ended August 2, 2014, the company earned $4,648 million revenues and $164 million earnings.[15]

On January 10, 2014, Neiman Marcus publicly announced that the company had suffered a data security breach. The forensic reports stated that malicious software (malware) was clandestinely installed on their system and that it attempted to collect or "scrape" payment card data in 77 of the 85 stores from July 16, 2013 to October 30, 2013. The original estimated compromised payment cards were approximately 1,100,000. Later investigation determined that the number of potentially affected payments cards is lower—approximately 350,000. Of the 350,000 payment cards that may have been affected by the malware, Visa, MasterCard and Discover have confirmed to date that approximately 9,200 of those were subsequently used fraudulently elsewhere.[16]

Investigators believe that the Neiman Marcus breach is almost certainly not the work of the same hackers of the Target breach in late 2013.[17] The cybersecurity breach took place despite the fact that Neiman Marcus had employed numerous security defenses (e.g., firewalls, network segmentation, encryption and intrusion detection systems). The malware penetrated Neiman Marcus system was exceedingly sophisticated.[18] Later news report by Bloomberg indicates that the FBI believes a Russian cyber-crime syndicate is behind the attack.[19]

---

[13] See "Corporate Profile" at http://phx.corporate-ir.net/phoenix.zhtml?c=118113&p=irol-homeProfile&t=&id=&, accessed February 27, 2015.
[14] See Neiman Marcus 10-K reports for fiscal year ended on August 02, 2014.
[15] See Fortune 500 2014, at http://fortune.com/fortune500/neiman-marcus-group-ltd-inc-527/, accessed February 27, 2015.
[16] See Neiman Marcus' letter to consumers at http://www.neimanmarcus.com/NM/Security-Info/cat49570732/c.cat, accessed February 27, 2015.
[17] See Bloomberg Business report at http://www.bloomberg.com/bw/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data, accessed February 27, 2015.
[18] In his testimony in the Congressional Hearing on Cybercrime and Privacy on February 04, 2014, Mr. Michael Kingston, Senior Vice President of Neiman Marcus, said: "Its complex, specialized elements helped to explain how the malware had successfully evaded detection, despite all of the security measures we had in place, in at least five different ways. First, the malware was apparently not known to the anti-virus community and had been written to evade anti-virus signatures. Second, the malware erased its tracks by removing the disk file that had caused it to run, even while the program itself was still running in memory –a highly unusual and difficult-to-achieve feature. Third, when the malware scraped and captured card data, it created encrypted output files, so the output files did not exhibit evidence of card-scraping activity –until they were decrypted. Fourth, the malware appeared to have features that were custom-built as a result of reconnaissance efforts within our systems that appear to have been clandestinely

Neiman Marcus responded to the cybersecurity breach in a number of ways. The company hired two computer forensic investigative firms, notified federal law enforcement. After removing of malware from the system, Neiman Marcus communicated to customers via multiple forms (e.g., emails, social media, mass communication outlets, mails), letting them know they would not be liable for fraudulent charges to their accounts, providing free enrollment in a credit monitoring service.[20]

Questions and Answers for Neiman Marcus Group

a. What cybersecurity procedures were in place prior to the actual breach?

"Our security measures included numerous firewalls at the corporate and store level, network segmentation, a customized tokenization tool, numerous encryption methods, an intrusion detection system, a two-factor authentication requirement, and use of industry-standard and centrally-managed enterprise anti-virus software."

-- Mr. Michael R. Kingston, Senior Vice President of Neiman Marcus, February 04, 2014 Congressional Hearing on Cybercrime and Privacy

b. How did the firm identify the cybersecurity breach?

"Tues. Dec.17: We receive a 'CPP report' from MasterCard showing 122 payment cards with confirmed fraud use, suggesting that the "common point of purchase" (CPP) may have been one Neiman Marcus store where these cards had been previously used over a several-month period.

Wed. Dec. 18: We call forensic investigative firms in order to start an investigation, consistent with the card brand protocol. A new CPP report is received showing 74 cards.

Fri. Dec. 20: We hire a leading forensic investigative firm to conduct a thorough investigation. They start immediately. A new CPP report is received showing 26 cards.

Mon. Dec. 23: We notify federal law enforcement. They follow up with us shortly thereafter and we have been working with them since then. A new CPP report is received showing 2,185 cards.

Sun. Dec. 29: The forensic investigation has not turned up any evidence of a data compromise, and we decide to bring on a second leading forensic investigative firm to accelerate the investigation and help us determine whether we have a problem.

---

conducted earlier in 2013. Finally, the malware carefully covered its tracks with a built-in capability that wiped out files evidencing its operation by overwriting them with random data –making forensic detection much more difficult.

[19] See the report at http://www.businessinsider.com/neiman-marcus-cyber-attack-russian-hackers-2014-4, accessed February 27, 2015.

[20] See the testimony of Mr. Michael R. Kingston, Senior Vice President of Neiman Marcus, February 04, 2014 Congressional Hearing on Cybercrime and Privacy; Neiman Marcus' letter to consumers at http://www.neimanmarcus.com/NM/Security-Info/cat4957__0732/c.cat, accessed February 27, 2015; and USA Today report at http://www.usatoday.com/__story/money/personalfinance/2014/01/16/neiman-marcus-credit-breach/4536009/, accessed February 27, 2015.

Wed. Jan. 1: For the first time, the forensic investigators find preliminary indications of malware that may have the capability to 'scrape' or capture payment card data. This is confirmed on January 2, but it remains unknown whether the malware was able to function on our systems."

-- Mr. Michael R. Kingston, Senior Vice President of Neiman Marcus, February 04, 2014 Congressional Hearing on Cybercrime and Privacy

c. What is the estimate of the ultimate cost, in terms of both private costs and externalities, of the cybersecurity breach to the firm and how is that cost derived?

No estimates on externality costs.

"… we incurred costs in fiscal year 2014 associated with this security incident, including legal fees, investigative fees, costs of communications with customers and credit monitoring services. In the future, payment card companies and associations may require us to reimburse them for unauthorized card charges and costs to replace cards and may also impose fines or penalties in connection with the Cyber-Attack, and federal and state enforcement authorities may also impose fines or other remedies against us. We expect to incur additional costs to investigate and remediate the matter in the foreseeable future. Such costs are not currently estimable but could be material to our future operating results.

As described in Note 15 of the Notes to Consolidated Financial Statements in Item 15, the Cyber-Attack has given rise to putative class action litigation on behalf of customers and regulatory investigations. At this point, we are unable to predict the developments in, outcome of, and economic and other consequences of pending or future litigation or government inquiries related to this matter. Any future criminal cyber-attack or data security incident may result in additional regulatory investigations, legal proceedings or liability under laws that protect the privacy of personal information, all of which may damage our reputation and relationships with our customers and adversely affect our business, operating results and financial condition."

"…we incurred approximately $12.6 million of expenses in fiscal year 2014 for costs related to the investigation of the Cyber-Attack, including legal fees, investigative fees, costs of communications with customers and credit monitoring services provided to customers. We expect to incur additional costs to investigate and remediate the Cyber-Attack in the foreseeable future. Such costs are not currently estimable but could be material to our future operating results."

-- Neiman Marcus August 02, 2014 10-K

d. Is there a concerted strategy towards cybersecurity investments in your firm, and, if so, how much does the firm annually invest in cybersecurity activities?

"The Capital Committee assists the Parent Board with ensuring that our information technology strategy and investments are aligned with our overall goals and objectives."

"If our information systems are damaged or cease to function properly, we may have to make a significant investment to fix or replace them, and we may suffer loss of critical data and interruptions or delays in our operations. To keep pace with changing technology, we must

continuously implement new information technology systems as well as enhance our existing systems. Moreover, the successful execution of some of our growth strategies, in particular the expansion of our omni-channel and online capabilities, is dependent on the design and implementation of new systems and technologies and/or the enhancement of existing systems."

Prior to the breach, Neiman Marcus disclosed in its 2013 10-K:

"We also believe capital investments for information technology in our stores, websites, distribution facilities and support functions are necessary to support our business strategies. As a result, we are continually upgrading our information systems to improve efficiency and productivity.

In the past three fiscal years, we have made capital expenditures aggregating $393.5 million related primarily to:

- the construction of a new store in Walnut Creek, California and construction of a distribution facility in Pittston, Pennsylvania;
- e-commerce and technology investments;
- enhancements to merchandising and store systems; and
- the renovation of our main Bergdorf Goodman store on Fifth Avenue in New York City and Neiman Marcus stores in Bal Harbour, Florida and Chicago, Illinois.

Currently, we project gross capital expenditures for fiscal year 2014 to be approximately $190 to $200 million. Net of developer contributions, capital expenditures for fiscal year 2014 are projected to be approximately $170 to $180 million."[21]

After the breach, Neiman Marcus made similar disclosure in its 2014 10-K, but with significant higher amount in capital expenditures:

"We also believe capital investments for information technology in our stores, websites, distribution facilities and support functions are necessary to support our business strategies. As a result, we are continually upgrading our information systems to improve efficiency and productivity.

In the past three fiscal years, we have made capital expenditures aggregating $473.3 million related primarily to:

- the construction of a new store in Walnut Creek, California (opened in fiscal year 2012) and a distribution facility in Pittston, Pennsylvania;
- e-commerce and technology investments;
- enhancements to merchandising and store systems; and
- the renovation of our main Bergdorf Goodman store on Fifth Avenue in New York City and Neiman Marcus stores in Bal Harbour, Florida, Chicago, Illinois and Oak Brook,

[21] Note the investment amount is the total for all capital investments. The current SEC disclosure guidance does not require firms to disclose capital investments on information technology and/or information security. Hence, we are not able to obtain the accurate amounts on these two specific items.

Illinois.

Currently, we project gross capital expenditures for fiscal year 2015 to be approximately $310 to $330 million. Net of developer contributions, capital expenditures for fiscal year 2015 are projected to be approximately $275 to $295 million."

e. Does your firm consider the risks associated with potential cybersecurity breaches, and, if so, how?

Yes, but there's no specificity on how they consider the risk in generally, and in particular, there's no clear indication on how they use the risk to determine the level of investments in cybersecurity activities.

Prior to the breach, Neiman Marcus had a bulletproof disclosure in the 2013 10-K:

"**A material disruption in our information systems could adversely affect our business or results of operations.**

We rely on our information systems to process transactions, summarize our operating results and manage our business. Our information systems are subject to damage or interruption from power outages, computer and telecommunications failures, computer viruses, cyber-attack or other security breaches and catastrophic events such as fires, floods, earthquakes, tornadoes, hurricanes and acts of war or terrorism.

To keep pace with changing technology, we must continuously implement new information technology systems as well as enhance our existing systems. The successful execution of some of our growth strategies is dependent on the design and implementation of new systems and technologies and/or the enhancement of existing systems, in particular the expansion of our omni-channel and online capabilities.

The reliability and capacity of our information systems is critical to our operations and the implementation of our growth initiatives. Any disruptions affecting our information systems, or delays or difficulties in implementing or integrating new systems, could have an adverse effect on our business, in particular our Online operation, and results of operations.

A breach in information privacy could negatively impact our operations.

The protection of our customer, employee and company data is critically important to us. We utilize customer data captured through both our proprietary credit card programs and our online activities. Our customers have a high expectation that we will adequately safeguard and protect their personal information. A significant breach of customer, employee or company data could damage our reputation and relationships with our customers and result in lost revenues, fines and lawsuits."

In 2014, after the cybersecurity breach, Neiman Marcus made detailed discussion on the breach in the 2014 10-K:

"**A breach in information privacy could negatively impact our operations.**

The protection of our customer, employee and company data is critically important to us. We utilize customer data captured through both our proprietary credit card programs and our in-store and online activities. Our customers have a high expectation that we will adequately safeguard and protect their personal information. Despite our security measures, our information technology and infrastructure may be vulnerable to criminal cyber-attacks or security incidents due to employee error, malfeasance or other vulnerabilities. Any such incident could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. In addition, we outsource certain functions, such as customer communication platforms and credit card transaction processing, and these relationships allow for the storage and processing of customer information by third parties, which could result in security breaches impacting our customers.

We discovered in January 2014 that malicious software (malware) was clandestinely installed on our computer systems (the Cyber-Attack). Based on information from our forensic investigation, it appears that the malware actively attempted to collect payment card data from July 16, 2013 through October 30, 2013 at 77 of our 85 stores, on different dates at each store within this time period. During that time period, information from approximately 350,000 customer payment cards could have been potentially collected by the malware.

We are actively cooperating with the U.S. Secret Service in its investigation into the Cyber-Attack. In testimony before Congress in February 2014, a Secret Service official explained that the attack on our systems was exceedingly sophisticated, and was unprecedented in the manner in which it was customized to defeat our defenses and remain undetected. The Secret Service official also testified that we used a robust security plan to protect customer data, but that, given its level of sophistication, the attacker nevertheless succeeded in having malware operate on our systems.

In light of the Cyber-Attack, we have taken steps to further strengthen the security of our computer systems, and continue to assess, maintain and enhance the ongoing effectiveness of our information security systems. Nevertheless, there can be no assurance that we will not suffer a similar criminal attack in the future, that unauthorized parties will not gain access to personal information, or that any such incident will be discovered in a timely way. In particular, the techniques used by criminals to obtain unauthorized access to sensitive data change frequently and often are not recognized until launched against a target; accordingly, we may be unable to anticipate these techniques or implement adequate preventative measures."

f. What, if any, cybersecurity insurance did the company have in place prior to the breach?

No disclosure in SEC filings. No news reports.

g. What sort of cybersecurity related information sharing arrangements did the firm have in place prior to the breach?

No reports on information sharing arrangements. As a matter of fact, when Target started the Retail Cyber Intelligence Sharing Center (R-CISC) after the 2013 breach at Target, Neiman Marcus was not a member.[22]

h. How did the firm respond to the cybersecurity breach (include any changes in the firm's procedures and policies toward cybersecurity as a result of the breach)?

In its letter to consumers, Neiman Marcus stated:[23]

"We are taking a number of steps to contain the situation in all our stores including:

- We have disabled the malware we discovered in the course of our investigation.
- We are working directly with federal law enforcement in its investigation.
- We are conducting a full review of all of our payment card information systems and vulnerability assessment with the payment card brands, our merchant processor, a leading investigations, intelligence and risk management firm, and a leading, payment brand approved forensics firm.
- We are reviewing our intrusion detection systems and firewalls.
- We are reinforcing our security tools.
- We are reviewing and hardening our systems.
- We are modifying our software and security credentials."

In the 2014 10-K report, Neiman Marcus disclosed:

"We are actively cooperating with the U.S. Secret Service in its investigation into the Cyber-Attack."

"In light of the Cyber-Attack, we have taken steps to further strengthen the security of our computer systems, and continue to assess, maintain and enhance the ongoing effectiveness of our information security systems."

Neiman Marcus also hired its first information security officer, Sarah Hendrickson. Hendrickson joined the luxury retailer Nov. 3, 2014 and reports to CIO Michael Kingston.[24]

---

[22] See news report at http://www.slashgear.com/target-other-retailers-join-cyber-intelligence-sharing-co-op-15329218/, accessed at February 27, 2015.
[23] See http://www.neimanmarcus.com/NM/Security-Info/cat49570732/c.cat - 6.
[24] See news report at http://blogs.wsj.com/cio/2014/11/10/neiman-marcus-names-first-chief-information-security-officer/, accessed on February 27, 2015.

i. How did the cybersecurity breach affect the firm's disclosure in financial reports and public announcement?

There has been a significant change in the firm's 10-K (annual report) filed for SEC as a result of the cybersecurity breach. These changes include: a discussion of the data breach in part I, item 1A, risk factor discussion of the 10-K; part I, item 3, legal proceedings; part II, item 6, selected financial data; part II, item 7, management's discussion and analysis of financial condition and results of operations; item 8 financial statements and supplementary data; notes to consolidated financial statements 14, other expenses; notes to consolidated financial statements 15, commitment and contingencies.[25]

[25] Neiman Marcus' earnings in fiscal year 2014 seem to be significantly influenced by the cyber-attack. In its MD&A section of the 2014 10-k report, Neiman Marcus highlighted the following numbers:

	Fiscal year ended	
(in millions)	August 2, 2014 (Combined)	August 3, 2013 (Predecessor)
Specialty Retail Stores	$ 426.9	$ 411.4
Online	160.7	157.7
Corporate expenses	(56.0)	(46.7)
Other expenses	(190.1)	(23.1)
Corporate depreciation/amortization charges	(170.9)	(52.9)
Corporate amortization of inventory step-up	(129.6)	—
Total operating earnings	$ 41.0	$ 446.4

"We incurred other expenses of $190.1 million, or 3.9% of revenues, in fiscal year 2014. These expenses consisted primarily of costs incurred in connection with the Acquisition and costs incurred related to the Cyber-Attack."

Appendix Neiman Marcus Stock Price Chart 2013-2014 (Taken from Yahoo! Finance)

3. RSA

Background: RSA LLC, the Security Division of EMC, provides software and hardware used to protect, monitor, and manage access to computer networks and enterprise software. EMC Corporation (sometimes referred to as EMC^2) is an American multinational corporation that provides Information Technology as a Service, and works to help firms store, manage, and analyze their data (Reuters, 2015).

RSA was named after the initials of its co-founders, Ron Rivest, Adi Shamir, and Len Adleman, developers of public key encryption (Rivest, 1978). Among its products include the SecurID authentication token1, an easy-to-use, convenient, self-contained method for effective user identification (EMC, 2015). RSA is a subsidiary of data storage systems maker EMC (Hoovers, 2015).

In March 2011, RSA acknowledged that "sophisticated hackers launched a spear phishing attack that exploited an Adobe Flash zero-day vulnerability to successfully infiltrate its systems and steal information related to its SecurID products (Moscaritolo, 2011). A spear phishing attack is one that appears to come from someone within the organization, is more likely to be trusted, and mistaken as legitimate. In this instance the attacker sent two different phishing emails with the subject line "2011 Recruitment Plan" over a two-day period, to two small groups of employees.

In this case, one employee retrieved the email from his Junk folder and opened the attachment, which was an Excel spreadsheet entitled "2011 Recruitment plan.xls". The spreadsheet contained a zero-day exploit that installed a backdoor through an existing Adobe Flash vulnerability that injected malicious code into the employee's computer, allowing full access into the machine. The attacker then installed a remote administration tool, which allowed external control of the employee's computer, at which point he used his access to transfer password protected files from the RSA file server to a compromised machine at a hosting provider. These files were subsequently deleted by the attacker from the compromised host, removing evidence of the attack (RSA FraudAction Research Labs, 2011).

Shortly after RSA discovered the attack, the firm issued a warning to its customers that the information stolen could be used to sidestep RSA's security products. However, with this initial admission, the firm provided few details about the true extent of the breach, and did not highlight that with the stolen information the hackers could generate valid SecurID token values to penetrate protected systems (Moscaritolo, 2011).

SecurIDs tokens provide the users with an electronic key for their computers, that use a two-pronged approach to confirm the identity of the system user. This approach could prevent hackers from obtaining a user's passwords, since the SecurID generates new strings of digits every minute. The current string must be used along with a personal identification number access is granted to the network.

However, RSA did not fully disclose the extent of the breach and accompanying vulnerability of their ubiquitous SecurID tokens, used by nation's biggest banks and large technology companies, until June 2011. "Bank of America, JPMorgan Chase, Wells Fargo and Citigroup said they planned to replace the tokens as soon as possible. The banks declined to say how many customers would be affected, although SAP said that most of its 50,000 employees used RSA's

tokens and that it was seeking to replace them all." Although firms made the changes suggested by RSA after their initial notification in March (these included increased monitoring and adding an additional password to the remote log-in process), the vulnerability would require the reprogramming of the tokens (Schwartz & Drew, 2011).

Consequently, on May 21, 2011 several of the nation's defense contractor suffered cyber breaches. The hackers used duplicate SecurID electronic keys, based on the data retrieved from the RSA attack. The only firm to publically acknowledge the attack was the Lockheed Martin Corp, a global security and aerospace company that employs about 112,000 people worldwide, with sales of over $45 billion in 2014 (Finkle, 2011). On Saturday, May 21, 2015, Lockheed Martin issued the following press release.

> *On Saturday, May 21, Lockheed Martin detected a significant and tenacious attack on its information systems network. The company's information security team detected the attack almost immediately, and took aggressive actions to protect all systems and data. As a result of the swift and deliberate actions taken to protect the network and increase IT security, our systems remain secure; no customer, program or employee personal data has been compromised* (Lockheed Martin, 2011).

The statement has some ambiguity, as it states the attack was detected almost immediately, but clearly asserts that there was no breach of any significant data. Lockheed Martin's security professional acted swiftly and disabled all remote access, restricted telecommuters, issued new SecurID tokens, and had all employees reset their passwords (Schwartz M. J., 2011).

Questions and Answers for EMC

a. What cybersecurity procedures were in place prior to the actual breach?

It is not clear what cybersecurity measures were in place at the time of the breach. The firm appeared to be the target of a focused spear phishing attack, and a single employee using poor security practices opened the attachment that contained the malware, which was loaded on the infected computer, providing the hacker access to the infected machine.

b. How did the firm identify the cybersecurity breach?

This attack was detected by RSA's Computer Incident Response Team, while the attack was in progress. In many cases, this type of attack is often not detected for months, and in some cases it's not detected at all; firms learn of the breach from the government. As a result of the early detection, RSA was able to respond fairly quickly and employ countermeasures, unfortunately the damage had already been done (RSA FraudAction Research Labs, 2011).

c. What is the estimate of the ultimate cost, in terms of both private costs and externalities, of the cybersecurity breach to the firm and how is that cost derived?

Based on the impact of the breach the gross margin percentages for the RSA Information Security segment declined to 56.8% in 2011, down from 69.6% in 2010 and 69.2% in 2009 (EMC Corporation, 2012). Additionally, the firm reported that:

In the first quarter of 2011, we incurred and accrued costs associated with investigating the attack, hardening our systems and working with our customers to implement remediation programs. In the second quarter of 2011, we recorded a $66.3 million charge in cost of sales related to the expansion of the customer remediation programs. We expanded our customer remediation programs to respond to heightened customer concerns resulting from press coverage relating to an unsuccessful cyber-attack on one of our defense sector customers, as well as broad media coverage of cyber-attacks on other high profile organizations. At December 31, 2011, we had a remaining reserve of $46.6 million included in accrued liabilities on the consolidated balance sheet. We considered whether additional losses might result from the pending remediation efforts beyond our existing accrual and concluded that no additional material losses related to the remediation efforts are reasonably possible. We expect that the remediation efforts will be substantially completed by the end of the second quarter of 2012 (EMC Corporation, 2012).

d. Is there a concerted strategy towards cybersecurity investments in your firm?

No strategy was identified in the financial reports or the press.

e. Does your firm consider the risks associated with potential cybersecurity breaches, and, if so, how?

In the 2010 10K Item 1a, Risk Factors, the following short write-up for cyber-security breaches was included:

Security breaches could expose us to liability and our reputation and business could suffer.
We retain sensitive data, including intellectual property, books of record and personally identifiable information, in our secure data centers and on our networks. It is critical to our business strategy that our infrastructure remains secure and is perceived by customers and partners to be secure. Despite our security measures, our infrastructure may be vulnerable to attacks by hackers or other disruptive problems. Any such security breach may compromise information stored on our networks. Such an occurrence could negatively affect our reputation as a trusted provider of information infrastructure by adversely affecting the market's perception of the security or reliability of our products or services.

In the 201110K Item 1a, Risk Factors, the write-up for cyber-security breaches was changed to the following, with the changes underlined:

Cybersecurity breaches could expose us to liability, damage our reputation, compromise our ability to conduct business, require us to incur significant costs, or otherwise adversely affect our financial results.

We retain sensitive data, including intellectual property, proprietary business information and personally identifiable information, in our secure data centers and on our networks. We face a number of threats to our data centers and networks of unauthorized access, security breaches and other system disruptions. It is critical to our business strategy that our infrastructure remains secure and is perceived by customers and partners to be secure.

Despite our security measures, our infrastructure may be vulnerable to attacks by hackers or other disruptive problems, such as the sophisticated cyber-attack on our RSA division that we disclosed in March 2011. Any such security breach may compromise information stored on our networks and may result in significant data losses or theft of our, our customers', our business partners' or our employees' intellectual property, proprietary business information or personally identifiable information. In addition, we have outsourced a number of our business functions to third party contractors, and any breach of their security systems could adversely affect us.

A cybersecurity breach could negatively affect our reputation as a trusted provider of information infrastructure by adversely affecting the market's perception of the security or reliability of our products or services. In addition, a cyber-attack could result in other negative consequences, including remediation costs, disruption of internal operations, increased cybersecurity protection costs, lost revenues or litigation.

f. What, if any, cybersecurity insurance did the company have in place prior to the breach?

No disclosure in SEC filings. No news reports.

g. What sort of cybersecurity related information sharing arrangements did the firm have in place prior to the breach?

The EMC Corp., as well as RSA, participates extensively in information sharing organizations. EMC Corp. is a member to the Information Technology Information Sharing and Analysis Center (IT-ISAC, 2015).

RSA also recognized the value of partnering and information sharing of cyber security information and is a member of the Financial Services – Information Sharing and Analysis Center (FS-ISAC). RSA continued its strategic relationship with FS-ISAC and is a member of the FS-ISAC Board of Advisors (FS-ISAC, 2015).

h. How did the firm respond to the cybersecurity breach (include any changes in the firm's procedures and policies toward cybersecurity as a result of the breach)?

Shortly after the breach was discovered EMC Corp. released the following open letter to all of RSA's customers (EMC Corp., 2011).

Open Letter to RSA Customers

Like any large company, EMC experiences and successfully repels multiple cyber-attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber-attack in progress being mounted against RSA.

We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.

We have no evidence that customer security related to other RSA products has been similarly impacted. We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident.

Our first priority is to ensure the security of our customers and their trust. We are committed to applying all necessary resources to give our SecurID customers the tools, processes and support they require to strengthen the security of their IT systems in the face of this incident. Our full support will include a range of RSA and EMC internal resources as well as close engagement with our partner ecosystems and our customers' relevant partners.

We regret any inconvenience or concern that this attack on RSA may cause for customers, and we strongly urge you to follow the steps we've outlined in our SecurCare Online note. APT threats are becoming a significant challenge for all large corporations, and it's a topic I have discussed publicly many times. As appropriate, we will share our experiences from these attacks with our customers, partners and the rest of the security vendor ecosystem and work in concert with these organizations to develop means to better protect all of us from these growing and ever more sophisticated forms of cyber security threat.

Sincerely,
/s/ Art Coviello
Art Coviello
Executive Chairman

As indicated in the letter EMC Corp. took steps to increase security of their cyber systems, although no details were provided.

EMC Corp. also briefed individual customers on how to secure their systems in the aftermath of the breach. However, Coviello did not disclose exactly what information was taken or specifically how it might affect customers. Though, the customer firms were required to sign nondisclosure agreements vowing not to disclose the advice that was provided (Reuters, 2015).

The second phase of this attack took place when the compromised tokens were used to penetrate other firms. Lockheed Martin's IT administrators identified an intrusion in May, 2011. The firm

was forced to shut down its computer systems and disrupt its operations. Lockheed then required its employees to reset its passwords, as well as reissuing SecurID tokens for it 120,000 employee workforce. Other defense contractors, i.e. Northrop Grumman and L3 Communications, also reported security breaches, allegedly associated with RSA's SecurID tokens. As a result, RSA received much criticism over its handling of their original breach, and the issuance of replacement tokens (Hoffman, 2015).

i. How did the cybersecurity breach affect the firm's disclosure in financial reports and public announcement?

The firm's 10K for 2011 (the year of the breach) included a more coverage of the cybersecurity risk, and the impact of the remediation. The risk portion was covered above. The coverage of the loss

2011 10K (EMC Corporation, 2011)

From Page 29

> *The gross margin percentages for the RSA Information Security segment were 56.8%, 69.6% and 69.2% in 2011, 2010 and 2009, respectively. The decrease in the gross margin percentage in 2011 compared to 2010 was due to a decrease in product margins. The decrease in product margins was caused by costs accrued associated with working with our customers to implement remediation programs in the first quarter of 2011 and to the $66.3 charge related to the expansion of the customer remediation programs that we recorded in the second quarter of 2011. We expanded our customer remediation programs in the second quarter of 2011 as a result of the heightened customer concerns resulting from press coverage related to an unsuccessful cyber-attack on one of our defense sector customers, as well as broad media coverage of cyber-attacks on other high profile organizations.*

From Page 79, RSA Special Charge

> *In March 2011, RSA was the target of a sophisticated cyber-attack which resulted in information related to RSA's SecurID products being compromised. In the first quarter of 2011, we incurred and accrued costs associated with investigating the attack, hardening our systems and working with our customers to implement remediation programs. In the second quarter of 2011, we recorded a $66.3 million charge in cost of sales related to the expansion of the customer remediation programs. We expanded our customer remediation programs to respond to heightened customer concerns resulting from press coverage relating to an unsuccessful cyber-attack on one of our defense sector customers, as well as broad media coverage of cyber-attacks on other high profile organizations. At December 31, 2011, we had a remaining reserve of $46.6 million included in accrued liabilities on the consolidated balance sheet. We considered whether additional losses might result from the pending remediation efforts beyond our existing accrual and concluded that no additional material losses related to the remediation efforts are*

reasonably possible. We expect that the remediation efforts will be substantially completed by the end of the second quarter of 2012.

Finally from Page 93

T. Selected Quarterly Financial Data (unaudited)

Quarterly financial data for 2011 and 2010 is as follows (tables in thousands, except per share amounts):

2011	Q1 2011	Q2 2011	Q3 2011	Q4 2011
Revenues	$4,607,618	$4,845,338	$4,980,201	$5,574,431
Gross profit	2,699,051	2,880,287	3,066,265	3,523,339
Net income attributable to EMC Corporation	477,148	546,494	605,649	832,046
Net income per weighted average share, diluted: common shareholders	$ 0.21	$ 0.24	$ 0.27	$ 0.38

2010	Q1 2010	Q2 2010	Q3 2010	Q4 2010
Revenues	$3,890,692	$4,023,497	$4,212,271	$4,888,666
Gross profit	2,218,519	2,359,199	2,486,974	2,966,289
Net income attributable to EMC Corporation	372,704	426,216	472,516	628,559
Net income per weighted average share, diluted: common shareholders	$ 0.17	$ 0.20	$ 0.22	$ 0.29

The second quarter of 2011 includes an after-tax charge related to the expansion of customer remediation programs resulting from a cyber-attack on RSA of $56.2 million or $0.03 per diluted share, as well as an after-tax realized gain on the sale of VMware's strategic investment in Terremark Worldwide, Inc. of $28.9 million or $0.01 per diluted share, net of the related portion of non-controlling interest in VMware. The fourth quarter of 2010 includes a special tax charge related to our tax-related reorganizations of $83.3 million or $0.04 per diluted share.

In spite of the major breach suffered, EMC Corp., did not seem to elaborate on their cybersecurity investments and/or processes.

Conclusion

In the aftermath of this breach, RSA concluded that their security breach was engineered by a nation-state with a goal to ultimately use the information about the SecurID tokens, to use that information to hack into major US defense contractors. The attacker were successful, at least in one attributed case—Lockheed Martin's breach, previously highlighted. But, RSA was slow to provide information (Greene, 2012). "Separately, CNet reported Monday that hackers in China appear to have launched the attacks against Lockheed Martin and two other military suppliers, L-3 Communications and Northrop Grumman" (Quittner, 2011). In the end RSA replaced 40 million SecurID tokens at 30,000 companies, which continue to be used (Quittner, 2011).

References for RSA Case

EMC Corp. (2011). *Form 8K March 17, 2011.* Hopkinton, MA: EMC Corp.

EMC Corporation. (2011). *Form 10-K.* Washington, D.C.: United States Securities and Exchange Commission.

EMC Corporation. (2012). *Form 10-K.* Washington, D.C.: United States Securities and Exchange Commission.

EMC. (2015). *RSA SecurID Hardware Tokens*. Retrieved from EMC: http://www.emc.com/security/rsa-securid/rsa-securid-hardware-tokens.htm

Finkle, J. a.-E. (2011, May 27). *Exclusive: Hackers Breached U.S. Defense Contractors*. Retrieved from Reuters: http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527

FS-ISAC. (2015, March 31). *Affiliates*. Retrieved from Financial Services-Information Sharing and Analysis Center: https://www.fsisac.com/strategic-sponsors-0

Greene, T. (2012, January 19). *Network World.* Retrieved from RSA, unapologetic, looks to move beyond The Breach: http://www.networkworld.com/article/2184921/malware-cybercrime/rsa--unapologetic--looks-to-move-beyond-the-breach.html

Hoffman, S. (2015, March 31). *RSA SecureID Breach Costs EMC $66 Million.* Retrieved from CRN: http://www.crn.com/news/security/231002862/rsa-secureid-breach-costs-emc-66-million.htm

Hoovers. (2015). *RSA Security LLC Company Information*. Retrieved from Hoovers: http://www.hoovers.com/company-information/cs/company-profile.RSA_Security_LLC.ef345dbdf6a59dd7.html

IT-ISAC. (2015, March 31). *IT-ISAC Membership*. Retrieved from The Information Technology - Information Sharing and Analysis Center: http://www.it-isac.org/#!members/c1tsl

Lockheed Martin. (2011, May 28). *Lockheed Martin Customer, Program And Employee Data Secure*. Retrieved from Lockheed Martin: http://www.lockheedmartin.com/us/news/press-releases/2011/may/LockheedMartinCustomerPro.html

Moscaritolo, A. (2011, June 7). *RSA Confirms Lockheed Hack Linked to SecurID Breach*. Retrieved from SC Magazine: http://www.scmagazine.com/rsa-confirms-lockheed-hack-linked-to-securid-breach/article/204744/

Quittner, J. (2011). Token Appreciation. *American Banker , 176* (88), 5.

Reuters. (2015). *EMC Corp Profile*. Retrieved from Reuters: http://www.reuters.com/finance/stocks/companyProfile?rpc=66&symbol=EMC

Rivest, R. S. (1978, February). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* . Vol. 21, No. 2, pp. 120-126.

RSA FraudAction Research Labs. (2011, April 1). *Anatomy of an Attack*. Retrieved from RSA Speaking of Security: https://blogs.rsa.com/anatomy-of-an-attack/

Schwartz, M. J. (2011, May 30). *Lockheed Martin Suffers Massive Cyberattack*. Retrieved from Information Week: Dark Reading: http://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013

Schwartz, N. D., & Drew, C. (2011, June 7). *RSA Faces Angry Users After Breach*. Retrieved from New York Times.

4. JPMorgan Chase & Co.

Background: JPMorgan Chase & Co. is a financial holding company, and ranked as the largest U.S. Bank[26] and the sixth largest bank in the world.[27] JPMorgan Chase employs over 260,000 U.S. employees, making the company the 17th largest employers in the in the nation.[28] The firm has reports four major business segments: Consumer & Community Banking, Corporate & Investment Bank, Commercial Banking, and Asset Management. In 2014, JP Morgan Chase reported income of over $21.7 billion on net assets of over $232.1 billion.[29]

On August 27, 2014, BloombergBusiness reported that JPMorgan Chase, along with for other banks, were breached by hackers.[30] The initial Bloomberg report indicated that the theft involved gigabytes of data that could lead to accounts being drained. On September 10, 2014, JP Morgan Chase reported to its customers via its website, that the firm had not seen any spike in fraud related to the breach.[31] In subsequent SEC filings and other communications, the firm maintained that unusual customer fraud did not increase following the breach. The firm's Form 8-K filed on October 2, 2014, reiterated this claim, but did indicate that computer files containing names, addresses, phone numbers and email addresses for 76 million household and 7 million small businesses had been compromised.[32] Moreover, the October 2, 2014, Form 8-K also indicated account numbers, passwords, user IDs, dates of birth or Social Security numbers remained intact.[33] In the Management's Discussion and Analysis section of the firm's 10-K (annual) report for 2014 (filed with the SEC on February 24, 2015), JPMorgan Chase made the same claim and added that the cybersecurity breach had no material adverse effect on the firm's operations. [34]

The initial Bloomberg report of breach indicated that "the way the criminals navigated through elaborate layers of security indicates a degree of skill beyond an ordinary hacker" and that the FBI was "investigating whether Russian hackers attacked JPMorgan and at least one other bank in retaliation for sanctions on the country over its involvement in the Ukraine military conflict."[35] Also, in August 27, 2014, *The New York Times* reported, "Security experts said the hackers chose to pursue account information, not disruption, which is the earmark of state-

---

[26] See http://en.wikipedia.org/wiki/List_of_largest_banks_in_the_United_States, accessed March 16, 2015.
[27] See http://en.wikipedia.org/wiki/List_of_largest_banks, accessed March 16, 2015.
[28] See http://en.wikipedia.org/wiki/List_of_largest_employers_in_the_United_States, accessed March 16, 2015.
[29] See their 10K Annual Report fro 2014, filed on February 24, 2015 and available at http://investor.shareholder.com/jpmorganchase/secfiling.cfm?filingID=19617-15-272, accessed March 16, 2015
[30] See http://www.bloomberg.com/news/articles/2014-08-27/customer-data-said-at-risk-for-jpmorgan-and-4-more-banks, accessed March 17, 2015.
[31] See the firm's September 12, 2014, Form 8-K, available at http://investor.shareholder.com/JPMorganChase/secfiling.cfm?filingID=1193125-14-339482, accessed March 17, 2015.
[32] See http://investor.shareholder.com/JPMorganChase/secfiling.cfm?filingID=1193125-14-362173, accused March 17, 2015.
[33] See http://investor.shareholder.com/JPMorganChase/secfiling.cfm?filingID=1193125-14-362173 , accessed March 17, 2015.
[34] See http://files.shareholder.com/downloads/ONE/4109756056x0xS19617-15-272/19617/filing.pdf, page 142, accessed on March 18, 2015.
[35] Bloomberg, 2014-08-27, op. cit.

sponsored attacks."[36] A September 12, 2014 *New York Times* story reported that more than 90 of JP Morgan Chase's servers were attacked in a hack that began in June and was not detected until late July, and that, in addition to customer information, the hackers obtained a list of software applications used by the bank.[37] The theft of the list of the banks software applications was troubling in that it left open the hackers would use this information to find vulnerabilities in the software as an opening to future, and perhaps more damaging, attacks to the bank. The *Times* story also advanced the theory that the sophistication of the attack "may have involved some coordination or assistance from a foreign government," with Russia being a prime suspect.[38] The same *Times* article insinuated that employee turnover among JP Morgan Chase's security team, including the spring departure of the bank's chief information security officer who was not replaced until after the attack was already under way, may have been a contributing factor to the success of the attack. The story indicated, however, "that the bank was able to stop the hackers before they could siphon customer accounts."[39] An October 2014 *New York Times* story, while again raising the possibility that the breach may have been sponsored by Russia, mentioned that the officials from the Treasury Department, the Secret Service and the FBI were all involved with investigating the breach[40].

The presumption that the summer 2014 cyber-attack on JPMorgan Chase was a sophisticated state sponsored attack has recently been challenged. According to a December 22rd *New York Times* story[41], of JP Morgan Chase failed to update a server with a dual password scheme that would allow two-factor authentication may. Such a double authentication system, standard in the industry, would have prevented hackers from gaining access to their computer systems by the use of stolen credential for a JPMorgan employee. The *Times* story also pointed out that the attack did not involve the use of a sophisticated zero day attack (i.e., targeting a previously unknown vulnerability in software) or use the type of destructive malware used in the Sony attack. According to the article, "the F.B.I. officially rule out the Russian government as a culprit" by mid-October 2014.[42] The article also noted that the National Security Agency (NSA) was also involved with the breach investigation, given JPMorgan Chase's leading position in banking and finance, an industry designated by NSA as a critical infrastructure industry.

On March 15, 2015, the *New York Times* reported that criminal charges would soon be filed against alleged perpetrators of the JPMorgan Chase cybersecurity breach.[43] The article suggested that the suspects lived in a country having an extradition treaty with the United States, and thus would rule out that they are Russians.

---

[36] See http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0, accessed March 18, 2015.
[37] See http://www.nytimes.com/2014/09/13/technology/after-breach-jpmorgan-still-seeks-to-determine-extent-of-attack.html, accessed, March 18, 2015.
[38] New York Times.com 2014/09/13, ibid.
[39] New York Times.com 2014/09/13, ibid.
[40] See, http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/, accessed March 18, 2015.
[41] See, http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/, accessed March 18, 2015.
[42] New York Times.com 2014/12/22, ibid.
[43] See http://www.nytimes.com/2015/03/16/business/dealbook/authorities-closing-in-on-hackers-who-stole-data-from-jpmorgan-chase.html, accessed March 18, 2015

Questions and Answers for JPMorgan Chase

a. What cybersecurity procedures were in place prior to the actual breach?

Although the specific procedures used by JPMorgan Chase prior to the breach have not been identified, it is clear from the letter to shareholders by the CEO Jamie Dimon published in the 2013 Annual Report, April 9, 2014 (prior to the breach) that the firm was very concerned with cybersecurity. That letter contained a special section with the title "CYBERSECURITY UPDATE," in which Dimon stated that cybersecurity was a "critical priority of the entire company" and that the company would be spending "$250 million annually with approximately 1,000 people focused on the effort."[44]

b. How did the firm identify the cybersecurity breach?

According to the New York Times published dated October 31, 2014, Hold Security, a security consulting company, discovered the breach in July 2014. [45] The attack was thought to have begun at the website for the JPMorgan Chase Corporate Challenge, where the breach allowed "hackers to pose as the race website operator and intercept traffic, such as race participants' login credentials."[46] As reported in the October 3, 2014 New York Times story, the JPMorgan's security team were then able to block the attackers from stealing the most sensitive information about customers.[47]

c. What is the estimate of the ultimate cost, in terms of both private costs and externalities, of the cybersecurity breach to the firm and how is that cost derived?

In his April 8, 2015 letter to shareholders in the company's 2014 Annual Report (10K), the CEO Jamie Damien states (pp. 41), "Importantly, cyber-attacks to date have not resulted in material harm to our clients or customers and have not had a material adverse impact on our results or operations."[48]

There is no indication that the firm considers externalities.

---

[44] See page 22 of the firm;s 2013 annual report, available at http://files.shareholder.com/downloads/ONE/4109756056x0x742266/2bd13119-52d2-4d78-9d85-a433141c21ae/01-2013AR_FULL_09.pdf

[45] Goldstein, M and N. Perlroth, October 31, 2014, "Luck Played Role in Discovery of Data Breach at JPMorgan Affecting Millions," *New York Times*, accessed online on April 23, 2015 at http://dealbook.nytimes.com/2014/10/31/discovery-of-jpmorgan-cyberattack-aided-by-company-that-runs-race-website-for-bank/

[46] New York Times.com 2014/10/13, ibid.

[47] Goldstein, M, N. Perlroth, and D. Sanger, October 3, 2014, "Hackers' Attack Cracked 10 Financial Firms in Major Assoult," *New York Times*, accessed online on April 23, 2015 at http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/

[48] See http://files.shareholder.com/downloads/ONE/4109756056x0x820066/f831cad9-f0d8-4efc-9b68-f18ea184a1e8/ JPMC-2014-AnnualReport.pdf

d. Is there a concerted strategy towards cybersecurity investments in your firm, and, if so, how much does the firm annually invest in cybersecurity activities?

"J.P. Morgan Chase & Co. Chairman and Chief Executive James Dimon said the bank would double spending on cybersecurity over the next five years, his first public remarks following the data breach that hit the nation's largest bank this summer….

He said J.P. Morgan over the next four to five years was likely to double its spending on cybersecurity from $250 million annually in 2014. 'We have to be vigilant,' he said, adding that issues around cybersecurity 'will happen for a long time.'"[49]

The December 22, 2014 *New York Times* story reported that, after the breach, "JPMorgan set up a 'business control group' of about a dozen technology and cybersecurity executives to assess tha fallout and to prevent hackers form breaching its network in the future."[50]

In his April 8, 2015 letter to shareholders in the company's 2014 Annual Report (10K), the CEO Jamie Damien states (pp. 41-42):

> Over the next two years, we will increase our cybersecurity spend by nearly 80% and enhance our cyber defense capabilities with robust testing, advanced analytics and improved technology coverage. We will strengthen our partnerships with government agencies to understand the full spectrum of cyber risks in the environment and increase our response capabilities.[51]

e. Does your firm consider the risks associated with potential cybersecurity breaches, and, if so, how?

In his April 8, 2015 letter to shareholders in the company's 2014 Annual Report (10K) , the CEO Jamie Damien devotes an entire section, titled "Cybersecurity remains a top priority," to this question. In the Management's discussion and analysis section (pp. 142-143), there is a long section titled "Cybersecurity." Cybersecurity risks are considered at the very top of the firm as, "The Board of Directors and the Audit Committee are regularly apprised regarding the cybersecurity policies and practices of the Firm as well as the Firm's efforts regarding this attack and other significant cybersecurity events."

f. What, if any, cybersecurity insurance did the company have in place prior to the breach?

None indicated.

---

[49] From http://www.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976, October 10, 2014, accessed March 18, 2015

[50] New York Times.com 2014/12/22, ibid.

[51] See http://files.shareholder.com/downloads/ONE/4109756056x0x820066/f831cad9-f0d8-4efc-9b68-f18ea184a1e8/JPMC-2014-AnnualReport.pdf

g. What sort of cybersecurity related information sharing arrangements did the firm have in place prior to the breach?

Like most major banks, JPMorgan Chase belonged to the Financial Information Sharing and Analysis Center (F-ISAC).

h. How did the firm respond to the cybersecurity breach (include any changes in the firm's procedures and policies toward cybersecurity as a result of the breach)?

See the answer to question d.

i. How did the cybersecurity breach affect the firm's disclosure in financial reports and public announcement?

The 2014 breach resulted in additional communications to the public via 8K reports and statements to the press. Overall, however, the breach appears to have had little impact on the firm's disclosures concerning cybersecurity threats and the firm's actions to counter such threats. The likely reason is that JPMorgan appeared to be keenly aware of the growing cybersecurity risks prior to the breach. In the firm's 2013 10K, released February 20, 2014 (prior to the breach), the word "breach" appeared 24 times and the word "cyber" appeared 12 times. In the firm's 2014 10K (covering the year of the breach), released February 24, 2015, the word "breach" appears 22 times and the word "cyber" appears 6 times. As noted in the answer to question number 3 above, the 2014 10K reports that the breach had no material effect on the firm. [52]

[52]See http://investor.shareholder.com/jpmorganchase/secfiling.cfm?filingID=19617-14-289 for the 2013 10K and http://files.shareholder.com/downloads/ONE/4109756056x0xS19617-15-272/19617/filing.pdf for the 2014 10K.

Appendix

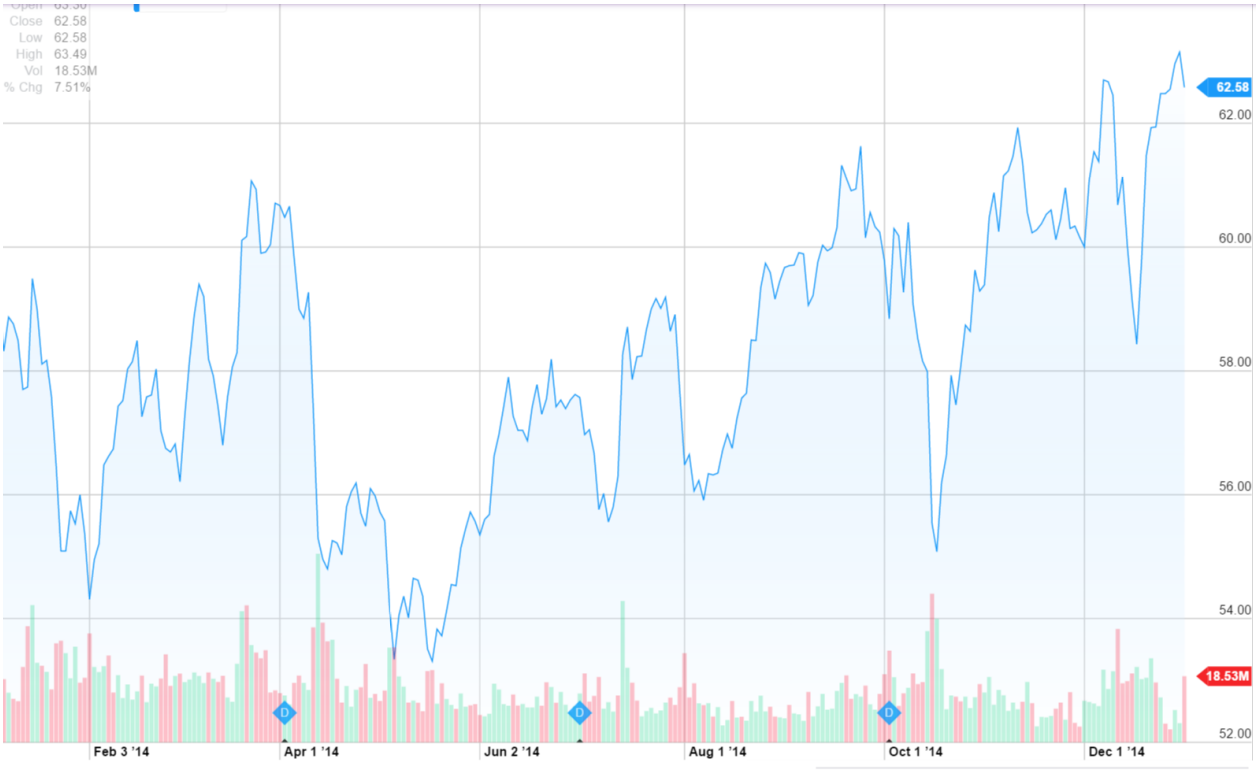
Comparative Income Statements

Income Statement — Get Income Statement for:

Period Ending	Dec 31, 2014	Dec 31, 2013	Dec 31, 2012
Total Revenue	**91,066,000**	**96,381,000**	**93,646,000**
Cost of Revenue	-	-	-
Gross Profit	**91,066,000**	**96,381,000**	**93,646,000**
Operating Expenses			
Research Development	-	-	-
Selling General and Administrative	61,274,000	70,467,000	64,729,000
Non Recurring	-	-	-
Others	3,139,000	225,000	3,385,000
Total Operating Expenses	-	-	-
Operating Income or Loss	**29,792,000**	**25,914,000**	**28,917,000**
Income from Continuing Operations			
Total Other Income/Expenses Net	-	-	-
Earnings Before Interest And Taxes	37,689,000	35,264,000	39,960,000
Interest Expense	7,897,000	9,350,000	11,043,000
Income Before Tax	29,792,000	25,914,000	28,917,000
Income Tax Expense	8,030,000	7,991,000	7,633,000
Minority Interest	-	-	-
Net Income From Continuing Ops	21,762,000	17,923,000	21,284,000
Non-recurring Events			
Discontinued Operations	-	-	-
Extraordinary Items	-	-	-
Effect Of Accounting Changes	-	-	-
Other Items	-	-	-
Net Income	**21,762,000**	**17,923,000**	**21,284,000**
Preferred Stock And Other Adjustments	-	-	-
Net Income Applicable To Common Shares	**20,093,000**	**16,593,000**	**19,877,000**

FromYahoo.Finance – see http://finance.yahoo.com/q/is?s=JPM+Income+Statement&annual

Appendix JP Morgan Stock Price Chart for 2014[53] (Taken from Yahoo! Finance)



[53] Taken from Yahoo!Finance, see http://finance.yahoo.com/echarts?s=JPM+Interactive#{"customRangeStart":1388552400,"customRangeEnd":1420002000,"range":"custom"}

IV. SURVEY

A. Methodology

A questionnaire-based survey (see subsection B of this section of the Report) for the survey instrument) was also part of the research conducted under the DHS contract. The data collected from the survey is being used to statistically test the final hypotheses. Prior to mailing the questionnaire-based survey, a pilot study was conducted to assess the survey instruments reliability and validity. The questionnaire was appropriately revised based on the results of the pilot study and the results of the case studies and interviews with senior executives discussed elsewhere in the Report. We sent approximately 2,000 questionnaires to the CFOs and CIOs of roughly 1,600 major organizations from a variety of industries (with a focus on industries that are critical to the U.S. national infrastructure). After about 8 weeks, a second mailing of the survey was resent to the non-respondents. After taking into consideration the returned questionnaires where the executives had either left the companies or the firms had moved, we had a usable response rate of approximately 10% to our questionnaire study (i.e., 171 usable responses).

Preliminary analysis of the data gathered from the survey respondents was performed, and the results of that analysis are presented in Subsection C of this Report. The analysis included calculation of descriptive statistics on the perceived difficulty of determining the benefits and riskiness associated with cybersecurity investments. Multivariate statistical techniques were also used to test the hypotheses noted previously in this Report. Subsection C of this section of the Report contains the above noted analysis.

B. Survey Instrument

DEPARTMENT OF HOMELAND SECURITY (DHS) SPONSORED SURVEY

on

CYBERSECURITY INVESTMENTS BY FIRMS IN THE PRIVATE SECTOR

Project PI: Dr. Lawrence A. Gordon, EY Professor of Managerial Accounting and Information Assurance, RH Smith School of Business, University of Maryland (UMD).

Co-PI: Dr. Martin P. Loeb, Deloitte & Touche Faculty Fellow and Chair of Accounting and Information Assurance, RH Smith School of Business, UMD.

Co-PI: Mr. William Lucyshyn, Director of Research and Senior Research Scholar, Center for Public Policy and Private Enterprise, School of Public Policy, UMD.

The following survey is being conducted by investigators at the University of Maryland, as part of a larger study being sponsored by the Department of Homeland Security (DHS) concerning expenditures decisions related to cybersecurity activities by firms in the private sector of the U.S. economy. It should take no longer than 20 minutes to complete. The underlying objective of this research is to understand the challenges associated with making cybersecurity investments in the private sector, and to recommend policies for facilitating the appropriate level of such investments. Your organization was selected because it operates in one of the critical infrastructure industries (e.g., telecommunications, defense, energy, health care, and transportation).

Your participation is voluntary and all information provided in response to this survey will be recorded in a completely anonymous fashion, and only the aggregate results will be reported. The individual data points will only be seen by the researchers analyzing the survey responses. All of your responses to this questionnaire will be held in strict confidence. Furthermore, postmarked envelopes used to return this questionnaire will be separated and destroyed prior to data entry. Neither you, your business unit, nor your firm, will ever be associated with responses to this questionnaire.

Once completed, this research will be made publicly available. This research is intended to assist organizations to make better cybersecurity investment decisions. By completing this survey, you are indicating that you are at least 18 years of age, you have read this consent information, and your questions have been answered, and you voluntarily agree to participate in this research study. Enclosed is a postage-paid envelope for your return of this survey. If you have misplaced this envelope, send your completed survey, without a return address, to:

Dr. Lawrence A. Gordon
University of Maryland
Robert H. Smith School of Business
College Park, Maryland 20742

DEPARTMENT OF HOMELAND SECURITY (DHS) SPONSORED SURVEY

on

CYBERSECURITY INVESTMENTS BY FIRMS IN THE PRIVATE SECTOR

A. Which of the below categories describes your organization's principal operations (circle the correct answer/s):

Consulting
Defense
Education
Energy
Financial Services
Health Care
Information Technology
Law Enforcement
Legal
Manufacturing
Retail
Telecommunications
Transportation
Utilities
Other (please specify)

B. How many employees are in your organization (circle the correct answer)?

1-99
100-499
500-1,499
1,500-9,999
10,000-49,999
50,000 or more

C. What is your organization's approximate gross annual revenue (circle the correct answer)?

Under $10 million
$10 million to $99 million
$100 to $1 billion
Over $1 billion

D. Which of the below titles best describes your position within your organization (circle the correct answer)?

CEO (Chief Executive Officer)
CFO (Chief Financial Officer)
CIO (Chief Information Officer)
CSO (Chief Security Officer)
Chief Privacy Officer
Security Officer
Systems Administrator
Other (please specify)

E. Approximately what portion of your firm's IT budget is devoted to cybersecurity related activities (circle the correct answer)?

1-2%	12-15%
3-5%	16-20%
6-8%	Greater than 20%
9-11%	

F. For the following set of statements, indicate your level of agreement/disagreement by circling the number provided to the right of the statement. All answers should be in the context of the organization in which you work.

	Strongly Disagree						Strongly Agree
1. Decisions regarding cybersecurity expenditures are made based on a comparison of the expected benefits resulting from defrayed costs associated with cybersecurity breaches.	1	2	3	4	5	6	7
2. Deriving the expected benefits from cybersecurity expenditures is a relatively straightforward process.	1	2	3	4	5	6	7
3. The expected benefits from cybersecurity expenditures are based largely on the expected cost avoidance/savings associated with preventing cybersecurity breaches.	1	2	3	4	5	6	7
4. The expected benefits from cybersecurity expenditures take into consideration the potential competitive advantage derived from strong cybersecurity within your organization.	1	2	3	4	5	6	7
5. The externalities (i.e., spill-over costs to other organizations that in no way affect your organization) are considered in decisions regarding cybersecurity expenditures.	1	2	3	4	5	6	7
6. My organization is actively involved in sharing information regarding our cybersecurity activities.	1	2	3	4	5	6	7
7. My organization would likely share much more information concerning our cybersecurity activities if the government could guarantee limited liability associated with any information shared.	1	2	3	4	5	6	7
8. The likelihood (or probability) that a cybersecurity breach will occur in my organization is extremely difficult to estimate.	1	2	3	4	5	6	7
9. It is a straightforward process to estimate the future dollar value of losses associated with:	Strongly Disagree						Strongly Agree
a. costs of detecting future cybersecurity breaches	1	2	3	4	5	6	7
b. costs of correcting future cybersecurity breaches	1	2	3	4	5	6	7
c. potential lost revenue due to future cybersecurity breaches	1	2	3	4	5	6	7
d. potential liability resulting from future cybersecurity breaches	1	2	3	4	5	6	7
10. My organization usually decides on major cybersecurity investments based on some form of net present value or return on investment.	1	2	3	4	5	6	7

11. The following federal government incentives would encourage my organization to spend more than is currently the case on cybersecurity activities:	Strongly Disagree						Strongly Agree
a. Tax incentives	1	2	3	4	5	6	7
b. Cost sharing	1	2	3	4	5	6	7
c. Grants	1	2	3	4	5	6	7
d. Technical assistance	1	2	3	4	5	6	7
e. Priority government contracting	1	2	3	4	5	6	7
f. Expedited security clearance process	1	2	3	4	5	6	7
g. Public recognition	1	2	3	4	5	6	7
h. Regulation	1	2	3	4	5	6	7
i. Information Sharing	1	2	3	4	5	6	7
j. Other (Specify) _____	1	2	3	4	5	6	7
12. Cybersecurity breaches in my organization are more often due to insider threats or carelessness than external threats.	1	2	3	4	5	6	7
13. A critical determinant of the actual expenditures on cybersecurity activities in my organization is whether or not a major cybersecurity breach has recently occurred in my firm.	1	2	3	4	5	6	7
14. A critical determinant of the actual expenditures on cybersecurity activities in my organization is whether or not a high visibility cybersecurity breach recently occurred in other firms.	1	2	3	4	5	6	7
15. The 2011 SEC Disclosure Guidance on Cybersecurity Risks and Cyber Incidents has increased my organization's focus on cybersecurity related activities.	1	2	3	4	5	6	7
16. Cybersecurity is an important component of my organization's approach to the internal controls of financial reporting systems.	1	2	3	4	5	6	7
17. In determining the risk associated with cybersecurity breaches, my organization considers the expected value of the loss.	1	2	3	4	5	6	7
18. In determining the risk associated with cybersecurity breaches, my organization considers the largest potential loss.	1	2	3	4	5	6	7
19. My organization has insurance that covers, at least in part, the costs associated with cybersecurity breaches.	1	2	3	4	5	6	7
Other comments (attach additional sheets if required):							

C. Preliminary Results

A preliminary analysis of the 171 usable returned surveys, utilizing descriptive statistics, as well as univariate and multivariate statistical tests, yielded some interesting results. While many of the results were not surprising, a number of new insights were obtained.

Our analysis began by examining the responses to parts A-E of the survey (see pages 119-120), and preparing five Figures to characterize the firms sampled, the positions of personnel completing the survey, and an estimate of the proportion of IT budgets that are used for cybersecurity activities.

Figure 1 illustrates the distribution of industries covered by the survey. One can readily see that nearly two thirds of the respondents were in Financial Services, Health Care, or Manufacturing.

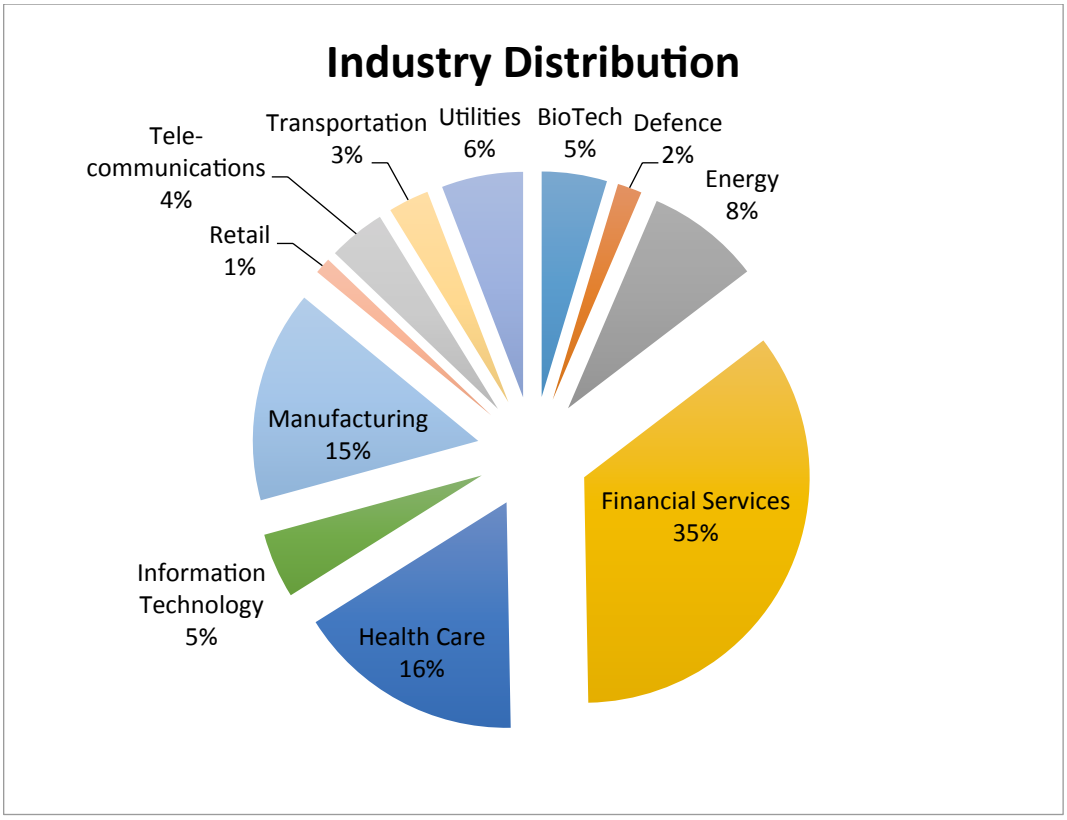


Figure 1: Industry Distribution of Respondents' Firms

Figures 2 and 3 illustrate the size, as measured by headcount and revenue, of the firms responding to the survey. As shown in Figure 2, about 48% of the respondents reported that their firms had less than 500 employees, and 18% had 10,000 or more employees. Turning to firm revenue (Figure 3), one sees that about 40% of the respondents reported that their firms had revenues of less than $100 million and 33% generated revenue of over $1 billion.

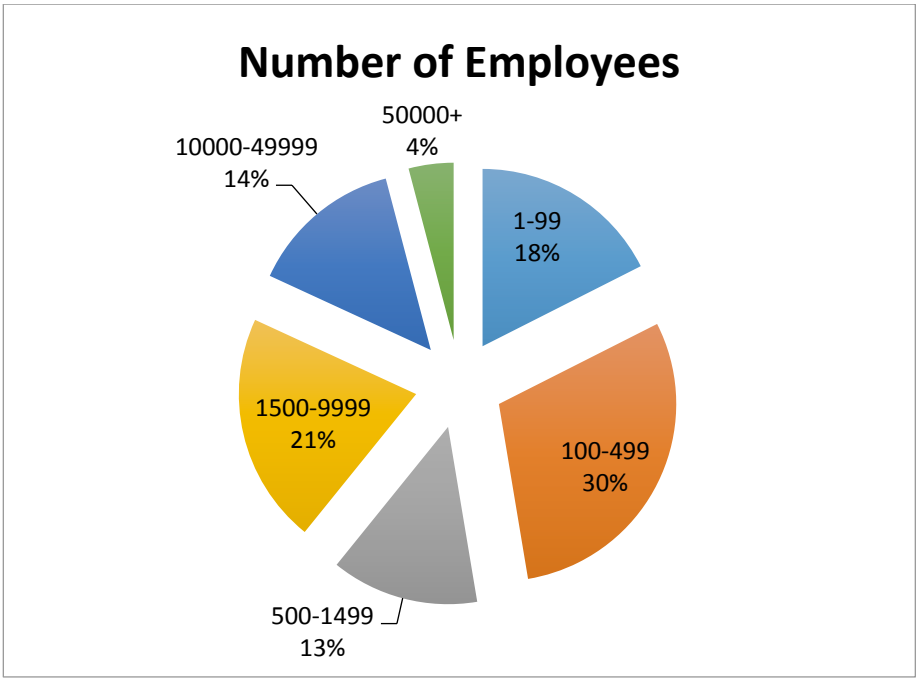


Figure 2: Number of Employees of Respondents' Firms

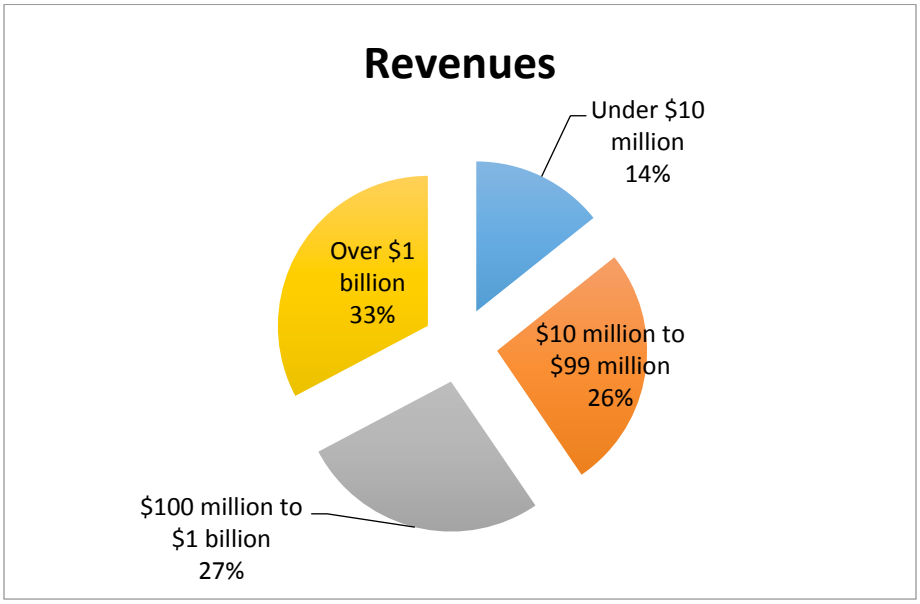


Figure 3: Revenue Distribution of Respondents' Firms

Figure 4 illustrates that about 45% of the respondents were Chief Financial Officers (CFOs) and about 39% of the respondents held the titles of Chief Information Officer, Chief Security Officer, or Chief Information Security Officer.

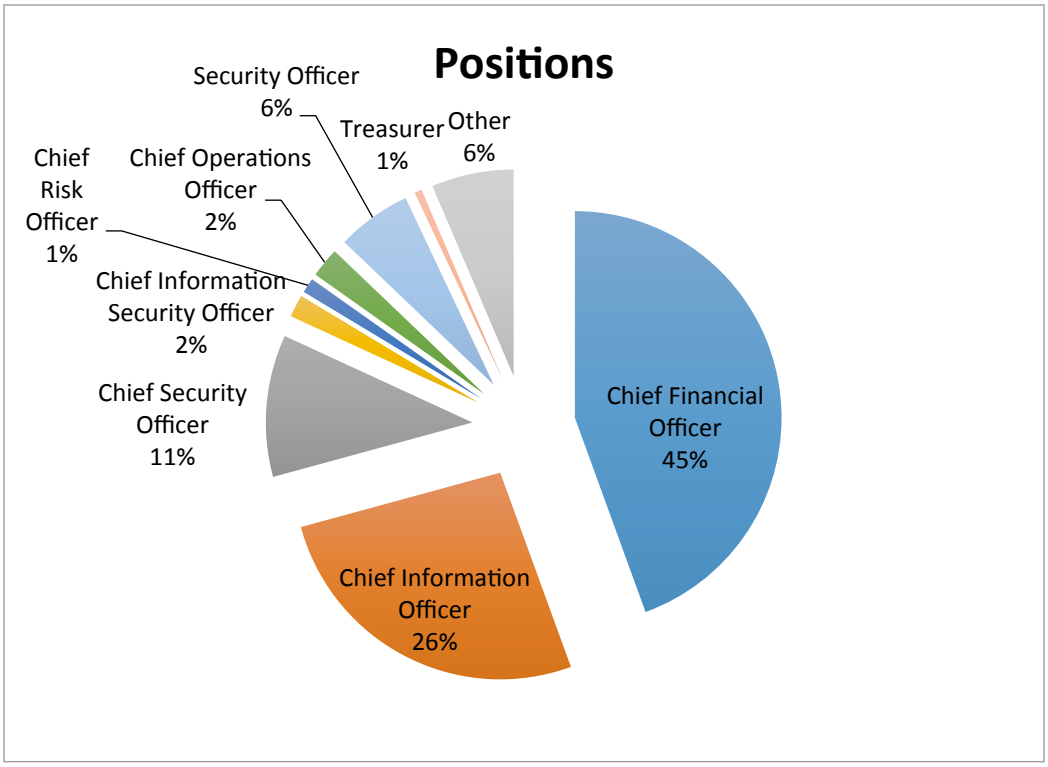


Figure 4: Job Titles of Respondents

Figure 5 illustrates that of the number of the respondents answering question E, more than 50 (or about 32 %) reported that their firms devoted 3-5% of their IT budgets to cybersecurity. A slightly larger number of respondents (about a third of respondents) reported that their firms devoted more than 9% of their IT budgets to cybersecurity.

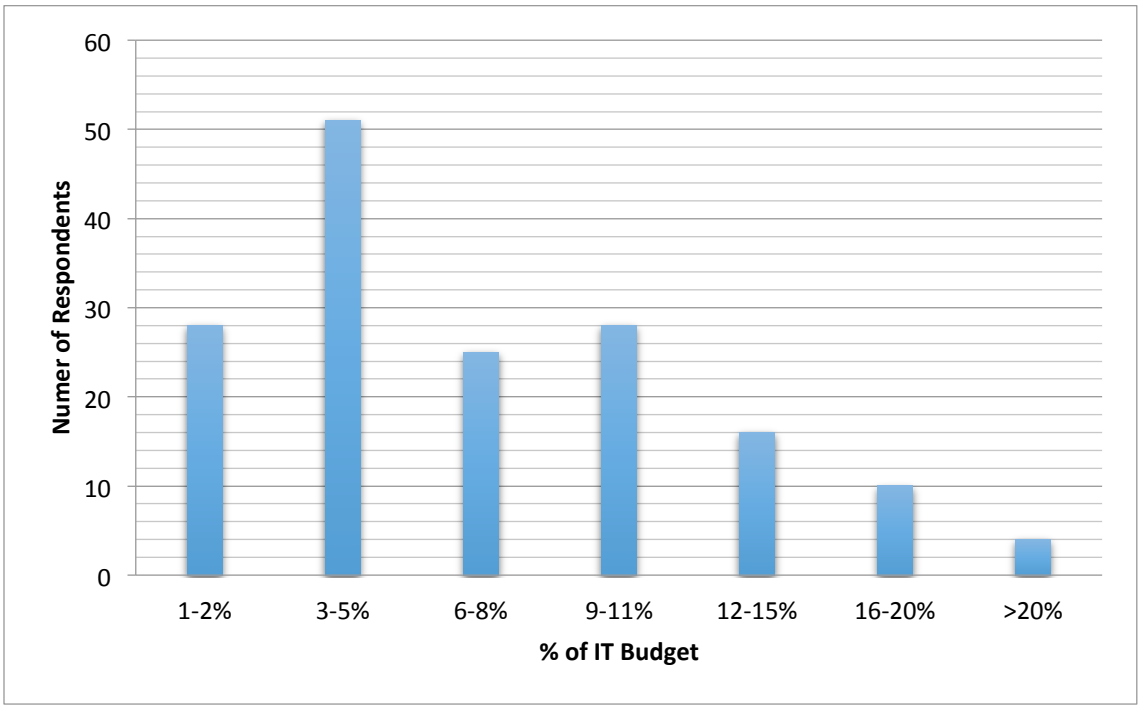


Figure 5: Percentage of IT Budget Devoted to Cybersecurity of Respondents' Firm

After the analysis characterizing the sample, we examined how firm size, industry, and the respondents' positions (CFO vs. non-CFO) affected the responses (extent of agreement) with the statements given in the 19 sections provided in part III of the survey (see pages 121-122). Figures 6-11 illustrate the analysis that focused on the effect of firm size (measured by firm revenues) on consideration of externalities (Figure 6), on information sharing (Figure 7), on the difficulty/ease of estimating the potential costs of cybersecurity breaches (Figure 8), on how the firm would respond, in terms of increased information sharing, to limiting the firm's liability (Figure 9), and how the respondents perceived their firms would react, in terms of increased spending on cybersecurity, to six specified possible government incentives (Figure 10).

Figure 6 illustrates the finding that respondents were neutral (i.e., the overall averaged response 3.5) with respect to the statement that their firms considered externalities in making cybersecurity funding decisions. Figure 6 also illustrates that consideration of externalities increases (but is still low) as the size firm size increases.

Average Scores to Survey Questions Based on Firm Revenue

(Strongly Disagree = 1; Strongly Agree = 7)

Survey Question F5. The externalities (i.e., spill-over costs to other organizations that in no way affect your organization) are considered in decisions regarding cybersecurity expenditures.

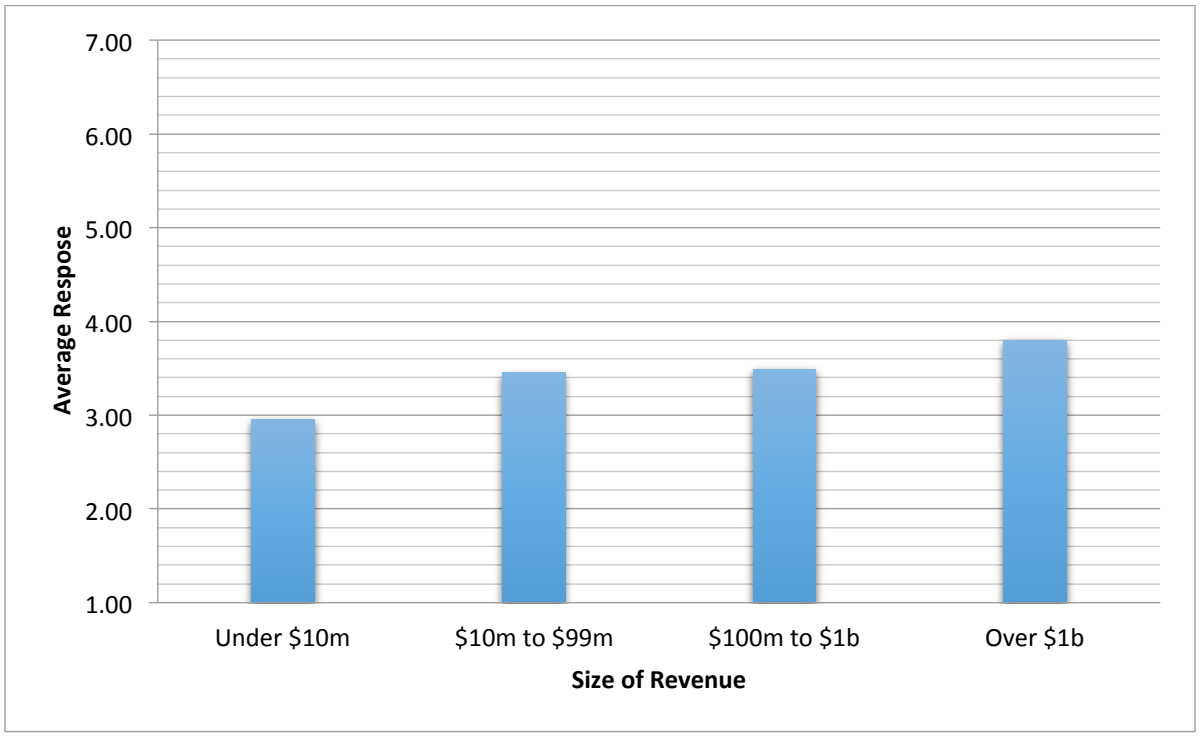


Figure 6: Average Response to Externalities Question (F5) by Size of Revenue of Respondents' Firms

Figure 7 provides evidence of the common perception that larger firms are more actively involved in sharing cybersecurity related information than are smaller firms. While Figure 7 illustrates the relationship between firm size and involvement in information sharing, the relationship was statistically confirmed using ordered logistic regression.

Average Scores to Survey Questions Based on Firm Revenue
(Strongly Disagree = 1; Strongly Agree = 7)

Survey Question F6. My organization is actively involved in sharing information regarding our cybersecurity activities.

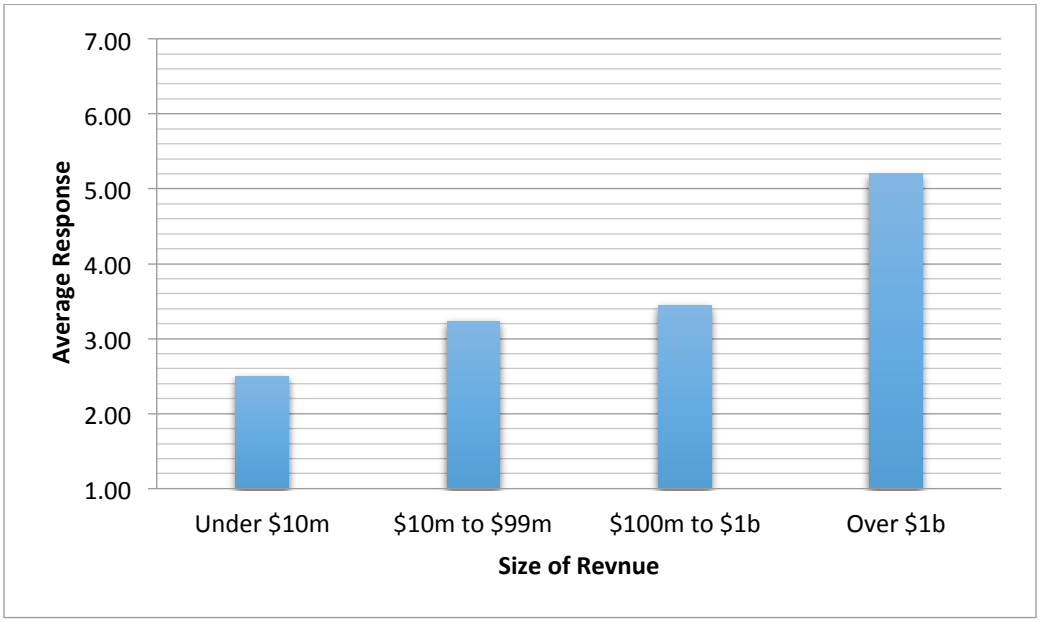


Figure 7: Average Response to Information Sharing Question (F6) by Size of Revenue of Respondents' Firms

Survey question F9, sought to address the degree of difficulty respondents perceived in their firm's ability to estimate various costs associated with future potential cybersecurity breaches. The types of cybersecurity breach costs addressed were the future (a) costs of detection, (b) costs of correction, (c) lost revenue, and (d) the liability costs. Respondents, on average, indicated estimating each of these cost was not straightforward (i.e., the average degree of agreement by respondents with the statement in question F9 was found to be less than 3.5 for each of the four types of breach costs). This is illustrated in Figure 8, and provides confirmatory evidence that estimating costs of breaches is far from straightforward.

Average Scores to Survey Questions Based on Firm Revenue

(Strongly Disagree = 1; Strongly Agree = 7)

Survey Question F9. It is a straightforward process to estimate the future dollar value of losses associated with:

a. costs of detecting future cybersecurity breaches
b. costs of correcting future cybersecurity breaches
c. potential lost revenue due to future cybersecurity breaches
d. potential liability due to future cybersecurity breaches

Figure 8: Average Response to Questions on Ease of Estimating Costs if Breached (F9) by Size of Revenue of Respondents' Firms

Figure 9 illustrates that respondents believe that their firms would share more cybersecurity information if the government could guarantee that their liability from shared information was limited. Figure 9 illustrates that the impact of limiting liability is more pronounced, the larger is the firm.

Average Scores to Survey Questions Based on Firm Revenue

(Strongly Disagree = 1; Strongly Agree = 7)

Survey Question F7. My organization would likely share much more information concerning our cybersecurity activities if the government could guarantee limited liability associated with any information shared.

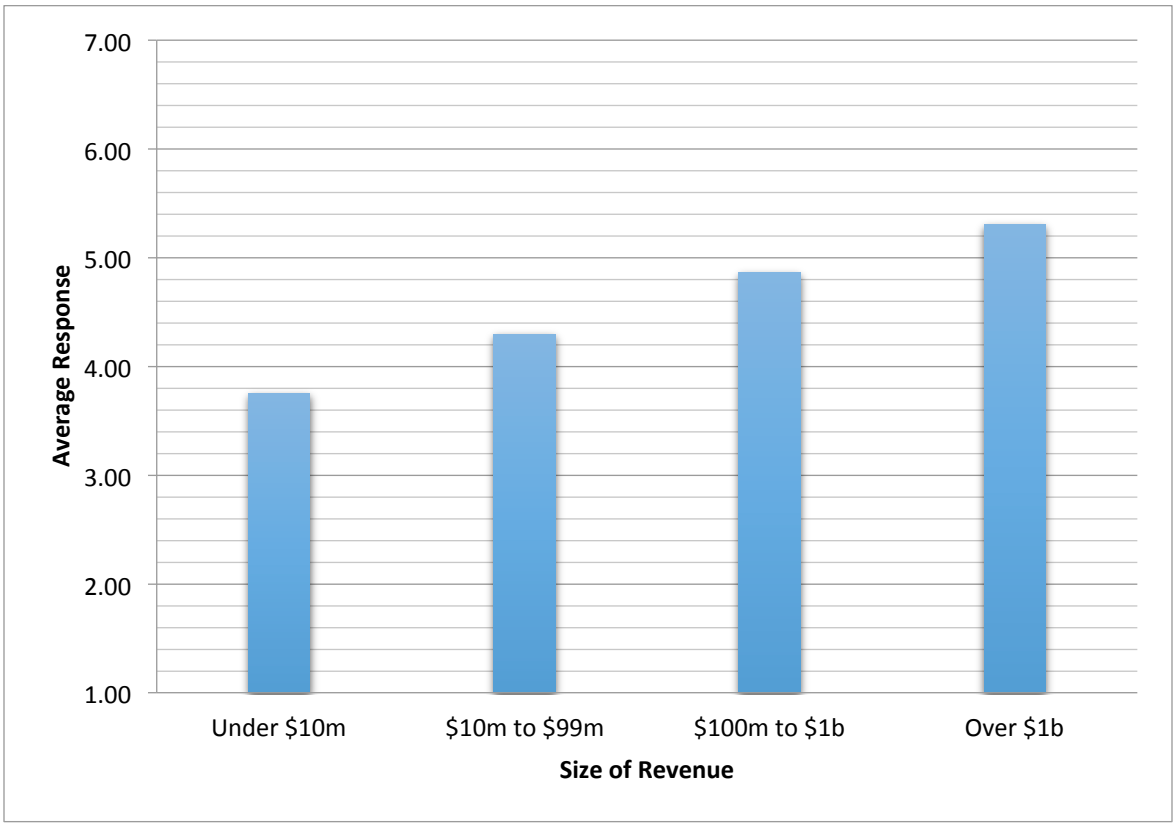


Figure 9 Average Response to Limited Liability Question (F7) by Size of Revenue of Respondents' Firms

Question F11 of the survey aimed to gauge a respondent's perception of the effectiveness of various possible government incentive programs on their firm's spending on cybersecurity. Figure 10 illustrates that tax incentives, cost sharing incentives, and grants are perceived to be useful in increasing cybersecurity spending by private firms of all sizes. The respondents from all firms with revenues of at least $10 million, also perceive that if the government provided technical assistance, the firms would increase their cybersecurity funding. Furthermore, irrespective of firm size, respondents believe that there would be little effect on their firm's cybersecurity spending from: (1) priority government contracting, (2) expedited security clearance policies (3) and public recognition.

Average Scores to Survey Questions Based on Firm Revenue

(Strongly Disagree = 1; Strongly Agree = 7)

Survey Question F11. The following federal government incentives would encourage my organization to spend more than is currently the case on cybersecurity activities:

a. Tax incentives
b. Cost sharing
c. Grants
d. Technical assistance
e. Priority government contracting
f. Expedited security clearance process
g. Public recognition
h. Regulation
i. Information sharing

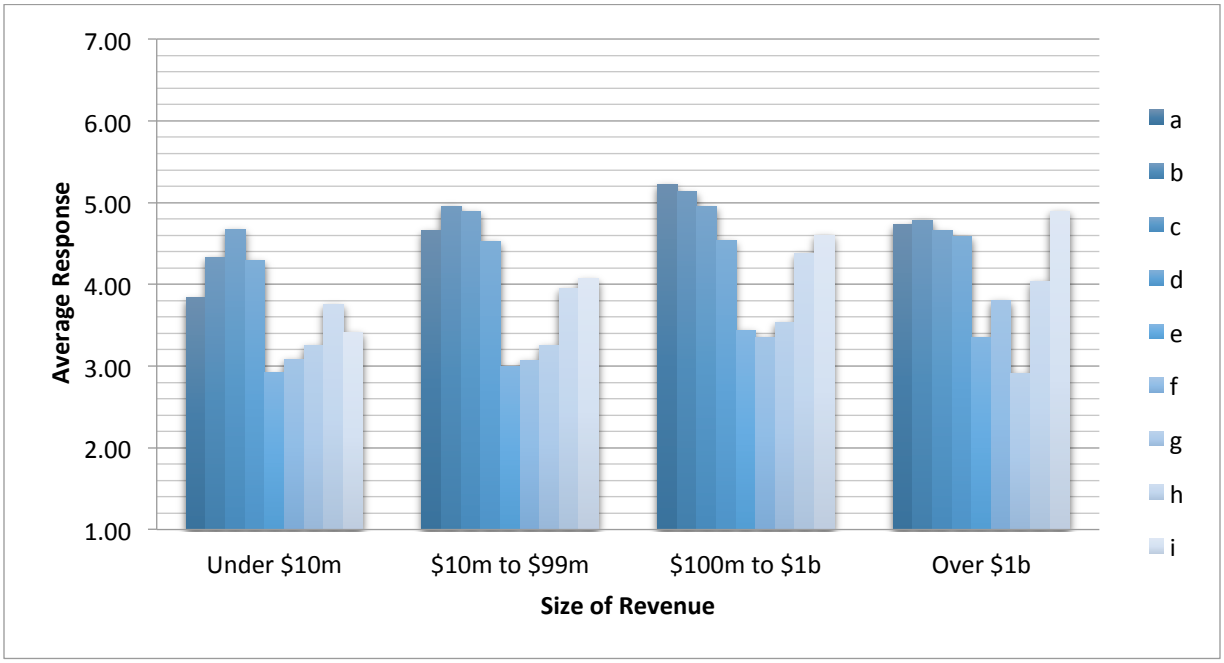


Figure 10 Average Response to Questions on Incentives (F11) by Size of Revenue of Respondents' Firms

In addition to the analysis previously presented, we compared the mean responses to the 19 questions in part F of the survey CFOs versus non-CFOs. We found some interesting and statistically significant results. The responses from CFOs were significantly more conservative, in the sense that:

a. CFOs feel more difficult to estimate the likelihood of future cybersecurity breaches and losses related to these breaches. This suggests that in addition to improved availability of data on breaches and their costs, CISO's may need more training in developing and presenting their business case for future cybersecurity investments.
b. CFOs state their firms are less involved in information sharing and are less likely to share more information, even if limited liability were guaranteed.
c. CFOs were more reserved in estimating the probable effectiveness of suggested incentives.

Next, we used ordered logistic regression to explore the relationship between the size of the respondents' firms and their forecasted reactions to various possible government incentives. We found that compared to smaller firms, larger firms perceive more value from tax incentives, expediting the security clearance process, and information sharing as incentives to increase cybersecurity investments. We also used ordered logistic regression to examine the drivers of the percentage of IT funds devoted to cybersecurity activities. We found that:

a. If firms believe cybersecurity is an important component of internal control, they are more likely to devote a higher percentage of IT budget to cybersecurity.
b. Larger firms (in terms of sales) tend to spend a smaller percentage of their IT budget on cybersecurity related activities.
c. Whether or not a major cybersecurity breach has occurred in an organization has an impact of the percentage of the IT budget spent on cybersecurity related activities.
d. If firms have cybersecurity insurance, they are more likely to devote a higher percentage of IT budget to cybersecurity (presumably due to the cost of the insurance).
e. If firms consider the potential competitive advantage derived from strong cybersecurity in cybersecurity investment decisions, they are more likely to devote a higher percentage of IT budget to cybersecurity.

Following is a list summarizing the primary results of our preliminary analysis:

1. Larger firms are more actively involved in information sharing than are smaller firms.
2. Firms, particularly the larger firms, are likely to share more information concerning cybersecurity activities if limited liability is guaranteed.
3. In general, the value of incentives tends to be associated with firm size.
4. All firms, regardless of their size or industry, find it difficult to estimate the future dollar value of losses associated with cybersecurity breaches.
5. Of six possible incentives designed to motivate firms to increase their spending on cybersecurity activities, respondents indicated that the top three incentives (in terms of likely effectiveness) would be the incentives associated with cost sharing, grants, and tax incentives.

6. Government incentives related to expediting the security clearance process, providing technical assistance, and information sharing were perceived to do little to motivate firms to spend more on cybersecurity activities.
7. Priority government contracting for firms that meet some cybersecurity standard was also perceived to do little to motivate an increase in spending on cybersecurity activities.
8. Chief Financial Officers (CFOs) are less optimistic than Chief Information Officers (or Chief Information Security Officers) when it comes to estimating their ability to anticipate cybersecurity breaches and the costs of such breaches.
9. Based on multivariate analysis, it appears that the factors which are the most significant determinants of the percentage of an organizations IT expenditures devoted to cybersecurity activities are: (a) the degree to which cybersecurity is viewed as an important component of the organization's internal control of financial reporting systems, (b) the size of the organization, and (c) whether or not a major cybersecurity breach has occurred in an organization.
10. Firms having cybersecurity insurance are more likely to devote a higher percentage of IT budget to cybersecurity.
11. Firms that believe they can gain a competitive advantage via stronger cybersecurity are more likely to devote a higher percentage of their IT budget to cybersecurity activities.

D. Articles in Progress and Forthcoming Presentations

The preliminary results discussed above, plus additional sophisticated statistical analyses of the data collected from the survey respondents, will form the basis of several articles being written for publication in various journals. One such article will focus on a multivariate analysis of the determinants of the portion of the IT budget that firms spend on cybersecurity related activities. This article is being written for an academic journal (e.g., *Journal of Computer Security*).

A second article, being written for a professional/practitioner oriented journal (e.g., *Communications of the ACM*), will focus on the role of incentives in facilitating information sharing. A third article being written (again, for a professional/practitioner oriented journal) will focus on the role of incentives for encouraging cybersecurity investments.

Besides the above noted articles, as well as other articles that will likely be written based on the data collected from the survey respondents, we also plan on presenting the results of the theoretical and empirical findings from this research project at several additional (i.e., additional to those presentations mentioned in the next Section of this Report) conferences, forums, and workshops over the next year. We will, of course, acknowledge the sponsors of this research in all such papers and presentations.

V. SUMMARY OF OTHER SUPPORTING ACTIVITIES

In addition to writing papers, we disseminated the results of our research projects via a variety of presentations at various conferences, workshops, and forums. The results of this research project also provided direct input to two new courses being offered at the University of Maryland (UMD) at College Park. A listing of these presentations and a brief description of these new courses are provided below.

A. Presentations at Conferences/Workshop/Forums

06/05/2015	London School of Economics Cybersecurity and Entrepreneurship Presentation
05/27/2015	Participated in NIST workshop on the "Economic Incentives for Safer and Privacy Friendly Smart Cities"
05/19/2015	Atlantic Council's Meeting on "The Economic Mechanics of Cyber Risk"
05/18/2015	IBM/Smith School Business (Cybersecurity) Analytics 2015 Annual Workshop
04/13/2015	Netherlands' National Cyber Security Center (NCSC) 2015 Annual Meeting
03/03/2015	Presentation to JPM Chase Executives at Maryland Cybersecurity Center
02/10/2015	Luncheon talk to International Security and Economic Policy (ISEP) group from UMD's School of Public Policy
02/02/2015	Met with Tom Finan, DHS to discuss his work with us (i.e., there may be some way to link up with his work on Cybersecurity Insurance with our work).
01/14/2015	Forum on "Financial Information Systems and Cybersecurity: A Public Policy Perspective"
12/17/2014	DHS 2014 R&D Showcase and Technical Workshop
10/31/2014	Johns Hopkins University - Senior Executive Cybersecurity Conference
06/25/2014	DHS Workshop at Penn State University
06/10/2014	Maryland Cybersecurity Center's Symposium
04/11/2014	Board of Regents Meeting, University System of Maryland
01/08/2014	Forum on "Financial Information Systems and Cybersecurity: A Public Policy Perspective"
09/2013	DHS CSD-PI Meeting 2013

B. New UMD University Courses

- "**Accounting and Economic Aspects of Cybersecurity**"

Developed and offered (spring, 2014) the above noted undergraduate course for UMD's Honors College. This course is part of UMD's new prestigious Living-Learning ACES (Advanced Cybersecurity Experience for Students) Honors program. Northrop Grumman is major business partner in this program. The majority of the students currently in the program are computer science and electrical and computer engineering majors. However, there are also numerous students from such departments as math, business, and psychology in the program. This course is being offered again in the fall of 2015.

- **"Research on Accounting and Economic Aspects of Cybersecurity"**

Developed the above noted Master's level course for Smith School of Business students. The plan is to offer this course for the first time in either 2015 or 2016.

VI. PLAN FOR ESTABLISHING A CYBERSECURITY ECONOMICS LAB (CySEL)

A. Executive Summary

This document provides a recommendation for the establishment of a Cybersecurity Economics Lab (CySEL) to study, and ultimately increase, cybersecurity investments by private sector firms. Given the recognition that the problem of increasing cybersecurity is as one of designing appropriate economic incentives as it is of designing technological solutions, this proposal outlines the scope and potential benefits of establishing a Cybersecurity Economics Lab. The proposed CySEL would: (1) conduct economic experiments in a controlled environment to gain insights on the effectiveness of various proposed incentives and regulations to spur private investment in cybersecurity, (2) develop and maintain a database on cybersecurity investments and costs (including the costs of cybersecurity breaches) for longitudinal (as well as cross-sectional) economic studies, and (3) provide education and training for CISOs and other managers in the private sector to enhance their ability to compete effectively for scarce internal cybersecurity funding (thereby, providing a boost to cybersecurity investments in the private sector). This document proposes initial seed funding by DHS for two year at a level of $300,000 per year, followed by a third year of shared funding with industry sponsors. It is proposed that the initial funding period would conclude at the end of three years, and DHS would then make the continue/discontinue decision.

B. Utility to the Department of Homeland Security

There is continued concern that profit-oriented firms in the private sector may not be investing a sufficient amount in cybersecurity. In addition, it is unclear as to whether or not the funds invested in cyber security activities are being allocated in an efficient manner. Given that roughly 85% of the United States' critical infrastructure assets are owned by private sector firms, both of these concerns are important for National Security reasons as well as for firm-level success. The results of this research should prove useful to DHS to help mitigate incomplete and asymmetric information barriers that hamper efficient security decision-making. In addition, the results of this research should prove useful to DHS in terms of guiding the development and evaluation of policies and regulations related to the security of the nation's infrastructure.

C. Technical Approach

Cybersecurity activities within organizations are, in large part, the result of difficult economic decisions associated with the allocation of scarce resources. Determining how much to invest in cybersecurity, and how to allocate that investment, are part of the resource allocation process. Deriving the requisite economic incentives to motivate individual behavior to make decisions in favor of increasing investments in cybersecurity activities is also part of the economic conundrum associated with cybersecurity. As Michael Daniel (2014, p. 2), special assistant to President Obama and Cybersecurity Coordinator at the White House, stated in his discussion of why the cybersecurity problems are so hard to resolve: "So the logical conclusion has to be that we don't fully understand the economics and psychology of cybersecurity … Technology cannot compensate for bad business practices in cybersecurity."

The importance of economics to an organization's cybersecurity activities has been recognized for some time (e.g., see, Anderson; 2001, Gordon and Loeb, 2001, 2006; Gordon, Loeb, and Lucyshyn, 2003a,b; Gordon, Loeb and Sohail, 2003; Anderson and Moore, 2009; Gordon, Loeb, and Zhou, 2011; Gordon, Loeb, Lucyshyn and Zhou, 2015). The U.S. Department of Homeland Security (DHS) recognized the importance of economics to cybersecurity activities in its BAA 1103 Call for research proposals by including TTA – Cyber Economics as one of its issues of concern. As a result of BAA 1103, an economics-based research project being supported by DHS is entitled "Challenges to Cybersecurity Investments." The investigators on this project are Drs. Lawrence A. Gordon (Principal Investigator), Martin P. Loeb (Co- Principal Investigator), and Mr. William Lucyshyn (Co- Principal Investigator). One outgrowth of the Gordon, Loeb, Lucyshyn project is the recommendation for the establishment of a Cybersecurity Economics Lab (CySEL). The overall mission of CySEL would be to conduct three fundamental activities that improve our understanding and use of economic principles in addressing cybersecurity-related problems. These activities, their specific objectives and their benefits, are discussed below.

I. Conduct laboratory-based economic studies (i.e., experimental economics) concerned with assessing the impact of economic incentives on various cybersecurity-related issues.

There are many challenges for firms in determining their level of investment in cybersecurity. These challenges include the need for the capability to develop and test alternative policies for improving cybersecurity related investments, examining their effectiveness and gauging any unintended consequences. For example, cybersecurity investments (or their lack thereof) have spillover effects, including the free-rider and tragedy of commons effects, on other firms. As one firm invests more in cybersecurity, there may be positive spillover effects (i.e., what economists call externalities) that will likely reduce the incentives for other firms to invest in cybersecurity. Poor cybersecurity by one firm will likely have negative spillover effects on other firms. Unfortunately, there are currently few incentives for firms to increase their investments in cybersecurity to mitigate these negative spillover effects. As a result of these externalities, there is a need for policies that create incentives and/or regulations to encourage private sector firms to increase their investments in cybersecurity.

Objective: The objective of this activity is to conduct various economic studies, in a laboratory setting (i.e., laboratory experiment), that have important implications for facilitating cybersecurity investments by private sector firms in the critical infrastructure industries. These studies would address such issues as the impact of various economic incentives on: (1) increasing cybersecurity investments, taking into consideration externalities, as well as private costs, (2) encouraging the sharing of cybersecurity-related information among firms, (3) embedding stronger security during the production of products, and (4) reducing the negative behavior of hackers. The work conducted in carrying out this objective would be coordinated with the activities of the DETER Project, which is funded by the Department of Homeland Security, the National Security Agency and the Department of Defense (see: http://deter-project.org/about_deter_project). The work conducted in carrying out this objective would also be coordinated with the SRI field-based research experiments, being funded by DHS, that are concerned with assessing how economic and behavioral incentives can be used to improve cybersecurity.

Benefits: Addressing the impact of economic incentives on some issues, such as the four noted above, is difficult to assess via a typical empirical study. A key reason for this difficulty is that there are a variety of factors that determine the actual way these issues are ultimately handled within a given firm. These factors include, but are not limited to, the way a firm generates its revenues (e.g., via the Internet or through actual brick-n-motor stores), the degree to which technology effects the way a firm interacts with its supply chain partners, the size of a firm, the time frame during which the incentives are considered, the firm's industry, etc. Thus, in a study based on an actual empirical setting, assessing the impact of economic incentives on the various issues noted above can only be done on an *ex post* basis, using crude approximations for statistical analysis purposes. More to the point, such an approach rarely allows for the proper control of all the factors that impact the effect of economic incentives. A well-designed laboratory experiment, however, permits control of these factors in a manner that facilitates sound statistical tests, thereby providing valuable insight into the anticipated effect of implementing an incentive.

II. Develop, maintain and analyze, over an extended period of time, a database on cybersecurity investments, the types of major cybersecurity breaches, and the cost of cybersecurity breaches.

A key challenge related to making and evaluating cybersecurity-related investments by firms in the private sector is related to the general opaqueness of the level of cybersecurity investments of firms, and the associated level and costs of breaches incurred by firms. This lack of data also makes it difficult to establish an efficient insurance market. Thus, there is a need to develop a database (e.g. on the actual level of cybersecurity investments by firms, as well as the breaches incurred by these firms) that could be maintained by a trusted third party to assist with the evaluation of investment decisions. This database would also track, over time, the effects of cybersecurity investments on the level and costs of cybersecurity breaches within specific firms

Objective: The objective of this activity is to gather and analyze data relevant to the way private sector firms make cybersecurity investment decisions, the amount these firms invest in cybersecurity activities, the way such firms respond to cybersecurity breaches, and the cost of cybersecurity breaches. In assessing the cost of cybersecurity breaches on firms, externalities, as well as private costs, will be considered. The analysis of data collected in carrying out this objective would include the use of visual and data analytics techniques, and would draw upon the activities of the Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA), which is a Department of Homeland Security University Center of Academic Excellence (see: http://www.ccicada.org/about-ccicada/). This part of the proposed research project would also provide data that would be useful in facilitating other on-going research projects being supported by DHS. For example, the data collected related to cybersecurity breaches and investments could be combined with the malicious activities data being collected by Dr. Mingyan Liu to examine whether organizations actually improve their cybersecurity after breaches, as well as to examine the relationship between cybersecurity investments and malicious activities.

Benefits: Data on the process firms follow in making cybersecurity investment decisions and the amount firms spend on such investments is sparse. In addition, there is no organized collection of data that tracks the way firms actually respond to cybersecurity breaches over time. Some of this

data (e.g., a firm's reaction to a major cybersecurity breach) is available via various public sources (e.g., SEC filings by firms listed on the various stock exchanges), although codification of such data does not currently exist. In contrast, other parts of the required data (e.g., cybersecurity investments) are not available via public sources. A concerted effort at collecting and analyzing the above noted data, over an extended period of time (i.e., data of a longitudinal nature), would be extremely beneficial to facilitating research that could help us understand the best way to address some of the vexing problems associated with cybersecurity risk management. In addition, collecting and analyzing data related to the types of major cybersecurity breaches, and the cost of such breaches, over time, would help in assessing the impact of the 2011 SEC Disclosure Guidance on Cybersecurity Risks and Incidents and the NIST Framework for Improving Critical Infrastructure Cybersecurity.

III. Provide education and training for private sector firms on "making the business case" for cybersecurity investments.

There is a need to assist executives in firms (especially CIOs and CISOs) in developing a capability to conduct the analysis necessary to make the appropriate level of investment in their organization's cybersecurity activities. This need is especially prevalent in new start-up firms, as well as small to medium size firms, that do not have the funds to hire individuals with the requisite training to conduct cost benefit-analysis related to cybersecurity investments.

Objective: The objective of this activity is to assist those individuals within organizations (e.g., CIOs and CISOs), who are responsible for securing funding for cybersecurity related activities, to more effectively compete for funds within their organizations. Particular emphasis would be placed on assisting new, small, and medium size firms, although large firms would be welcome to participate in this activity.

Benefits: Cybersecurity-related investments need to compete for scarce resources in a manner similar to the way other potential investments (e.g., an investment in a new product line) need to compete for resources. In other words, organizations have finite resources and the amount of funds requested for a variety of investment opportunities far exceeds the amount of funds available. Thus, a fundamental approach to allocating funds to the competing requests is via cost-benefit analysis, or what practitioners often call "making the business case." Unfortunately, many individuals responsible for securing funds for cybersecurity activities are not well versed in the techniques associated with cost-benefit analysis. This situation puts requests for investments related to cybersecurity investments at a competitive disadvantage within many firms (relative to other investment requests within the same firm). In other words, CIOs and CISOs need to be able to understand the language of communication used by those individuals (CFOs) controlling organizational funds. By offering training on how to "make the business case" for cybersecurity investments, the above described situation can be at least partially addressed.

D. Budget and Schedule

The plan would be for U.S. Department of Homeland Security (DHS) to provide funding for the first two years, at a rate of $300,000 for each year. DHS Funding for a third year, at a rate of

$150,000, would be conditioned on having the $150,000 matched by industry sponsors. At the end of the third year DHS would have the option to continue, or discontinue, funding CySEL.

References for Section VI

Anderson, Ross. "Why information security is hard-an economic perspective." In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, IEEE, (2001), pp. 358-365.

Anderson, Ross, and Tyler Moore. "The economics of information security." *Science* 314, no. 5799 (2006), pp. 610-613.

Daniel, M. "Remarks By Special Assistant To The President and White House Cybersecurity Coordinator," Gartner Security and Risk Management Conference, June 23, 2014 (see: http://insidecybersecurity.com/iwpfile.html?file=jul2014%2Fcs07022014_michael_daniel_remarks.pdf).

Gordon, L.A. and M.P. Loeb, "The economics of information security investment." *ACM Transactions on Information System Security* 5, no. 4 (2002), pp. 438-457.

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

Gordon, L.A., M.P. Loeb, and W. Lucyshyn, "Information security expenditures and real options: A wait-and-see approach," *Computer Security Journal* 19, no. 2 (2003,a), pp. 1-7.

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

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and T. Sohail. "The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities." *Journal of Accounting and Public Policy* 25, no. 5 (2006), pp. 503-530.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, "The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective, *Journal of Accounting and Public Policy*, (forthcoming 2015).

Gordon, L.A., M.P. Loeb and L. Zhou, "The Impact of Information Security Breaches: Has there been a Downward Shift in Cost?" *Journal of Computer Security* 19, no. 1 (2011), pp. 33-56.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model," *Journal of Information Security* 6, no. 1(2015), pp. 24-30.

VII. RECOMMENDATIONS AND CONCLUDING REMARKS

A. General Recommendations:

Several general recommendations based on the findings from this entire research project are provided below. These recommendations are as follows:

1. Improve SOX and the SEC disclosure guidance

The simple act of increased disclosure would likely improve cybersecurity practices. That is, a more effective utilization of SOX and the SEC Disclosure Guidance could go a long way toward resolving the problem associated with underinvestment in cybersecurity activities by a large subset of private sector firms. For example, if it were made clear that major cybersecurity breaches or other cybersecurity related weaknesses represent material weaknesses in the internal control systems of firms, many firms would quickly realize the value of increasing their investments in cybersecurity as a means of reducing the likelihood of such cybersecurity breaches (and, in turn, reducing the likelihood that their auditors cite a cybersecurity related material weakness in their internal control system).

2. Continue to work to improve information sharing

Information sharing has the potential for reducing the uncertainty surrounding cybersecurity investment decisions. Reducing this uncertainty should encourage timelier, and more cost efficient, cybersecurity investments. Information sharing is also likely to lessen the common tendency by firms to wait for a major cybersecurity breach before investing significant incremental funds for cybersecurity activities. However, as pointed out elsewhere in this Report, there is a need for some sort of limited liability protection associated with the cybersecurity related information that is shared. Thus, limiting the liability for firms that share information should be vigorously pursued.

3. Develop incentives for firms to increase the level of cybersecurity investment

There is clear evidence that firms in the private sector are not investing enough into cybersecurity, especially when externalities are considered. However, there is a great deal of private sector resistance to greater federal regulation of private sector cybersecurity implementation. The general belief is that such regulation would not be successful for a variety of reasons; principal among those is the speed with which the technology and threats evolve. To date, the current administration has resisted regulatory initiatives in favor of voluntary-based incentives. The National Institute of Standards and Technology (NIST) released a voluntary framework, developed collaboratively with industry. This framework, which has thus far generally received favorable feedback, consists of cybersecurity guidelines and practices to promote the protection of critical infrastructure assets. One approach is to offer private sector firms cybersecurity investment incentives that are linked to the NIST framework.

Although incentives to encourage larger cybersecurity investments by private sector firms clearly have the potential to be beneficial, our research indicates that the effectiveness of such incentives

depends on the specific incentive and on other firm-related factors (e.g., whether or not a firm is able and willing to increase its spending on cybersecurity activities). Of course, as noted below and elsewhere in this Report, evaluation of incentives would be facilitated by laboratory experiments, and the collection of significantly more data.

4. Encourage the development of a vibrant cybersecurity insurance market

Cyber insurance policies could provide a partial market-based solution for developing and monitoring cybersecurity standards. Moreover, insurance companies could incentivize other behaviors. For example, insurance companies could provide discounts to firms actively engaged in information sharing. There are, however, several concerns with currently available insurance policies that limit the utility of these policies. Among these concerns are the following: the high deductibles and low coverage ceilings associated with the policies (especially for third parties). In addition, before a more vibrant insurance market develops, better actuarial data is required.

5. Develop risk-based models to help firms estimate the benefits from cybersecurity investments.

Given the difficulties associated with estimating the benefits from cybersecurity investments, there is a need for the development of a generic approach or framework that firms could use to estimate such benefits. Such a framework should take into consideration different perspectives toward risk management.

6. Develop a capability to conduct laboratory-based economic studies (i.e., experimental economics) concerned with assessing the impact of economic incentives on various cybersecurity-related issues.

There are many challenges for firms in determining their level of investment in cybersecurity. These challenges include the need for the capability to develop and test alternative policies for improving cybersecurity related investments, examining their effectiveness, and gauging any unintended consequences. The objective of above noted recommendation is to conduct various economic studies concerning the impact of economic incentives, in a laboratory setting (i.e., laboratory experiment), for facilitating cybersecurity investments by private sector firms in the critical infrastructure industries.

7. Develop, maintain and analyze, over an extended period of time, a database on cybersecurity investments, the types of major cybersecurity breaches, and the cost of cybersecurity breaches.

There is a dearth of data related to private sector investments in cybersecurity activities, and associated levels of losses. As a result, it is difficult for the government to evaluate the effect of policy options associated with incentives and regulations on private sector firms. A database on the level of investments in cybersecurity activities (and their effectiveness) by private sector firms could be maintained by a government agency and/or a research center within a university. The mere collection of such data could (and most likely would) serve to provide an incentive, via the marketplace, for firms to invest more into cybersecurity related activities. This data would also improve the ability of firms to make and evaluate their cybersecurity related investments, as well as for the development of a more efficient cybersecurity insurance market.

8. Provide education and training for private sector firms on "making the business case" for cybersecurity investments.

Cybersecurity investments are not made in isolation of other firm related investments. Thus, as with any investment, firms make decisions concerning cybersecurity investments within the context of the organization's other investment needs. That is, they compete for scarce resources within the context of a variety of interactive requirements. For cybersecurity activities to be increased, and sometimes even maintained, a compelling risk-based cost-benefit analysis must be made. Unfortunately, many individuals responsible for securing funds for cybersecurity activities are not well versed in the techniques associated with cost-benefit analysis. These individuals would benefit from a dedicated training program focusing on "making the business case" for cybersecurity investments. This need is especially prevalent in new start-up firms, as well as small to medium size firms, that do not have the funds to hire individuals with the requisite training to conduct cost benefit-analysis related to cybersecurity investments. This education and training program could be established in conjunction with a university and open to all firms, at a minimal cost to firms.

B. Concluding Remarks:

The above recommendations do not address many of the specific findings contained in this study. For example, as noted in Section IV during the discussion of the findings from our questionnaire-based survey, there are clear differences between the way large firms vs. small firms view issues related to cybersecurity activities (including investments and information sharing related to such activities) that need to be considered in conjunction with the above recommendations. Thus, it is important that there be flexibility in the implementation of any of these recommendations.

About the Authors

Lawrence A. Gordon.

Dr. Lawrence A. Gordon is the EY Alumni Professor of Managerial Accounting and Information Assurance at the University of Maryland's Robert H. Smith School of Business. He is also an Affiliate Professor in the University of Maryland Institute for Advanced Computer Studies. Dr. Gordon earned his Ph.D. in Managerial Economics from Rensselaer Polytechnic Institute. An internationally known scholar in the areas of managerial accounting and cybersecurity economics, Dr. Gordon's research focuses on such issues as economic aspects of cybersecurity, corporate performance measures, cost management systems, and capital investments. He is the author of roughly 100 articles, published in such journals as *The Accounting Review*, *ACM Transactions on Information and System Security*, *Journal of Financial and Quantitative Analysis*, *Journal of Computer Security*, *Accounting Organizations and Society*, *Journal of Accounting and Public Policy*, *MIS Quarterly*, *Decision Sciences*, *Omega, Journal of Business Finance and Accounting*, *European Accounting Review*, *Accounting and Business Research*, *Managerial and Decision Economics*, *Communications of the ACM*, and *Management Accounting Research*. Dr. Gordon's current research emphasizes the importance of utilizing concepts from managerial accounting and economics within an information-based economy. In particular, he is considered one of the pioneers in the emerging field of cybersecurity economics. Dr. Gordon is the coauthor of the Gordon-Loeb Model (link is external), which provides an economic framework for deriving an organization's optimal level of cybersecurity investments. This Model has been featured in *The Wall Street Journal* (link is external) and the *Financial Times* (link is external). Dr. Gordon also is the author of several books, including Managerial Accounting: Concepts and Empirical Evidence, Managing Cybersecurity Resources: A Cost-Benefit Analysis and Capital Budgeting: A Decision Support System Approach. In addition, he is the Editor-in-Chief of the *Journal of Accounting and Public Policy* (link is external) and serves on the editorial boards of several other journals. In two authoritative studies, Dr. Gordon was cited as being among the world's most influential/productive accounting researchers.

The recipient of numerous research and teaching awards, Dr. Gordon has been an invited speaker at numerous universities around the world, including Harvard University, Columbia University, Carnegie Mellon University, University of Toronto, London Business School, London School of Economics, the University of Manchester, IE Business School, and the University of California-Berkeley. He also has served as a consultant to several private (e.g., IBM) and public (e.g., U.S. General Accounting Office, now the Government Accountability Office) organizations. He has also been an invited speaker at over 50 professional (i.e., non-academic) meetings. In October 2007, he was invited to provide Congressional Testimony (link is external) concerning his research on cybersecurity economics before a Subcommittee of the U.S. House Committee on Homeland Security. In addition to the Smith School of Business, Dr. Gordon's research on cybersecurity economics has been supported by the National Security Agency and the Department of Homeland Security.

Dr. Gordon's Ph.D. students (i.e., those students for whom he has served as the Chair or Co-Chair of their dissertation) have had initial placements as an Assistant Professor of Accounting at

the Business Schools of such universities as: Northwestern University, University of Southern California, Purdue University, Rensselaer Polytechnic Institute, IE Business School, McGill University, National Taiwan University, College of William & Mary, University of Hong Kong, and Michigan State University. His former M.B.A. students frequently call him on the "Management Accounting Hotline" (affectionately named by his students) to discuss issues confronting their organizations. Dr. Gordon also is an active member of various professional organizations, a frequent contributor to the popular press (e.g., *The Wall Street Journal, USA Today and Financial Times*), and served as the President of the University of Maryland Faculty/Staff Club for over a decade.

Prior to joining the University of Maryland, Dr. Gordon was a faculty member at McGill University and the University of Kansas. He also served as a Visiting Scholar at Columbia University while on sabbatical from the University of Maryland.

Martin P. Loeb

Martin P. Loeb is the Deloitte & Touche Faculty Fellow and Professor of Accounting and Information Assurance (AIA) at the Robert H. Smith School of Business at the University of Maryland, College Park. Dr. Loeb is also an affiliate professor in the University of Maryland Institute of Advanced Computer Studies (UMIACS). Dr. Loeb received his Ph.D. from the Managerial Economics and Decision Sciences (MEDS) group at Northwestern University's Kellogg School of Management. He received his BS in mathematics and economics from the State University of New York at Stony Brook.

Dr. Loeb's research interests span a number of economic and business fields. In his early career, he conducted research on economic mechanism design, incentive regulation, cost allocations, and cost-based procurement contracting. His research papers in those areas have been published in leading academic journals such as *American Economic Review, Journal of Accounting Research, Journal of Law and Economics, Journal of Public Economics, Management Science*, and *The Accounting Review*. More recently, his research focuses on economic aspects of information security, the interface between managerial accounting and information technology, and the effect of regulation on cyber security. His papers in these areas have been published in such journals as *ACM Transactions on Information and System Security, Communications of the ACM, Journal of Accounting and Public Policy, Journal of Computer Security,* and *MIS Quarterly.* Together with Lawrence A. Gordon, he developed a model that provides a mathematical economic approach for deriving an organization's optimal investment level in cybersecurity. That model, which has become known as the Gordon-Loeb Model, has been featured in *The Wall Street Journal* and *The Financial Times*. Gordon and Loeb also co-authored Managing Cybersecurity Resources: A Cost-Benefit Analysis, a book providing a more extensive guide for managers facing the tradeoffs related to information security investments. Loeb's scholarly work has garnered over 5,000 Google Scholar citations.

Loeb has also served in a number of editorial roles in the profession. Loeb has also served on the editorial board of *The Accounting Review, The British Accounting Review, Journal of Business Finance and Accounting,* and *Review of Accounting Studies*. He currently is an editor of *Journal of Accounting and Public Policy*, and has served as a guest editor for *MIS Quarterly* and the *Journal of Information Systems Frontiers*.

Dr. Loeb currently serves as the Chair of the AIA Department. The *Wall Street Journal* (Recruiter's Survey) ranked the School's accounting program #7 in the United States. In 2015, the Financial Times ranked the doctoral program at the University of Maryland's Robert H. Smith School of Business #9 in the world.

William Lucyshyn

William Lucyshyn is the Director of Research and Senior Research Scholar, at the Center for Public Policy and Private Enterprise, in the School of Public Policy, at the University of Maryland. In this position, he directs research on critical policy issues related to the increasingly complex problems associated with improving public sector management and operations, and how government works with private enterprise. Current projects include: the economics of cybersecurity, public and private sector partnering, and identifying government sourcing and acquisition best practices. He also teaches a course on federal acquisition and has recently served on the two congressionally mandated Defense Science Board task forces. He has authored numerous reports, book chapters, and journal articles. Previously, Mr. Lucyshyn served as a program manager and the principal technical advisor to the Director of the Defense Advanced Research Projects Agency (DARPA) on the identification, selection, research, development, and prototype production of advanced technology projects.

Prior to joining DARPA, Mr. Lucyshyn completed a 25-year career in the U.S. Air Force. Mr. Lucyshyn received his Bachelor Degree in Engineering Science from the City University of New York, and earned his Master's Degree in Nuclear Engineering from the Air Force Institute of Technology.

Lei Zhou

Lei Zhou holds a B.S. in Economics and Management from Tsinghua University and Ph.D. in Accounting and Information Assurance from the University of Maryland, College Park. She taught at McGill University before joining the University of Maryland as Visiting Assistant Professor.

Dr. Zhou's research interests focuses on economics of information security, security investments and managerial accounting issues. She has published in the *European Accounting Review*, *Journal of Computer Security* and *Journal of Information Security*, and has a forthcoming paper in *Journal of Accounting and Public Policy*. Dr. Zhou's teaching interests are in the areas of managerial accounting, accounting analytics, accounting information systems and cybersecurity.