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

Contents lists available at ScienceDirect

J. Account. Public Policy

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

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

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

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

A B S T R A C T

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

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

http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.001
0278-4254/

1. Introduction

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

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

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

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

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

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

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

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