Journal of Information Security, 2015, 6, 24-30
Published Online January 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.61003

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 23 September 2014; revised 20 October 2014; accepted 14 November 2014

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: Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, **6**, 24-30. http://dx.doi.org/10.4236/jis.2015.61003

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 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:

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

and

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

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 law-suits 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