Scientific Research Publishing

Journal of Information Security, 2018, 9, 133-153
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms

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

How to cite this paper: Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2018) Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*, **9**, 133-153.
https://doi.org/10.4236/jis.2018.92010

Received: January 4, 2018
Accepted: February 9, 2018
Published: February 12, 2018

Abstract

Investments in cybersecurity are critical to the national and economic security of a nation. There is, however, a strong tendency for firms in the private sector to underinvest in cybersecurity activities. This paper reports the results of a survey designed to empirically assess whether treating cybersecurity as an important component of a firm's internal control system for financial reporting purposes serves as a driver for private sector firms to invest in cybersecurity activities. The findings, in this regard, are significantly positive. The study also shows that a firm's concern over the risk of incurring a large loss due to a cybersecurity breach and the degree the firm treats cybersecurity investments as generating a competitive advantage are drivers of the level of private sector investment in cybersecurity activities. The implications of the empirical results for designing public policies to mitigate the tendency of private sector firms to underinvest in cybersecurity are also explored.

Keywords

Cybersecurity, Investment, Determinants, Survey

1. Introduction

Cybersecurity is a national priority in countries throughout the world (e.g., see [1]). In the U.S., for example, on February 12, 2013, President Obama issued Executive Order (EO) 13636 [2], entitled "Improving Critical Infrastructure Cybersecurity". As noted in President Obama's EO:

> … The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such

> threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties ([2], Section 1).

One of the key aspects of President Obama's EO 13636 [2] was to task National Institute for Standards and Technology (NIST) with developing a Cybersecurity Framework within one year of the date of the EO. On February 12, 2014, NIST released its "Framework for Improving Critical Infrastructure Cybersecurity" [3]. On May 11, 2017, President Trump issued EO 13800 [4], entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure". A key feature of President Trump's EO is the requirement that all U.S. federal government agencies adopt the NIST Framework referred to above. As noted in President Trump's EO:

> Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order ([4], Section 1).

Although cybersecurity is considered a national priority, firms in the private sector tend to underinvest in cybersecurity activities relative to what is optimal [5]. This point is especially true for those firms that are profit oriented. There are at least four reasons that have been identified in the literature that account for this situation: First, unlike an investment that generates new revenues, investments in cybersecurity focus primarily on the cost savings (or what is often called cost avoidance) associated with preventing cybersecurity breaches.[1] Due to the strong emphasis placed on sales growth in private sector firms, cost savings projects are at a clear disadvantage compared to revenue generating projects in private sector firms [5] [6]; Second, the cost savings generated from cybersecurity investments are not observable; Third, because of the myriad of uncertainties associated with cybersecurity, many private sector firms tend to take a "wait-and-see" approach toward a portion of their spending on cybersecurity activities [7] [8]. Although in some cases such an approach is justified on an economic basis, in other cases the opposite is likely true; Fourth, due to the focus on company profits by most private sector firms, these firms tend to focus on what economists call private costs (*i.e.*, the costs that must be borne by the firms). The spill-over effects (*i.e.*, what economists call externalities) resulting from cybersecurity breaches are borne by other firms or individuals and therefore are frequently ignored, or given only lip-service, by private sector firms [5].[2]

[1]The terms *investment* and *spending* are used interchangeably in this paper.

[2]The sum of *private costs* plus *externalities* is what economists call *social costs*.

Unfortunately, there is limited research that focuses on ways to rectify the underinvestment in cybersecurity activities by private sector firms. The research that does exist in this area points out that compliance with government requirements is clearly associated with cybersecurity investments (e.g., see [9] [10]). In other words, compliance with government regulations serves to increase investments on cybersecurity activities by private sector firms. However, one aspect of compliance with government requirements as a driver (or determinant) of cybersecurity investments in private sector firms, which has largely been overlooked by cyber/information security researchers, is the need for large firms registered with the U.S. Securities and Exchange Commission (SEC) to file reliable financial reports with the SEC ([5]). The reliability of financial reports is defined in terms of satisfactory internal controls, as defined in the Sarbanes-Oxley Act (SOX) of 2002 [11]. Furthermore, any weaknesses in a firm's internal controls need to be identified by the firm's CEO (Chief Executive Officer) and CFO (Chief Financial Officer), as well as by the firm's external auditors.[3] Another aspect of compliance with government requirements as a potential driver of cybersecurity investments in private sector firms, often overlooked by cyber/ information security researchers, is the 2011 SEC Disclosure Guidance concerning cybersecurity [13]. The SEC Disclosure Guidance addresses the fact that firms should disclose their cybersecurity risks and cyber incidents in their financial reports with the SEC. Thus, the SEC Disclosure Guidance clearly emphasizes the importance of cybersecurity risks to firms.

SOX and the SEC Disclosure Guidance are both concerned with the reliability and transparency of financial reports filed by private sector firms that are publicly traded on U.S. stock exchanges. As pointed out by Gordon [14] in his Congressional Testimony, in today's digitally connected environment, reliable and transparent financial reporting are contingent on secure computer-based information systems. Gordon *et al.* ([5], p. 12) also argued that: "In a modern computer-based environment, firms cannot produce reliable financial reports without having secure computer systems." Thus, one way to increase cybersecurity investments in the private sector is to have private sector firms explicitly include cybersecurity as an important component of their internal controls for financial reporting systems. In fact, we would expect a positive association between the importance a firm attaches to cybersecurity as a component of its internal controls over financial reporting and the amount a firm spends on cybersecurity activities.

The primary objective of the study reported in this paper is to empirically assess whether the importance a firm attaches to cybersecurity as a component of its internal control over financial reporting is a driver of the amount of investment by a firm on cybersecurity activities. To our knowledge, this is the first

[3]Sections 302 and 404 of SOX specifically address the internal control requirements for the CEO, CFO and external auditors of firms. For a further discussion of these requirements, as well as issues related to material weaknesses in corporate internal controls, see the paper by Gordon and Wilford [12].

empirical study to examine this issue. Given the SEC's concern with cybersecurity risks being disclosed, the current study will also consider the empirical association between cybersecurity investments and the risk of incurring a large loss due to a cybersecurity breach. In addition, the current study will consider the association between cybersecurity investments and the potential for gaining a competitive advantage due to improved cybersecurity.

The primary findings from the current study indicate that there is a significant positive association between firms' spending on cybersecurity activities and their treatment of cybersecurity as an important component of the firm's internal controls over financial reporting. The current study also found that the risk of incurring a large loss from a potential cybersecurity breach is positively associated with the level of spending on cybersecurity activities. In addition, the current study found a positive association between a firm's spending on cybersecurity activities and whether or not the firm takes into consideration the potential competitive advantage derived from such spending.

The remainder of this paper proceeds as follows: In the next (second) section of the paper, we review the literature related to the impediments to cybersecurity investments in private sector firms and the determinants of cybersecurity investments by these firms; The second section of the paper also discusses the role of various firm-related characteristics (e.g., size, industry); The third section of the paper briefly discusses the Gordon-Loeb Model for Cybersecurity Investments, so as to provide some theoretical underpinnings of cybersecurity investments; The fourth section develops specific hypotheses concerning the determinants (or drivers) of cybersecurity investments; The fifth section of the paper discusses the empirical study, with a focus on the study's research design, measurement of variables, and sample used to test the hypotheses developed in the fourth section; The sixth section of the paper discusses the results of the empirical study; The seventh section of the paper discusses implications of the study's results; The eighth, and final, section of the paper provides some concluding comments, as well as directions for future research.

2. Literature Review

Investments in cybersecurity activities compete for funds (*i.e.*, resources) that could be used for other organizational activities. Indeed, there are always competing uses for finite organizational funds. Unfortunately, cybersecurity investments are generally at a disadvantage when competing for funds with many, if not most, other organizational investment opportunities. This point is especially true in terms of cybersecurity investments in private sector firms. This situation has led to private sector firms to underinvest in cybersecurity activities.

One key reason that firms in the private sector underinvest in cybersecurity activities is the fact that cybersecurity investments are viewed primarily as cost savings (sometimes called cost avoidance) investments because the major benefit from such investments are usually derived from avoiding or reducing the costs

associated with cybersecurity breaches.[4] In private sector firms, cost savings investments are generally more difficult to justify than revenue generating investments (e.g., an investment in a new product line) due to the emphasis that private sector firms place on revenue growth (see [6] [15]).[5] The emphasis on revenue growth by private sector firms is directly related to the fact that there is a strong correlation between a firm's revenue growth and its stock price, and a firm's stock price is a critical concern to investors and senior managers.[6]

An additional impediment to private sector investments in cybersecurity activities is that the cost savings that derive from the prevention of cybersecurity breaches are not explicitly observable. In other words, even when cybersecurity breaches are prevented or reduced due to cybersecurity investments, there are no cost savings to observe (*i.e.*, the costs associated with the potential breaches do not materialize and, therefore, cannot be observed). Thus, the expected cost savings from cybersecurity expenditures need to be estimated based on the difference between what the costs of breaches would have been in the absence of the cybersecurity investments as compared to the cost of breaches that actually occurred with the cybersecurity investments. As a result of the non-observability of the cost savings associated with cybersecurity investments, these investments are among the most difficult to justify on economic grounds to those in charge of a firm's resource allocation decisions (e.g., a firm's CFO).

The inability to explicitly observe the cost savings from cybersecurity investments means that developing reliable probabilistic models to predict the ex-ante benefits from investments in cybersecurity is generally significantly more difficult than developing reliable probabilistic estimates of the ex-ante benefits from many other types of organizational investment opportunities. In fact, convincing a firm's senior manager (e.g., the CFO) to increase the budget for cybersecurity activities often becomes more of an art than a science. Consequently, many firms defer a portion of their cybersecurity investments until a major cyber incidence occurs or the potential for a major cybersecurity breach clearly surfaces. In fact, it is often economically rational (from a real options perspective) for firms to take a wait-and-see approach to a portion of their cybersecurity investments (e.g., see [7] [8]). Anecdotal evidence supporting the wait-and-see approach is abundant. For example, after its cybersecurity breach in 2013, Target Corporation accelerated $100 million planned investments in cybersecurity activities. As noted in Target's 10-K Report filed with the SEC for the fiscal year ending February 1, 2014 ([17], p. 18), "…the company accelerated a previously planned in-

[4]As discussed in the next section of the paper, there are situations where cybersecurity activities could result in a competitive advantage and, in turn, generate new revenues.

[5]The capital investment (or capital budgeting) literature usually differentiates among revenue generating, cost savings and must do investments (see [16], Chapter 12). Revenue generating investments relate to projects that generate new revenues (e.g., a new product line), cost savings investments relate to projects that generate cost savings (e.g., replacing labor with new technology to do the same work), and must do investments relate to projects that are required by law (e.g., investment in pollution control facilities).

[6]This latter point is especially true where executive compensation is tied, at least in part, to the firm's stock price via stock options.

vestment of $100 million to equip our proprietary REDcards and all of our U.S. stores with chip-enabled smart-card technology by the first quarter of 2015". Of course, deferring a portion of a firm's cybersecurity investments until a major cyber incidence occurs or seems imminent, results in a spending delay at a minimum, if not ultimate underinvestment, in cybersecurity activities ([5] [6]).[7]

Another impediment to cybersecurity investments, compared to other organizational investment opportunities, relates to the fact that a large portion of the costs of cybersecurity breaches are not borne by the private sector firms incurring the breaches. Indeed, firms other than the one incurring a breach (e.g., business partners), as well as individuals (e.g., customers), often end up absorbing a large share of the costs associated with a cybersecurity breach. This spill-over effect is what economists call externalities. In other words, when a firm experiences a cybersecurity breach, there are private costs (*i.e.*, those costs borne by the firm incurring the cybersecurity breach) and externalities (*i.e.*, those costs borne by firms and individuals external to the firm incurring the cybersecurity breach, such as the costs to customers that have their identity stolen). However, since private sector firms focus on profits, it is well known that there is a tendency among these firms to either ignore, or only pay scant attention to, the externalities associated with cybersecurity breaches [8]. Thus, apart from the fact that cybersecurity investments are viewed primarily as cost savings projects and that the cost savings are unobservable, from society's perspective (*i.e.*, the social costs) there is good reason to conclude that private sector firms underinvest in cybersecurity activities (e.g., [5] [6]).

Despite the above impediments to cybersecurity investments, private sector firms do make a substantial investment in cybersecurity activities. In fact, estimates clearly point out that firms spend a substantial amount on cybersecurity activities and the level of spending is increasing (e.g., see [19]).[8] The literature points out that there are several factors driving cybersecurity spending. These factors include compliance with existing regulations related to cybersecurity,[9] concern over the risks associated with a large loss due a cybersecurity breach, and the potential for gaining a competitive advantage ([8] [9]).

[7]It is often argued that the best way to address externalities is through government regulations (e.g., levy a heavy penalty on firms that incur a major cybersecurity breach). Although beyond the scope of the study reported on this paper, such an approach was raised during the Congressional Hearings in 2017 on the Equifax breach [18]. The relevant point for our study, however, is that externalities clearly lead to a situation where private sector firms tend to underinvest in cybersecurity activities relative to what is a socially optimal investment level.

[8]Private sector firms rarely disclose the amount spent specifically on cybersecurity activities. Thus, the estimates of the amount private sector firms spend on cybersecurity are largely guesswork. An exception to the preceding statement can be found in the corporate reports filed with the SEC after experiencing a major cybersecurity breach. For example, in Target's 10-K Report [17], it was noted that the company was increasing its level of cybersecurity spending by $100 million. Note that the Computer Security Institute used to conduct an annual survey in which organizations were asked to report their information security spending [20] (their last survey was published in 2011). Other organizations (e.g., PwC, EY, Ponemon Institute/Accenture) conduct annual cybersecurity surveys, but these surveys investigate threats and ex post costs of cybersecurity breaches but not the costs of cybersecurity spending [21] [22] [23].

[9]Although some cybersecurity regulations apply to all organizations, others are industry specific (e.g., organizations in the health care industry need to comply with the Health Insurance Portability and Accountability Act (HIPPA) [24] regulations and organizations in the financial institutions industry have to comply with Financial Industry Regulatory Authority (FINRA) and others are state specific (see http://www.ncsl.org/re-search/tele-communications-and-information-technology/cybersecurity-legislation-2017.aspx for recently passed state cybersecurity regulations).

Calls for increases in cybersecurity spending by private sector firms are often accompanied by calls for new government incentives to spur such spending. However, as pointed out by Gordon *et al.* [5], the effectiveness of new government incentives to spur cybersecurity spending by private sector firms is largely contingent on a firm's willingness and ability to increase the size of its budget for cybersecurity activities. Of course, given that firms have finite resources to spend on IT (information technology) items and activities, in the final analysis spending more on cybersecurity activities comes down to a resource allocation decision. Accordingly, we now turn our attention to examining how firms could derive the appropriate level of cybersecurity investments.

3. Gordon-Loeb Model for Cybersecurity Investments

There are several models that could be used to derive the appropriate level of cybersecurity investments. One of the models, which has received wide-scale acceptance among academicians and practitioners, is referred to in the literature as the Gordon-Loeb Model (hereafter referred to as the GL Model). The GL Model is based on the fundamental economic principle of cost-benefit analysis and is grounded in mathematics [25]. However, the GL Model provides a basic framework for deriving a firm's level of spending on cybersecurity activities that can be utilized without sophisticated mathematics (e.g., see [26]). In 2017, a report by the U. S. Better Business Bureau addressing issues related to cybersecurity investments in small businesses recommended the GL Model as a framework that "…provides a useful guide for organizations trying to find the right level of cybersecurity investment" ([27], p. 20). In an earlier study by the Armed Forces Communications and Electronics Association (AFCEA), it was noted that "…the Gordon-Loeb model has become the "gold standard" in the area of cyber economic models" ([28], p. 10). The GL Model has also been featured in many articles in the popular press, including articles in The Wall Street Journal [29] and The Financial Times [30].

The economics underlying the GL Model is based on the assumptions that the benefit from investments in cybersecurity activities are increasing at a decreasing rate and that 100% security is not achievable. As demonstrated in the paper by Gordon and Loeb [25], where the model was originally developed, under some general conditions, the maximum amount a firm should invest in cybersecurity activities should not exceed $1/e$ (or roughly 37%).[10] The GL Model is based on the following three fundamental components: 1) the value of information being protected; 2) the vulnerability/threat associated with a breach to an information set, which is commonly referred to as the probability that an information set will experience a cybersecurity breach; and 3) the productivity of an additional investment in cybersecurity. The implementation of the GL Model can be accomplished in the four simple steps provided below.[11]

[10]In the model, "e" represents a mathematical constant equal to approximately 2.7168.

[11]For a more detailed analysis of how to implement the GL Model, including an example, see [26]. A three-minute YouTube Video explaining the general nature of the Model, including the four steps discussed below can be found at: https://www.youtube.com/watch?v=cd8dT0FuqQ4.

Step 1: Estimate the value, which in turn is the potential loss, associated with each segmented information set in the organization.

Step 2: Estimate the probability that an information set will be breached based on the vulnerability/threat associated with each information set.

Step 3: Create a grid of all combinations of Steps (1) and (2) above. The values in the cells in this grid provide the expected losses from a cybersecurity breach to the information sets. These values also represent the potential benefits from additional cybersecurity investments (*i.e.*, the potential benefits are derived from preventing the expected losses).

Step 4: Derive the total level of cybersecurity investment by allocating additional funds to protect the information sets, subject to the constraint that the incremental benefit from an additional investment in cybersecurity exceeds (or at least equals) the incremental cost associated with the additional investment. An additional investment to protect an information set essentially reduces the probability (*i.e.*, vulnerability/threat) of a cybersecurity breach to that information set, and in turn reduces the expected loss from a cybersecurity breach to that information set.

The GL Model highlights the importance of reducing the probability (*i.e.*, vulnerability/threat) of a security breach in order to manage cybersecurity risk. A fundamental way a firm can reduce the probability of a cybersecurity breach is through its internal control system.[12] In fact, a strong internal control system plays, or at least could play, an important role in reducing a firm's ex ante probability of incurring a cybersecurity breach (or breaches) due to its focus on the effective/efficient operations of an organization and its focus on having an organization comply with relevant laws, regulations, and policies. Accordingly, given that publicly traded firms listed on U.S. stock exchanges are already required to report on their internal controls for financial reporting purposes under sections 302 and 404 of [11], it would seem beneficial to a firm's if it were to treat cybersecurity as an explicit component of its internal control system for financial reporting purposes. Indeed, a strong internal control system could help an organization better understand and identify the probability that it will incur a cybersecurity breach. A better understanding and identification of the probability that a firm will have a cybersecurity breach should, in turn, help the organization determine its appropriate level of cybersecurity investment that should be directed at reducing the *ex ante* probability of incurring a cybersecurity breach to a particular information set.

4. Hypotheses

The above discussion of the GL Model pointed out that treating cybersecurity as an explicit part of a firm's internal control system for financial reporting could help a firm better understand and identify the *ex ante* probability that it will in-

[12]Internal control is "a process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies." (see: https://en.wikipedia.org/wiki/Internal_control).

cur a cybersecurity breach. As a result, the firm should be in a better position to determine the appropriate, and possibly higher, level of investment in cybersecurity activities. More to the point, a private sector firm's internal control system, with its emphasis on operational effectiveness/efficiency and compliance with laws, regulations and policies, could play an important role in helping the firm to offset the tendency to underinvest in cybersecurity activities discussed in the previous sections of this paper. The above point was also made by Gordon *et al.* [31] [32], and during the Congressional Testimony by Gordon [14].

If a firm were to explicitly treat cybersecurity risks and cyber incidents as an important component of its internal control system for financial reporting purposes, the Sarbanes-Oxley Act of 2002 [11] would require major cybersecurity risks and breaches to be explicitly reported as material weaknesses in a firm's internal control report contained in the firm's 10-K Report filed with the SEC.[13] Since we know that "what you measure is what you get," giving explicit recognition to cybersecurity risks and breaches as part of a firm's internal control report would likely encourage firms to increase their level of investment in cybersecurity activities in an effort to avoid having to disclose weaknesses related to these concerns.

In sum, explicitly considering cybersecurity as an important component of a private sector firm's internal control system is likely to encourage a firm to invest more into cybersecurity related activities than otherwise would be the case. Of course, this is an empirical issue, which leads us to our first hypothesis that will be tested based on the below null hypothesis.

H_{01}: There is no association between the level of investment in cybersecurity activities and the degree to which a firm considers cybersecurity an important component of its internal controls for financial reporting.

As mentioned earlier in this paper, even though private sector firms tend to underinvest in cybersecurity activities, we know that firms make significant cybersecurity related investments in an effort to avoid experiencing cybersecurity breaches. In this regard, during the Congressional Hearing on February 4, 2014 [33], representatives from both Target Corporation and Neiman Marcus Corporation indicated that their firms had been spending very large sums of money (e.g., hundreds of millions of dollars at Target Corporation) on cybersecurity related activities prior to their companies' cybersecurity breaches in 2013. During his October 4, 2017 Congressional Hearing [18], the CEO of Equifax (Richard Smith) also pointed out that his company had invested significant amounts of money in cybersecurity related activities prior to its 2017 cybersecurity breach. It was also pointed out during the Congressional Testimony, as well as on Target's 2013 10-K Report, that after the Target experienced its major cybersecurity breach that the firm was accelerating $100 million of planned investments in

[13]Section 404 of the Sarbanes-Oxley Act (SOX) of 2002 [11] requires firms to include an internal control report as part of its 10-K Report filed with the SEC. This report is required to identify material weaknesses in a firm's internal control over financial reporting. Under SOX, independent auditors are required to attest to the internal control report for accelerated filers.

cybersecurity activities to be completed by the first quarter of 2015 (see [17], p. 18).

The above noted Congressional Hearings make it clear that organizations recognize the fact that cybersecurity breaches represent a critical potential risk factor for firms. In fact, it is increasingly common for executives to think of cybersecurity risk management as a critical component of their firms' overall enterprise risk management. Evidence attesting to this latter claim can be found in the 10-K Reports filed with the SEC by firms since the SEC issued its 2011 Disclosure Guidance on cybersecurity risks and cyber incidences [13]. More to the point, since the issuance of the 2011 SEC Disclosure Guidance, the 10-K Reports of nearly all firms have some mention of the risk associated with a potential cybersecurity breach.[14] In addition, the conceptual discussion of the GL Model for cybersecurity investments made it clear that the size of an expected loss due to a cybersecurity breach is directly associated with the amount a firm should invest in cybersecurity activities.

The reaction to Target's 2013 cybersecurity breach by Target, and the reaction by other firms, provides strong empirical evidence of how firms view a major cybersecurity breach as a critical firm level risk factor. More to the point, Target's major cybersecurity breach triggered a significant increase in its cybersecurity spending as well as the spending by other firms in order to avoid a similar breach.[15]

In sum, it would appear that a critical risk factor associated with a firm's total level of cybersecurity investment is the potential for a large loss due to a cybersecurity breach. In order to test the above argument concerning the fact that a key determinant (driver) of cybersecurity investments is the concern that a large cybersecurity breach represents a critical potential risk factor for a firm, our empirical study tested the second null hypothesis stated below.

H_{02}: There is no association between the level of investment on cybersecurity activities and the way a firm views a large potential loss from a cybersecurity breach as a critical potential risk factor for the firm.

Another potential determinant (driver) of cybersecurity investments has to do with the potential competitive advantage a firm could derive from cybersecurity activities. As noted in the previous sections of this paper, the primary benefits from cybersecurity investments are usually considered to be the cost savings derived from avoiding cybersecurity breaches. This fact notwithstanding, there are some circumstances where a firm's cybersecurity activities could help to distinguish the firm from its competitors and thereby generate additional revenues for

[14]While it is true that the 10-K Reports of nearly all firms discuss the risk associated with a potential cybersecurity breach, the overwhelming majority of these discussions are of a "boiler-plate" nature. Although the beyond the scope of this paper, there are a variety of explanations for this boiler-plate approach. Chief among these explanations are the fact that: 1) firms do not want to frighten investors into thinking they have inordinate cybersecurity problems; and 2) firms do not want to provide a road-map for potential hackers concerning the way they address cybersecurity related issues.

[15]Many argue that the Target's breach caused the US to speed up its EMV (Europay, MasterCard and Visa) migration (*i.e.*, adoption of chip enhanced credit cards, see [34]).

the firm. Where this occurs, the cybersecurity investment would be revenue generating investment, as well as a cost savings investment. This situation seems especially likely in firms that compete in industries that generate a large portion, or all, of their revenues via the Internet, where cybersecurity is critical to gaining customer confidence regarding on-line purchases (e.g., Internet-based firms such as Amazon, Inc. and E-Bay). In addition, a competitive advantage due to cybersecurity activities seems particularly relevant for small businesses because most small businesses do not have large sums of money to spend on cybersecurity activities. Thus, by devoting an unusually large amount of funds to cybersecurity, a small business might be able to create a competitive advantage over other small businesses in terms of cybersecurity.

A competitive advantage due to cybersecurity could have significant value in doing business with government agencies, especially since President Trump's Executive Order 13800 [4] requires all government agencies to incorporate the NIST framework for cybersecurity risk management [3]. That is, a firm that has addressed cybersecurity risk management in a manner that is consistent with the NIST framework could possibly enjoy a competitive advantage relative other firms that have not done the same in terms of obtaining government contracts. Of course, we would expect all firms to realize the importance of this potential competitive advantage via cybersecurity activities and, in equilibrium, to adjust their spending on cybersecurity activities accordingly.

The potential to create a competitive advantage, which in turn could generate additional revenues, could help to offset the tendency by private sector firms to underinvest in cybersecurity activities. To examine this argument, our empirical study tested the third null hypothesis stated below.

H_{03}: There is no association between the level of investment on cybersecurity activities and the degree to which an organization considers the potential competitive advantage derived from strong cybersecurity.

5. Empirical Study

5.1. Research Design

As part of a study sponsored by the U. S. Department of Homeland Security (DHS), we conducted a large-scale questionnaire-based survey of senior executives in private sector firms. The survey instrument was initially developed based on the existing literature, interviews with several senior executives involved in cybersecurity investment decisions, and four in-depth case studies of publicly traded private sector firms that experienced a major cybersecurity breach within the past few years. The four case studies were based on publicly available data, including data derived from the firms' 10-K, 10-Q, and 8-K reports filed with the U.S. Securities and Exchange Commission (SEC).[16]

Prior to finalizing the survey instrument, we conducted a small pilot study to

[16]The four firms that comprised the case studies were Target Corporation, Neiman Marcus Corporation, RSA, and JP Morgan Chase & Company.

assess the instrument's reliability and validity. The pilot study consisted of giving the survey instrument to five executives with several years of experience working on cybersecurity related issues. In general, the executives indicated that the survey questions had face validity. Based on their feedback, several minor changes were made to the questionnaire. As discussed in the sample section of this paper, the final survey instrument, along with a cover letter stating that the study was being sponsored by DHS, was sent to a large number of senior executives.

The dependent variable in the study is the portion (measured in terms of percentage) of IT budget devoted to cybersecurity. This variable was allowed to range from 1 (1% - 2%) to 7 (greater than 20%) possible discrete values. Most of our independent variables were also measured based on ordinal survey responses, ranging from 1 (strongly disagree) to 7 (strongly agree). The one exception concerns the last independent variable, which was measured on a 1 to 4 scale. A more complete description of how these variables, including how they were measured, is provided below.

The responses to the survey were measured based on ordinal data, using a 1 - 7 scale for most of the questions related to the variables shown in Equation (1) below, and a 1 - 4 for one of the variables shown in that equation. Since the distance between adjacent values of the answers to the questions are not necessarily equal, we used a logistic regression model for conducting our primary statistical analyses associated with testing the three hypotheses discussed in the last section of this paper. Logistic regression measures the relationship between the dependent variable and independent variables, by estimating the probability of the dependent variable, using a logistic function (*i.e.*, the cumulative logistic distribution). The results help to explain how the values of independent variables affect the probability that the dependent variable equals a specific value (in our case, "how much" is the percentage of IT budget devoted to cybersecurity). The model we used is formally stated as Equation (1) below:

$$\log \frac{prob(Bgt)}{\left[1 - prob(Bgt)\right]} = \beta_0 + \beta_1 IC + \beta_2 CR + \beta_3 CA + \beta_4 Rev + \varepsilon. \quad (1)$$

The definitions of the variables used in Equation (1) are as follows. Bgt is the response to the question: "Approximately what portion of your firm's IT budget is devoted to cybersecurity related activities?" IC refers to the level of (dis)agreement to the statement: "Cybersecurity is an important component of my organization's approach to the internal controls of financial reporting systems." CR refers to the level of (dis)agreement to the statement: "In determining the risk associated with cybersecurity breaches, my organization considers the largest potential loss." CA refers to the level of (dis)agreement to the statement: "The expected benefits from cybersecurity expenditures take into consideration the potential competitive advantage derived from strong cybersecurity within your organization." Rev refers to a firm's gross annual revenues, which is used in this study to control for the varying sizes of the firms being represented by the survey respondents.

5.2. Measurement of Variables

Dependent Variable

The dependent variable of concern in the empirical study discussed in this paper is the annual level of investment (*i.e.*, expenditures) on cybersecurity activities made by a firm. Unfortunately, firms do not accumulate the expenditures for cybersecurity related activities in one subsidiary account. Thus, rather than asking the survey respondents to indicate a dollar amount of expenditures on cybersecurity activities, we asked them to indicate the portion (measured in terms of percentage) of the firm's IT budget that was devoted to cybersecurity related activities. As shown in Equation (1), this variable is denoted as *Bgt*. There were seven possible choices, from which the survey respondents could select one. These choices were: 1) 1% - 2%; 2) 3% - 5%; 3) 6% - 8%; 4) 9% - 11%; 5) 12% - 15%; 6) 16% - 20%; and 7) greater than 20%.

Measuring the annual level of investment (*i.e.*, expenditures) on cybersecurity activities in terms of the percentage of the firm's IT budget devoted to cybersecurity activities was done for two reasons. First, since the firms in our sample vary in size, combined with the fact that the objectives of the study is to identify the main determinants (drivers) of cybersecurity investments, we concluded that asking respondents to indicate the percentage of the IT budget devoted to cybersecurity activities would result in more comparable findings across respondents than focusing on specific dollar amounts spent on cybersecurity activities (even after controlling for firm size). Second, based on the interviews with executives prior to completing the final survey instrument that was sent out to our sample (as discussed above), we concluded that we were far more likely to get meaningful responses to a question concerning the cybersecurity spending relative to the overall IT budget than a question concerning the exact dollar amount spent on cybersecurity. A fundamental reason for reaching this conclusion is the fact that the executives made it clear that the estimates of cybersecurity expenditures likely varies substantially among firms. Although this variation in estimates affects the information gathered related to the percentage of the firms' IT budget, the variance in the way this number is estimated is probably much smaller than it would be for the interpretation of what constitutes the actual dollar amounts. Thus, for purposes of this study, level of investment in cybersecurity activities refers to the percentage of IT budget devoted to such activities.

Independent Variables

As shown in Equation (1), our model included one independent variable that is associated with each of the hypotheses discussed in the last section of this paper. More to the point, *IC* (*i.e.*, which refers to internal control of financial reporting) is associated $\mathbf{H_{01}}$, *CR* (which refers to the cybersecurity risk associated with a large loss) is associated with $\mathbf{H_{02}}$, and *CA* (which refers to the potential competitive advantage derived from cybersecurity) is associated with $\mathbf{H_{03}}$. As noted above, these variables are measured on a 1 to 7 scale, where 1 represents "strongly disagree" and 7 represents "strongly agree".

Rev (which represents the dollar amount of a firm's gross annual revenues) is another independent variable included in Equation (1) and, as noted above, is used as a control variable to account for the varying sizes of the firms included in the study. This variable was measured in terms of four possible choices, from which the survey respondents could select one. These choices are: 1) under $10 million; 2) $10 million to $99 million; 3) $100 million to $1 billion; and 4) over $1 billion. It should be noted that, although not specified as a specific hypothesis, our expectation is that the larger the firm, the smaller the percentage of the IT budget devoted to cybersecurity related activities. The reason for this later expectation is that a significant portion of IT costs are fixed, rather than variable, and lend themselves to large economies of scale (e.g., the cost of hardware, software, and key personnel).

5.3. Sample

The survey instrument was sent to a total of approximately 2000 senior executives responsible for either the technical aspects of cybersecurity investments (*i.e.*, Chief Information Officers [CIOs]) or the financial aspects of cybersecurity investments (*i.e.*, Chief Financial Officers [CFOs]) of approximately 1600 major U.S. organizations. These organizations represented a variety of industries that are normally viewed as being part of the U.S. critical infrastructure (see Table 1).

After approximately eight weeks from the initial mailing of the survey instrument, a second mailing of the survey instrument was sent out. Since all participants in the study were guaranteed anonymity, the second mailing was sent to all 1600 organizations with a cover letter indicating that, if the targeted individuals had already responded to the survey, no further action was required (*i.e.*, we did not want more than one response from a given individual). After taking into consideration the returned questionnaires due to the fact that either a CIO or CFO was no longer with the organization or that the organization itself was no longer in existence (e.g., via a merger or acquisition), we had a usable response rate of approximately 10% (*i.e.*, 158 responses).[17]

6. Results

Panel A of Table 1 shows the percentage of the IT budget devoted to cybersecurity activities by the firms responding to our survey. As shown in **Panel A**, most respondents (*i.e.*, 129 out of 158) indicated that the percentage of the IT budget spent on cybersecurity activities in their firms is between 1% and 11%, with the interval of 3% - 5% being the most popular response (*i.e.*, 50 responses). More than 16% of the respondents (*i.e.*, 26 out of 158) indicated that the percentage of the IT budget spent on cybersecurity activities in their firms is between

[17]Response rates for questionnaire-based surveys related to cybersecurity issues are notoriously low, and it is not surprising that nearly all cybersecurity surveys (e.g., [21] [23]) report only the number of respondents, but not the response rate. One survey reporting the response rate is [20], in which there were 616 respondents out of 5000 mailings. Thus, a response rate of 10% in our study is in line with other cybersecurity cost studies.

Table 1. Descriptive statistics concerning usable survey responses. **Panel A:** Percentage of IT budget devoted to cybersecurity; **Panel B:** Size distribution by annual revenue; **Panel C:** Industry distribution.

Panel A

IT budget devoted to cybersecurity	1% - 2%	3% - 5%	6% - 8%	9% - 11%	12% - 15%	16% - 20%	More than 20%	Total
Number of observations	26	50	25	28	16	10	3	158

Panel B

Revenue	Under $10 million	$10 million to $100 million	$100 million to $1 billion	Over $1 billion	Total
Number of observations	23	40	43	52	158

Panel C

Industry	Number of observations
Biotech	8
Defense	3
Energy	14
Financial services	52
Health care	26
Information technology	8
Manufacturing	26
Retail	2
Telecommunications	6
Transportation	4
Utilities	9
Total	158

12% and 20%. Less than 2% of the respondents (*i.e.*, 3 out of 158) indicated that the percentage of the IT budget spent on cybersecurity activities in their firms is more than remain 20%.

As shown in **Panel B** of Table 1, roughly one third of the respondents (*i.e.*, 52 out of 158) are from firms with annual revenues greater than $1 billion, more than half of the respondents (*i.e.*, 83 out of 158) are from firms with annual revenues between $10 million and $1 billion, and roughly 15% (*i.e.*, 23 out of 158) of the respondents are from firms with revenues less than $10 million. **Panel C** of Table 1 shows that two thirds of the respondents indicated that their firms operate primarily in either the Financial Services, Health Care or Manufacturing industries. The rest of the respondents indicated that their firms operate primarily in either the Biotech, Defense, Energy, Information Technology, Retail, Telecommunications, Transportation or Utilities industries.[18]

[18]Given the small number of firms in many of the industries, we did not attempt to conduct an industry analysis.

The results from the logistic regression analysis (*i.e.*, Equation (1) provided in the previous section of this paper) are provided in Table 2. The coefficients for *IC*, *CR* and *CA* are 0.2688, 0.2337, and 0.1744, respectively. The coefficients of *IC* and *CR* are significant and positive at the 5% level, and the coefficient of *CA* is significant and positive at the 10% level. These results suggest that a greater value in *IC*, *CR* and/or *CA* is likely to be associated with a higher percentage of IT budget devoted to cybersecurity related activities, hence provide support for all three of our hypotheses. More to the point, these results indicate that three important determinants (drivers) of the percentage of a firm's IT budget devoted to cybersecurity are: 1) the extent to which management considers cybersecurity as an important component of a firm's internal controls of financial reporting systems; 2) the extent to which management considers the largest potential loss as a cybersecurity risk factor; and 3) the potential competitive advantages derived from strong cybersecurity.

As shown in Table 2, the coefficient for *Rev* (−0.4939) is significant and negative at the 1% level. This finding suggests that larger firms (*i.e.*, firms with higher revenues) are more likely to devote a smaller percentage of their IT budgets to cybersecurity. This finding is not surprising, given that a large portion of a firm's cybersecurity spending is fixed over some range of cybersecurity activity (e.g., investments in hardware, software and key personnel). Thus, although the absolute dollar amount invested in cybersecurity activities is usually higher for large firms when compared to small firms, it is logical for the percentage of the IT budget spent on cybersecurity related activities to be smaller for large firms than for small firms. Indeed, investments in cybersecurity activities are a good example of the benefits of economies of scale.

A unique aspect of the size factor became clearer during conversations between

Table 2. Logistic regression results[a,b].

Independent variables	Coefficient	P-value	Odd ratio estimates
IC	0.2688	0.0410	1.308
CR	0.2337	0.0198	1.263
CA	0.1744	0.0707	1.191
Rev	−0.4939	0.0005	0.610

a. Regression equation: $\log \frac{prob(Bgt)}{\left[1-prob(Bgt)\right]} = \beta_0 + \beta_1 IC + \beta_2 CR + \beta_3 CA + \beta_4 Rev + \varepsilon$. b. Notations: *Bgt* = the portion (measured in terms of percentage) of the firm's IT budget that was devoted to cybersecurity related activities. 1: 1% - 2%; 2: 3% - 5%; 3: 6% - 8%; 4: 9% - 11%; 5: 12% - 15%; 6: 16% - 20%; 7: greater than 20%. IC = level of (dis)agreement to the statement: "Cybersecurity is an important component of my organization's approach to the internal controls of financial reporting systems." 1: strongly disagree; 7: strongly agree. CR = level of (dis)agreement to the statement: "In determining the risk associated with cybersecurity breaches, my organization considers the largest potential loss." 1: strongly disagree; 7: strongly agree. CA = level of (dis)agreement to the statement: "The expected benefits from cybersecurity expenditures take into consideration the potential competitive advantage derived from strong cybersecurity within your organization." 1: strongly disagree; 7: strongly agree. *Rev* = gross annual revenues of the firms included in the study. 1: under $10 million; 2: between $10 million and $100 million; 3: between $100 million and $1 billion; 4: more than $1 billion.

the authors of this study and several CISOs. In particular, it was frequently pointed out that smaller to medium size firms often find themselves in the position of having to outsource a large portion of their cybersecurity activities due to the high cost associated with hiring a sufficient number of technically qualified personnel.

7. Implications

As indicated by the results of the current study, there is a significant positive association between the importance firms attach to cybersecurity for internal control purposes and the percentage of their IT budget spent on cybersecurity activities. This finding supports the conceptual argument provided in the paper by Gordon *et al.* [5] that a stricter enforcement of the internal control requirements under SOX, and implied by the SEC's Disclosure Guidance [13], is an important step in the direction of offsetting the underinvestment in cybersecurity activities by private sector firms (at least for their financial systems). An important policy level implication of this finding is that a stricter enforcement by the SEC of the internal control report requirements mandated by the Sarbanes-Oxley Act (SOX) of 2002 [11], and a more aggressive interpretation of the 2011 SEC Disclosure Guidance [13] on cybersecurity risk and cyber incidents, could help to offset the underinvestment in cybersecurity activities by private sector firms. In other words, if firms were required to disclose their cybersecurity material weaknesses in their internal control report included as part as their 10K-filing, as well as to provide more transparency concerning their cybersecurity risks and cyber incidents, they would likely increase the importance they attach to cybersecurity and, in turn, increase their cybersecurity spending.

Another finding from the current study was a significant positive association between the percentage of a firm's IT budget spent on cybersecurity activities and the way firms view a large potential loss from cybersecurity breach as a critical risk factor for the firm. Thus, a second policy level implication of the findings from the current study is that the U.S. federal government should facilitate a program that helps private sector firms identify and understand the risk of a large loss resulting from a major cybersecurity breach. The importance of such a program is highlighted by the fact that for some firms (especially small businesses), one security breach resulting in a large loss could force the firm into a precarious financial position (see Fanelli *et al.* [27] for some interesting data related to this concern). One way of accomplishing the goal of assisting firms identify and understand the risk of a large loss caused by a major cybersecurity breach is by the development of a publicly shared government sponsored database. Such a database could document the costs and risks associated with cybersecurity breaches to private sector firms. Although the above noted database could be developed on a national level, it might be worth exploring the possibility of developing such a database on a global level by an organization such as the World Bank or International Monetary Fund.

The current study also found a significant positive association between the percentage of a firm's IT budget spent on cybersecurity activities and the degree to which the firm considers the potential competitive advantage derived from strong cybersecurity. Thus, a third policy level implication of the findings from the current study is the opportunity for the U.S. federal government to help private sector firms better understand the potential competitive advantages from having a strong cybersecurity program in place. A better understanding of the potential competitive advantages of cybersecurity would, or at least should, encourage an increase in spending on cybersecurity activities by private sector firms. One way for the federal government to assist private sector firms to better understand the potential competitive advantage of cybersecurity is to either conduct, or provide support for, a comprehensive study on the competitive advantages accruing to firms that have a strong cybersecurity program in place.

8. Concluding Comments

Investments in cybersecurity are critical to the national and economic security of a nation. There is, however, a strong tendency for firms in the private sector to underinvest in cybersecurity activities. Given that roughly 85% of the U.S. Critical Infrastructure is owned by private-sector firms, this underinvestment in cybersecurity activities is clearly a serious concern to the national and economic security of the U.S. Unfortunately, there are some fundamental causes creating this situation. Four of the most important causes are as follows: First, cybersecurity investments are treated primarily as cost savings (or cost avoidance) investments by most private sector firms in the U.S. and such investments usually do not fare well compared to revenue generating investments; Second, the cost savings generated from cybersecurity investments are not observable; Third, given the high degree of uncertainty associated with the benefits of cybersecurity investments, there is a tendency for firms to take a "wait-and-see" approach to a large portion of potential cybersecurity investments; Fourth, private sector firms tend to ignore, or only pay "lip-service" to, the costs of the externalities (*i.e.*, spillover effects that are not charged to the firm) associated with cybersecurity breaches. The primary objective of the study reported in this paper has been to empirically assess whether treating cybersecurity as an important component of a firm's internal control system for financial reporting purposes could serve as a driver for offsetting the above noted tendency by private sector firms to underinvest in cybersecurity activities. In addition, the empirical study reported also considered whether concern over the risk of incurring a large loss due to a cybersecurity breach, as well as treating cybersecurity investments as potentially generating a competitive advantage, could serve as drivers for offsetting the above noted tendency by private sector firms to underinvest in cybersecurity activities.

The findings from the study reported in this paper support the arguments that all three of the above noted potential drivers do indeed increase cybersecurity

investments in private sector firms. More specifically, we found that treating cybersecurity as an important component of a firm's internal control system for financial reporting, firm-level concern over risk of a potentially large loss due to a cybersecurity beach, and considering cybersecurity investments as a firm-level potential competitive advantage are all important drivers (or determinants) of cybersecurity investments in private sector firms. As discussed in the previous sections of the paper, these findings have important implications for offsetting, at least partially, the underinvestment in cybersecurity activities by private sector firms.

As with all empirical studies, there are limitations with the empirical study forming the basis of this paper. One such limitation is that we ended up with only 158 usable responses to our survey. A second limitation is that there are many factors that drive cybersecurity investments in private sector firms not included in our study. In fact, one could come up with a long list of such factors. Indeed, controlling for all the potential factors driving cybersecurity spending presents a formidable problem. One way to address this problem in future research is to conduct laboratory experiments. The above limitations notwithstanding, we believe the study reported upon in this paper should help to improve our understanding of how to increase cybersecurity investments in private sector firms.

Acknowledgements

This work was supported by the US Department of Homeland Security (DHS) Science and Technology Directorate (Contract #N66001-112-C-0132); the Netherlands National Cyber Security Centre (NCSC); and Sweden MSB (Myndigheten för samhällsskydd och beredskap)—Swedish Civil Contingencies Agency.

References

[1] OECD (2012) Cybersecurity Policy Making at a Turning Point. https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[2] Obama, B. (2013) Executive Order—Improving Critical Infrastructure Cybersecurity. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[3] National Institute of Standards and Technology (NIST) (2014) Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[4] Trump, D. (2017) Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[5] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) Increasing Cybersecurity Investments in Private Sector Firms. *Journal of Cybersecurity*, **1**, 3-17. https://doi.org/10.1093/cybsec/tyv011

[6] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2014) Cybersecurity Investments in the Private Sector: The Role of Governments. *Georgetown Journal of International Affairs*, International Engagement on Cyber IV, 79-88.

[7] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Information Security Expenditures and Real Options: A Wait-And-See Approach. *Computer Security Journal*, **19**, 1-7.

[8] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. *Journal of Accounting and Public Policy*, **34**, 509-519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

[9] Moore, T., Dynes, S. and Chang, F. (2015) Identifying How Firms Manage Cybersecurity Investment. Working Paper. Southern Methodist University, Dallas, TX, 1-32.

[10] Filkins, B. (2016) IT Security Spending Trends. SANS Institute, Bethesda, MD, 1-23. https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

[11] The Senate and House of Representatives of the United States of America (2002) Sarbanes-Banes Oxley Act. https://www.sec.gov/about/laws/soa2002.pdf

[12] Gordon, L.A. and Wilford, A. (2012) An Analysis of Multiple Consecutive Years of Material Weaknesses in Internal Control. *The Accounting Review*, **87**, 2027-2060. https://doi.org/10.2308/accr-50211

[13] U.S. Securities and Exchange Commission (2011) SEC Disclosure Guidance: Topic No. 2. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[14] Gordon, L.A. (2007) Incentives for Improving Cybersecurity in the Private Sector: A Cost-Benefit Perspective. Congressional Testimony.

[15] Gordon, L.A. and Loeb, M.P. (2006) Managing Cybersecurity Resources: A Cost-Benefit Analysis. McGraw-Hill, Inc., New York.

[16] Gordon, L.A. (2004) Managerial Accounting: Concepts and Empirical Evidence. McGraw-Hill, Inc., New York.

[17] Target Corp. (2014) 10-K Report. https://corporate.target.com/annual-reports/2013/10-K/form-10-K

[18] C-SPAN (2017) Equifax Senate Banking Committee Hearing on Equifax Data Breach. https://www.c-span.org/video/?434469-1/equifax-ceo-testifies-senate-banking-panel

[19] Gartner, Inc. (2017) Gartner Says Detection and Response is Top Security Priority for Organizations in 2017. https://www.gartner.com/newsroom/id/3638017

[20] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2006) CSI/FBI Computer Crime and Security Survey. Computer Security Institute, San Francisco, CA. https://www.scribd.com/document/112548521/CSI-FBI-Computer-Crime-and-Security-Survey

[21] PwC (2017) Strengthening Digital Society against Cyber Shocks: Key Findings from the Global State of Information Security Survey 2018. https://www.pwc.com/us/en/cybersecurity/information-security-survey/strengthening-digital-society-against-cyber-shocks.html

[22] EY (2017) EY's 19th Global Information Security Survey 2016-17. http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/$FILE/GISS_2016_Report_Final.pdf

[23] Ponemon Institute (2017) 2017 Cost of Cyber Crime Study: Insights on the Security Investments that Make a Difference. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[24] U.S. Government (1996) Health Insurance Portability and Accountability Act (HIPPA). https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

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

[26] Gordon, L.A., Loeb, M.P. and Zhou, L. (2016) Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, **7**, 49-59. https://doi.org/10.4236/jis.2016.72004

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

[28] Armed Forces Communications and Electronics Association (AFCEA) (2013) The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. https://www.afcea.org/committees/cyber/documents/cybereconfinal.pdf

[29] Gordon, L.A. and Loeb, M.P. (2011) You May Be Fighting the Wrong Security Battles. *The Wall Street Journal.* https://www.wsj.com/articles/SB10001424053111904900904576554762089179984

[30] Palin, A. (2013) Maryland Professors Weigh Up Cyber Risks. *The Financial Times*. https://www.ft.com/content/606e0e5a-b345-11e2-b5a5-00144feabdc0

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

[32] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and 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**, 503-530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

[33] C-SPAN (2014) Target and Neiman Marcus Cybercrime and Privacy Congressional Hearing. https://www.c-span.org/video/?317553-1/hearing-cybercrime-privacy

[34] Malcolm, H. (2014) Target Breach Helps Usher in New World of Data Security. https://www.usatoday.com/story/money/business/2014/02/22/retail-hacks-security-standards/5257919/