Increasing cybersecurity investments in private sector firms

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

University of Maryland, College Park, MD 20472-1815, USA

*Corresponding author: E-mail: mloeb@rhsmith.umd.edu

Introduction

The percentage of US critical infrastructure assets owned by private sector firms is usually estimated to be somewhere in the neighborhood of 85% [Although the exact percentage is not known, the 85% figure has been used in various government reports (e.g. see http://www.gao.gov/products/GAO-07-39, accessed 26 October 2015)]. The way these assets are operated and managed has vastly changed over the last few decades due to the impact of the digital revolution related to computer-based information systems. These changes have increased the efficiency associated with using infrastructure assets. The digital revolution, however, has also created serious risks to the nation’s critical infrastructure due to actual and potential cybersecurity breaches (The term “cybersecurity” is used in this article to mean the protection of information that is transmitted via the Internet or any other computer network. The terms “cybersecurity” and “information security” are used interchangeably in this article). As noted by President Obama in his Executive Order on Cybersecurity of 12 February 2013:

Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront [1].

Numerous empirical studies point out the potential negative effects of these breaches on the performance of firms in the private sector (e.g. see [2]). The potential negative effects of cybersecurity risks and incidents on private sector firms have also been recognized by the US Securities and Exchange Commission (SEC), as evidenced by the publication of its Disclosure Guidance [3]. In fact, the SEC Disclosure Guidance recommends that firms disclose their cybersecurity risks and incidents in their annual 10-K reports.

The cybersecurity risks and incidents confronting private sector firms raise the following fundamental question: How much should a firm in the private sector invest in cybersecurity activities? Answering the above question has been the subject of Congressional Hearings (e.g. the 2007 Subcommittee of the US House Committee on Homeland Security), academic research (e.g. [4]), and discussions among executives (e.g. [5]). Unfortunately, there is no simple answer to this question. The above notwithstanding, it is helpful to keep in mind that private sector firms are driven to a large degree by the desire to earn profits. Consequently, cybersecurity investment decisions by private sector firms are largely the result of cost-benefit
analysis [In the private sector, cost-benefit analysis usually is based on some form of net present value (NPV) analysis].

Cost-benefit analysis, however, normally only considers the private costs associated with cybersecurity breaches (i.e. the costs to the firm directly affected by the breach). The externalities (i.e. spill-over costs to other firms, in both the private and public sectors, as well as to individuals) associated with cybersecurity breaches are generally not factored into the cybersecurity investment decisions by firms in the private sector (The sum of private costs and externalities is what economists refer to as social costs; an example of an externality related to cybersecurity would be a situation where a firm gets a computer virus and spreads that virus to its business partners through the firm’s computer interactions with these other firms. The spill-over costs would be the costs incurred by these business partners as a result of receiving the virus. If the spill-over costs could be easily traced to the firm spreading the virus, and the firm could be held liable for these costs, these costs would become part of the private costs of the firm spreading the virus). As Anderson and Moore [6] make clear the firm spreading the virus, and the firm could be held liable for these costs incurred by these business partners as a result of receiving the virus. If the spill-over costs could be easily traced to the firm spreading the virus, and the firm could be held liable for these costs, these costs would become part of the private costs of the firm spreading the virus). LeLarge ([7], p. 2210), emphasizing the effect of externalities, writes “security investments are always inefficient due to the network externalities.”

Holding externalities aside, there is evidence that firms invest in cybersecurity activities at a level below what would be optimal considering private costs alone. A cursory look at some firms that experienced a major cyberbreach recently (e.g. Target, Inc., JP Morgan Chase, Inc., and SONY, Inc.) indicates that it took a significant cyberbreach for the firms to ramp up their level of cybersecurity investments. Indeed, it is reasonable for the US federal government (hereafter referred to as the “government”) to assume that private sector firms are underinvesting in cybersecurity activities. Beginning with [8], the issue of incentive alignment has been a central theme in literature on the economics of cybersecurity. Pym et al. [9], for example, analyze the need for government intervention in cybersecurity in the context of an economic model of attackers and defenders. One should not be surprised, therefore, to find governments considering various incentives and/or regulations (hereafter referred to as government “incentives/regulations”) that would increase cybersecurity investments by firms in the private sector [The distinction between government “incentives” and “regulations” for purposes of this article is as follows. A government incentive (e.g. tax incentive for energy efficiency) provides some sort of subsidy to encourage firms to voluntarily take specific actions that are consistent with achieving a desired outcome. In contrast, a government regulation (e.g. [10]) is a law that mandates compliance with the law to achieve a desired outcome; pursuant to Presidential Executive Order 13636, the US Department of Homeland Security and the US Treasury Department have recently released reports examining possible incentives/regulations to motivate private firms to increase their investments in cybersecurity. In this regard, see [1, 11–13]].

The primary objective of this article is to apply and extend economic production theory to the problem of assessing the impact of actual or proposed government incentives/regulations designed to increase the cybersecurity investments by firms in the private sector. [While the model we present was motivated and is discussed in the context of cybersecurity, our analysis is more generally applicable to any loss-reducing investment by the firm (e.g. workplace safety or employee-theft prevention)]. The production theory framework is based on an analysis of the relationships among cybersecurity inputs and outputs. Our input–output analysis provides important insights regarding the impact of various types of government incentives/regulations designed to increase the cybersecurity investments by firms in the private sector (For purposes of this article, the terms “investments” and “expenditures” are used interchangeably). To our knowledge, this is the first study to conduct such an analysis.

The input–output analysis provided in this article shows that the impact of government incentives/regulations on the cybersecurity investment decisions of firms is dependent on two fundamental issues. The two issues are: (i) whether or not firms are utilizing the optimal mix of inputs to cybersecurity (i.e. whether or not firms are accurately conducting and using cost-benefit analysis related to the inputs of cybersecurity investments), and (ii) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. An analysis of these two issues results in general implications concerning whether government incentives/regulations will likely result in improvements in cybersecurity investments by private sector firms.

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

Literature review

Private costs of cybersecurity breaches

Cybersecurity breaches are a fundamental concern to firms in the private sector of an economy (Although outside the scope of this article, cybersecurity breaches are also a fundamental concern to organizations in the public sector, as well as to individuals). Estimates of the total costs associated with such breaches often are discussed in terms of billions of dollars. Estimates of the costs of a cybersecurity breach to an individual firm, hereafter referred to as private costs, are often based on surveys in which participants tend to consider only the explicit costs of such breaches (e.g. the costs of detecting and correcting breaches, as well as any actual loss of physical assets) [For example, the surveys conducted by several professional organizations (e.g. [14–16]) generally do not consider the implicit costs of cybersecurity breaches]. Once the implicit costs (e.g. potential lost sales, potential liabilities) are considered, the total actual losses to firms operating in the private sector could be closer to a trillion dollars. Although determining the exact dollar costs resulting from cybersecurity
breaches is problematic, there is little doubt that the number and sophistication of cybersecurity threats and breaches continue to grow (e.g. [15]).

One stream of empirical research on the costs of cybersecurity breaches has to do with the impact of such breaches on the stock market returns of firms that are publicly traded on the US stock exchanges [2, 17–23]. These studies are of particular relevance to the study contained in this article for the following three reasons. First, as noted in the introduction to this article, most of the critical infrastructure assets in the USA are owned by firms in the private sector, and the majority of these assets are owned by firms that are publicly traded on the US Stock Exchange (President Obama’s 12 February 2013 Executive Order 13636 [1] on “Improving Critical Infrastructure Cybersecurity” defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” As noted on the official website of the Department of Homeland Security (http://www.dhs.gov/critical-infrastructure-sectors, accessed 26 October 2015), critical infrastructure sectors include: the chemical sector, communications sector, energy sector, financial sector, healthcare and public health sector, transportation systems sector, the defense industrial base sector). Second, the impact of cybersecurity breaches on stock market returns implicitly considers such factors as potential lost sales and potential liabilities resulting from the breaches. Thus, the implicit, as well as the explicit, costs of cybersecurity breaches are incorporated into these studies (As noted earlier, empirical estimates of the costs of cybersecurity breaches based on surveys tend to ignore implicit costs. Florêncio and Herley [24] point out other serious methodological problems with such surveys). Third, the findings from these studies show that a particular cybersecurity breach could have a significantly negative impact on a firm, despite the fact that a large portion of these breaches does not have such an effect on firms.

A comprehensive study by Gordon et al. [2] examined the impact of cybersecurity breaches on the stock market returns of firms publicly traded on the US stock exchanges. Their study shows that, although some cybersecurity breaches do indeed have a statistically significant negative effect on firms, there has been a general downward shift in terms of the impact that cybersecurity breaches are having on firms (when measured in terms of the negative effect on the stock market returns of firms). These latter findings suggest, as pointed out by Gordon et al. [2], that investors are building up a tolerance for cybersecurity breaches and/or that firms are becoming much more adept at detecting and remediating such breaches prior to the point where such breaches cause critical damage to the firms. The above noted findings concerning the downward trend in the general impact of cybersecurity breaches on firms does not, however, negate the fact that devastating breaches can, and actually do, still occur. If anything, the findings by Gordon et al. [2] serve to highlight why it is so difficult to incentivize private sector firms to make the appropriate level of investments in cybersecurity activities. That is, the downward trend of the impact of cybersecurity breaches on stock market returns of firms in the private sector highlights the difficulties associated with expecting private sector firms to voluntarily incorporate the cost of externalities of such breaches in their decision-making. Furthermore, since the cybersecurity breaches seem to be having a decreasing effect on the stock market returns of firms experiencing the breaches, a real danger is that the tendency by private sector firms to underestimate the private costs associated with cybersecurity breaches will increase.

Cybersecurity investments considering only private costs

Investments on cybersecurity activities are best viewed in a manner similar to the way other investments are considered by an organization. In the private sector, this essentially means that benefits from investments need to be compared to the costs associated with such investments. In terms of accepting or rejecting an incremental cybersecurity investment opportunity, the basic analysis consists of computing the NPV. The use of cost-benefit analysis for efficiently allocating scarce resources (i.e. making the business case) is well established in the capital investment literature including the literature on investments in cybersecurity (e.g. see [25]).

The preceding discussion refers to the way a private sector firm might look at an incremental investment related to cybersecurity [Sophisticated models take into consideration such factors as real options (e.g. [26–28])]. Alternatively, if the firm were trying to optimize the total level of investments in cybersecurity activities, then the firm would want to minimize the sum of the costs of the cybersecurity investments plus the costs of the cybersecurity breaches. A rigorous approach to determining the optimal level of cybersecurity investments is provided by the Gordon-Loeb Model [4]. Gordon and Loeb [4] present an economic model to examine the optimal investment level of information security for a risk-neutral firm. Gordon and Loeb [4] show that, for two broad classes of cybersecurity breach functions, the optimal investment in information security is always less than or equal to $1/e$ (approximately, 36.79%) of the expected loss from a security breach. Although [4] demonstrated this result for only two (broad) classes of security breach functions, they conjectured that the $1/e$ rule is more general. Baryshnikov [29] proved that the $1/e$ rule “holds in full generality.” LeLarge [7] also proved the generality of the $1/e$ optimal investment rule.

Externalities and the social costs of cybersecurity breaches

As noted in the Introduction, externalities that arise from the networked environment play a significant role in the underinvestment in cybersecurity. One type of externality arises because some costs of a cybersecurity breach are imposed on other firms and consumers and are not borne by the firm experiencing the (initial) breach. An extreme example of such a negative externality arises when a cybersecurity breach results in a firm’s computers becoming part of a botnet. In this case, a cybersecurity breach could result in a firm’s computers launching attacks that are costly to consumers and other firms, but not costly to the firm that unknowingly hosts a source of the attack. Such a negative externality results in a firm’s private costs of a cybersecurity breach understating the social costs of a cybersecurity breach.

In contrast to negative externality, investing in cybersecurity creates a positive externality by decreasing the likelihood of a cybersecurity breach to consumers and other firms (as well as to the investing firm). This latter case (i.e. a positive externality) results in a firm’s private benefits from cybersecurity investment understating the social benefits of such investment. Given that firms recognize that their own cybersecurity is enhanced by the cybersecurity investments of other firms, cybersecurity acts to a degree like a public good and gives rise to firms free-riding on the cybersecurity investments of others. Without added incentives/regulations, firms do not take into account the externalities affecting social costs and benefits, thus leading to cybersecurity underinvestment. Furthermore, when the externalities associated with national security aspects of the critical infrastructure assets owned by private sector firms are considered, private costs and benefits of cybersecurity investment
further diverge from the social costs and benefits, thus accentuating the cybersecurity underinvestment problem.

Combating the underinvestment problem
Since the problem of underinvestment in cybersecurity has been well recognized, scholars, as well as information security professionals, have addressed the issue and analyzed a number of policy strategies designed to boost cybersecurity investment. One significant stream of research in the cybersecurity literature began with [30] (Moore and Anderson [31] provide a nice discussion of papers in this stream of literature). Taking into account the public goods nature of cybersecurity investment, Varian [30] provides a game-theoretic analysis of three scenarios where the overall reliability of the network depends on: (i) the efforts of all firms; (ii) on the effort of the firm supplying the smallest effort; and (iii) on the effort of the firm supplying the largest effort. Allowing the costs of effort to vary across firms, Varian [30] compares the social optimal with equilibrium under a strict liability policy and under a negligence policy. Note that in order to calculate the social optimal and determine optimal policies, the cost of effort must be known for each firm (in addition to function mapping effort to the probability of breach). Since the cost of effort may well be private information held by firms, asymmetric information is a further barrier to attaining the social optimal. Groves and Loeb [32] present a mechanism designed to handle such a problem in the context of public inputs. With the liability policy, a fine is imposed on firms when there is system failure (i.e. the occurrence of a breach); and with the negligence policy, a fine is only imposed on a firm if it failed to meet a predetermined standard level of effort (due care). While the liability policy only levies a fine after the system failure, Varian [30] recognized that via cybersecurity insurance, standards could be imposed ex ante.

The use of ex ante negligence policies has been widely used in other contexts and has been proposed as a remedy for cybersecurity investment. Anderson et al. [33] note the analogy with car safety and recommend that the European Union develop standards for network-connected equipment. Sales [34] also discusses the use of standards as a possible remedy to underinvestment in cybersecurity and Bauer and van Eeten [35] lists information security standards as a technical measure of promise. As can be seen by the title of his article, “A Voluntary Cybersecurity Framework is Unworkable – Government Must Crack the Whip,” Gyenes [36] goes further in advocating mandatory cybersecurity standards.

The model we present and analyze in the next section of this article considers regulation from an ex ante negligence perspective rather than form an ex post liability perspective. Shavell [37], in the context of safety regulation, demonstrated that neither the ex ante nor ex post approach to motivating the welfare maximizing level of effort “... is necessarily better than the other and, their joint use is generally socially advantageous” [37, p.271].”

Information disclosure, information sharing, and the promotion of cyberinsurance have also been proposed as means of encouraging firms in the private sector to invest more in cybersecurity. Romanosky et al. [38], while not directly examining whether or not added disclosure requirements lead to increased cybersecurity investment, examine the impact of data breach disclosure laws on reducing identity theft. Gordon et al. [39] and Gal-Or and Ghoze[40] provide game-theoretic models to investigate the benefits of information sharing. Cybersecurity insurance has also been investigated as a means of providing firms an incentive to strengthen their cybersecurity defenses. Insurance policies that require a level of due care (i.e. de facto standards) to attain a policy, or otherwise price policies (e.g. vary deductibles, premiums, and coverage) based on the policy holder’s cybersecurity defenses, provide such an incentive (Böhme and Schwartz [41] provide an excellent review of the cyberinsurance literature, while also providing a framework that unifies the literature as well as providing a guide for further research). Moore [42] examines additional incentive and regulatory strategies designed to increase cybersecurity investments by private firms (as well providing further discussion and analysis of the strategies presented above).

Cybersecurity inputs and outputs
Basic analysis
As pointed out in “Introduction” section, private sector firms will usually underinvest in cybersecurity. Accordingly, it is reasonable for the government to develop incentives/regulations to offset this underinvestment tendency. Ideally, the government would like to provide incentives/regulations to increase cybersecurity investments in private sector firms based on some target level of cybersecurity.

Following this logic, the incentives/regulations would be based on the outputs of the firms’ inputs (or activities) related to cybersecurity. Under such an approach, the government would let firms decide on the best mix of inputs to use in order to reach the target level of cybersecurity. In reality, however, there is little agreement on how to measure the cybersecurity level of firms. For example, should the number of breaches, the time it takes to identify and remediate breaches, or the total social costs associated with breaches be this output measure? Furthermore, even if there were agreement on which metric to use, we would still be left with the problem of agreeing on the right way to quantify the metric. As a result of the difficulties associated with defining and measuring the level of cybersecurity, it is common, as well as rational, for the government to consider incentives/regulations based on the inputs to strengthen cybersecurity (e.g. security systems such as intrusion detection/preventions systems, antivirus software, one time password tokens, improved software, firewalls, encryption, internal control systems, training programs, two-factor authentication and security policies and standards) (As previously noted, there are parallels between issues surrounding automobile safety and cybersecurity. The use of input regulation in the auto industry is widespread with government standards for everything from bumpers to padded instrument panels to brakes).

The relationships between the inputs and outputs of cybersecurity are illustrated in Fig. 1. This figure illustrates a case where a firm has three possible levels of cybersecurity represented by the three ISOSEC curves (ISOSEC3 > ISOSEC2 > ISOSEC1). Each ISOSEC curve in Fig. 1 represents the same level of cybersecurity for different combinations of inputs to cybersecurity. It is assumed, in Fig. 1, that the firm has two, and only two, inputs (X and Y) to improve its cybersecurity level (Due to positive network externalities, the firm’s cybersecurity level (output) would also depend on the cybersecurity outputs (and, therefore, indirectly on the cybersecurity inputs) of all other firms. In our analysis, we assume all other firms’ cybersecurity levels are fixed and concentrate on the first-order effects of input regulation). Let x represent the units of input X and let y represent the units of input Y. For simplicity, we assume the measure of X is such that the cost of a unit of X is one dollar, and similarly the measure of Y is such that the cost of a unit of Y is one dollar. Thus, one could think of x as the dollar expenditures for input X and y as the dollar expenditures for input Y.

The horizontal axis in Fig. 1 measures the amount of one cybersecurity input (e.g. timeliness of patch updating of the firm), denoted as X, for which we assume the government can get verifiable data. The
vertical axis measures the amount of a second cybersecurity input (e.g. software quality) or a composite of all other security inputs, denoted as $Y$, for which we assume the government cannot attain a verifiable measure. The firm’s level of cybersecurity is determined by the level of inputs $(x, y)$. As noted above, each ISOSEC curve is the set of all pairs of inputs $(x, y)$ resulting in a given level of cybersecurity and is assumed to be convex to the origin. The budget, $B$, for expenditures on cybersecurity inputs is the line segment given by the set \[ f(x, y) = \{ (x, y) \mid x/C_21 \leq 0, \ y/C_21 \leq 0, \ x+y=B \}. \] Dotted lines in Fig. 1 represents the budget lines for three budget levels, where $B_3 > B_2 > B_1$.

An efficient firm expands its ex ante cybersecurity level (i.e. decreases the probability of a cybersecurity breach) by selecting a combination of cybersecurity inputs where the budget line is tangent to an ISOSEC curve. The point of tangency is where the marginal benefit (i.e. the marginal increase in the cybersecurity level) of input $X$ equals the marginal benefit of input $Y$ [We have assumed the inputs are measured in a way that one unit of each input cost one dollar. More generally, the point of tangency is where ratio of prices of the cybersecurity inputs equals the marginal rate of technical substitution of the cybersecurity inputs (i.e. the ratio of the marginal benefits of the inputs)]. At that point, the firm reaches the highest ISOSEC for a given budget level. In other words, an efficient firm spends its given budget for cybersecurity activities on the optimal mix of inputs, given the costs of the different outputs. This will map out on the firm’s optimal cybersecurity expansion path shown in Fig. 1. If a firm were to take into account externalities, this would not change the firm’s expansion path [Taking externalities into account, however, would lead the firm to operate at a higher point on the expansion path. This statement is based on the assumption that externalities are only associated with the occurrence of a cybersecurity breach, and implicitly assumes that there are no externalities (e.g. pollution effects) associated with the use of one or more of the inputs $(X$ and $Y$)].

Now let us look at Fig. 2, and assume that the firm initially has a budget for cybersecurity expenditures equal to $B_1$. If the firm were efficient in its allocation of the cybersecurity budget ($B_1$) to inputs $X$ and $Y$ (i.e. the firm knows and uses the optimal mix of $X$ and $Y$ for a budget level of $B_1$), it would select the combination of inputs equal to $x_1$ and $y_1$. That is, $(x_1, y_1)$ represents the efficient allocation of $B_1$, in terms of providing the maximum cybersecurity level of ISOSEC$_1$. However, suppose that the government wants to raise the level of cybersecurity achieved by this firm to a target cybersecurity level of ISOSEC$_T$. That is, even if it were assumed that the firm is investing the optimal amount to cover its private costs of cybersecurity breaches, the government could believe the firm is not investing enough to cover the externalities associated with such breaches. Notice that this latter argument is independent of the government’s ability to measure the exact level of security.

To raise the firm’s cybersecurity level to ISOSEC$_T$, let us assume the government imposes a regulatory constraint on $X$ of $x_R$ (recall that the government can get verifiable data on $X$). In this article, we focus on the frictionless case where the regulator can enforce input standards without cost. In practice, the regulator could audit a firm’s compliance with the standards at a cost, although the audit would be imperfect [If we relax the assumption that the regulator can enforce the standards without costs, then adding compliance to our analysis would require considering the cost of auditing by the

---

**Figure 1.** Cybersecurity expansion path.
regulator, the penalties for non-compliance, and the fact that firms take into account the imperfect (i.e. probabilistic) nature of auditing. To the extent that firms take into account imperfect and costly enforcement, compliance would be lessened, as would the actual benefits of such input regulation; note that while enforcement of *ex ante* standards is imperfect and costly, enforcement of *ex post* liability rules are also imperfect and costly. Shavell [37] highlights two enforcement problems with liability rules: (i) prosecution is uncertain, and (ii) penalties sufficient to induce optimal behavior may not be feasible because of firms’ inability to pay such penalties.

However, under this scenario we also assume that the firm is not willing (or cannot afford) to raise its budget to \( B_2 \). In other words, we assume the firm’s budget is fixed at \( B_1 \). The firm would solve this constrained optimization problem by setting \( X \) at the \( x_R \) level and setting \( Y \) at the \( y_R \) level shown in Fig. 2. As shown in Fig. 2, at \((x_R, y_R)\), the cybersecurity level attained would be \( \text{ISOSEC}_R \), which represents a lower level of cybersecurity than the pre-regulation level of cybersecurity of \( \text{ISOSEC}_1 \). Thus, with the assumption that the firm remains with its initial cybersecurity budget constraint of \( B_1 \), the government regulation actually motivates the firm to decrease its level of cybersecurity. In other words, after complying with the regulation on input \( X \) (i.e. \( x \geq x_R \)), but not increasing its overall budget for cybersecurity spending (i.e. keeping the budget at \( B_1 \)), the firm is no longer using its inputs in an efficient manner. Suppose the firm responded to the regulation by increasing the cybersecurity budget by an amount less than \((x_R-x_1)\), so that the new budget equals \( B_0 \), where \( B_1 < B_0 < B_2 \). One can easily verify that there exists a threshold budget level, call it \( B_T \), where \( B_1 < B_T < B_2 \) such that for \( B_0 > B_T \), the firm responding to the regulation would select input levels such that the cybersecurity level would be less than the initial level \( \text{ISOSEC}_1 \). For example, if the firm were initially allocating its cybersecurity budget of \( B_1 \) inefficiently (i.e. the firm does not know the optimal mix of inputs for a given budget level) and spending \( x_1 \) on \( X \) and \( y_1 \) on \( Y \), a government regulation that forced the firm to spend \( y_1 \) on \( Y \) could possibly move the firm to spend \( x_1 \) on \( X \) instead of \( x_R \). In this scenario, the firm’s cybersecurity level would move from the \( \text{ISOSEC}_R \) to the \( \text{ISOSEC}_1 \), given the budget constraint of \( B_1 \) (Fig. 2).

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

![Figure 2. Inappropriate regulatory strategies can cause firms to reduce their overall levels of cybersecurity.](https://academic.oup.com/cybersecurity/article-abstract/1/1/3/2367124/132287104)
Implications
The preceding analysis shows that the potential for government incentives/regulations to increase cybersecurity investments by private sector firms is dependent on the following two fundamental issues: (i) whether or not firms are utilizing the optimal mix of inputs to cybersecurity, and (ii) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. Thus, three general implications are apparent from our input–output framework provided above. First, if it were assumed that the total expenditures by firms on cybersecurity activities (i.e. the budget for spending on cybersecurity inputs) are fixed, and that firms are already utilizing the optimal mix of cybersecurity inputs, for different levels of spending on cybersecurity (i.e. firms know the optimal expansion path shown in Fig. 1), government incentives/regulations that encourage changes in the resource allocations among cybersecurity inputs would lower the firms’ level of cybersecurity.

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

Third, if it were assumed that the cybersecurity budget of an organization is not fixed (i.e. relax the firm’s initial budget constraint), government incentives/regulations (e.g. mandatory cybersecurity standards, or tax incentives related to specific cybersecurity inputs) that encourage organizations to increase their cybersecurity investments could increase the cybersecurity level of such organizations. Whether or not the firm knows its optimal mix of inputs, a sufficient condition for an increase in a firm’s cybersecurity level is that the incentives/regulations would not cause a lowering of the expenditures on one or more cybersecurity inputs. There exist, however, other sufficient conditions such that even if the regulation on one input results in the lowering of expenditures on other inputs, the overall cybersecurity level would increase. If a lowering of the expenditures on some cybersecurity inputs were to occur, then the ultimate result on the cybersecurity level of a firm would be dependent on how the input level changes affect the marginal benefits of inputs (i.e. the output of cybersecurity input activities) could be unambiguously measured, then regulation on outputs would likely be the most effective means of addressing externalities.

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

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

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

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

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

If a security breach actually occurs, the firm will suffer a private monetary loss \(L\) and other firms, organizations, and individuals will suffer the external loss denoted as \(L^E\).

Assume the firm is able to determine the optimal mix of cybersecurity inputs (taking into account only its private costs, \(L\)). When making security investment decisions in the absence of regulation (and considering only private costs), the firm would choose cybersecurity expenditure levels of \(X\) and \(Y\) so that its total expected net benefits from the expenditures (i.e. the reduction in the expected private loss from a cybersecurity breach less the costs of the cybersecurity expenditures) is maximized. Letting \((x_1, y_1)\) denote the firm’s optimal levels of cybersecurity inputs in the absence of regulation, we have \((x_1, y_1)\) as the solution to the firm’s maximization problem [This optimization assumes that the firm’s cost-benefit analysis ignores the costs of externalities. Thus, what is referred to as the firm’s optimal level is the firm’s (private costs) optimal level, not the social welfare optimal]:

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

Denote \(S_1 = S(x_1, y_1, v)\), so that, \(S_1\) represents the optimal cybersecurity level that is obtained in the absence of regulation. In the presence of externalities (i.e. \(L^E > 0\)), however, the firm’s level of cybersecurity, \(S_1\), is below the socially optimal level [See [43] for an analysis of the magnitude of a firm’s underinvestment caused by ignoring the costs of externalities]. We denote the firm’s total level of cybersecurity expenditures in the unregulated case as \(B_1\), where \(B_1 = x_1 + y_1\).

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

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

For this scenario, the government requires the firm to spend at least $x_0$ on input $X$, where $x_0$ is greater than the initial unregulated level, $x_1$ and the firm is assumed to have to choose inputs levels $(x', y)$ such that $x' > x_0 = B_1$ (i.e. the total cybersecurity expenditures remain at the unregulated optimal amount). Formally stated, $(x', y)$ solves the firm’s following maximization problem:

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

s.t. $x + y = B_1$

$x \geq x_R$

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

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

$$x' = x_R > x_1,$$

$$y_R < y_1,$$

and

$$S_R > S_1.$$

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

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

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

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

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

For this scenario, assume prior to the introduction of the government regulation, the firm’s cybersecurity inputs are $(x_R, y_R)$, which may, or may not, differ from the optimal unregulated input mix $(x_1, y_1)$. Let $(x_R, y_R)$ be the firm’s input mix after the regulation. The government regulation requires the firm to spend at least $x_0 > x_R$ on $X$, so that regulation can be stated as $x_0 \geq x_R > x_R$. For this scenario, the firm’s cybersecurity level will increase, as will the firm’s budget for cybersecurity inputs. This observation is stated formally in the next proposition and the (straightforward) proof appears in the Appendix A.

Proposition 3 Assume the firm’s current cybersecurity input mix is $(x_R, y_R)$ and the firm meets the government regulation that $x_0 \geq x_R > x_R$ without decreasing its expenditures on input $Y$. Then the firm’s cybersecurity level will increase (i.e. the firm’s probability of a cybersecurity breach will decrease) and the firm’s budget for cybersecurity inputs will also increase.

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

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

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

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

s.t. $x \geq x_R$,

where $x_R > x_1$.

Denote $\hat{S} = S(\hat{x}, \hat{y}, v)$ (i.e. $\hat{S}$ represents the probability that a cybersecurity breach occurs under regulation) and define $\hat{B} = \hat{x} + \hat{y}$ as the total level of cybersecurity expenditures for the regulated case. The constraint $x \geq x_R$ must be binding [This can be shown by first assuming that $\hat{x} > x_R$. This means that $(\hat{x}, \hat{y})$ is a solution to $\max_{x,y} \left[ v - S(x, y, v) \right] | L - x - y$ without the constraint, i.e. $(\hat{x}, \hat{y}) = (x_1, y_1)$, which contradicts the assumption that $\hat{x} > x_R > x_1$. Hence, $x \geq x_R$ is a binding constraint]. Hence we have $x = x_R$.

In the next two propositions, we provide two sufficient conditions for the government regulation to result in a decrease in the probability of a cybersecurity breach. The first sufficient condition is that the cybersecurity inputs $x$ and $y$ are weakly complementary over the interval $[x_1, x_R]$, in the sense that an increase in $x$ will not decrease the marginal benefit of an increase in $y$ [Our use of the term weakly complementary is in the spirit of the discussion on production inputs in Ferguson (1969, p. 71)]. Formally, we assume $S_{xy} = \frac{\partial^2 S(x, y)}{\partial x \partial y} \leq 0$. 


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

We now examine the case where X and Y are not weakly complementary inputs. In that case, \(S_{xy} > 0\), and the inputs are said to be “competitive” in the sense that the marginal benefit of input Y declines when the input X increases. In this case, whether the regulation would induce a lower probability of a cybersecurity breach occurring is ambiguous. The firm is mandated to spend more on input X but would at the same time reduce expenditures on input Y (This can be proved in a similar fashion as Proposition 4), since the marginal benefit from input Y is now smaller. As a result, the decrease in the probability of a cybersecurity breach occurring from more spending on input X could be partly or even more than offset by the increase in the probability of a breach occurring due to less spending on input Y.

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

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

Proposition 5  If \(-\frac{S_{x_y}}{S_{x_y}} < \frac{S_{x_y}}{S_{x_y}}\) over interval \([x_1, x_R]\), it follows that \(S(\hat{x}, \hat{y}, v) < S(x_1, y_1, v)\).

Figures 4 and 5 summarize our analysis for Scenario 3B, i.e. when the firm is able to determine the optimal input mix and optimally adjusts the cybersecurity expenditure budget in response to the regulation. A regulation that increases expenditure on activity X from \(x_1\) to at least \(x_R\) would induce the firm to strictly obey the regulation and set \(\hat{x} = x_R\). The post-regulation input Y, however, may move along the vertical line at \(x = x_R\). In Figure 4, the solid vertical line at \(\hat{x} = x_R\) represents the region where the regulation would lower the probability of a cybersecurity breach (i.e. increase the cybersecurity level). Any breach probability functions that satisfy our sufficient condition \(-\frac{S_{x_y}}{S_{x_y}} < \frac{S_{x_y}}{S_{x_y}}\) would have post-regulation input mix falling into this region.

When X and Y are weakly complementary inputs, the firm would choose not to decrease input Y and the total cybersecurity level would increase. When X and Y are competitive inputs, the firm would decrease expenditures on input Y, but as long as the condition \(-\frac{S_{x_y}}{S_{x_y}} < \frac{S_{x_y}}{S_{x_y}}\) holds, the post-regulation cybersecurity level would still be higher. In Fig. 5, we combine Figs 3 and 4 to highlight that there is a region where the post-regulation \(y\) decreases and the probability of a cybersecurity breach also decreases (i.e. we have a higher cybersecurity level). In other words, a regulation may be able to lower the probability of a cybersecurity breach, even though the regulation results in a lowering of other inputs (i.e. input Y).
To provide the readers with examples, we consider a generalized version of the two single cybersecurity input breach functions discussed in [4]. These functions are $S^i(x, y, v) = \frac{a(x_1 + 1)^\beta_1}{(x_2 + 1)^\beta_2}$ for some $\alpha_1, \alpha_2 > 0, \beta_1 \geq 1, \beta_2 \geq 1$, and $S^i(x, y, v) = \frac{\alpha_1 x + 1 + \beta_1 y + 1}{\alpha_2 x + 1 + \beta_2 y + 1}$ for some $\alpha_1, \alpha_2 > 0$ [They include broad classes of functions widely used in economics literature. It can be easily verified that they satisfy conditions (1-4)]. In Appendix A, a straightforward proof is given to show that these functions satisfy Proposition 5. That is, for these generalized functions, the post-regulation optimal expenditures on input $Y$ decrease, yet the probability of a cybersecurity breach decreases.

Finally, we note that the model presented in this section, while providing insights in the context of cybersecurity, can also be used to analyze incentive/regulation in other contexts where the government seeks remedies for market failures due to externalities (e.g. pollution abatement and product safety). The economics literature on remedying externality problems is vast and continues to grow. For example, Cropper and Oates [44] provide an insightful review and analysis of externality remedies. Their analysis includes coverage of such classic economic remedies such as the imposition of Pigouvian taxes, marketable pollution permits, and standards. The parallels between environmental problems and cybersecurity problems have been noted before, most prominently by Camp and Wolfram [45] in suggesting marketable vulnerability permits.

**Existing government actions affecting cybersecurity investments**

Although there is as an a priori argument that firms will likely underinvest in cybersecurity activities, the government has already taken several actions that either have, or have the potential to, significantly offset the tendency by firms to underinvest in cybersecurity [The government actions discussed in this section (as well as the input incentive/regulations analyzed in our model) have no direct impact on security incentives of IT producers (i.e. software manufacturers, network operators, and network hardware manufacturers). Instead, these government actions affect the demand for improved cybersecurity, which in turn should provide indirect incentives for IT producers. Clearly, the design and analysis of direct incentives/ regulation for IT producers, while outside the scope of this article, is a topic worthy of further investigation (e.g. see [46]). Given the conditional impact of government incentives/regulations on cybersecurity investments by private sector firms, it is strongly recommended that the existing actions be recognized, evaluated, and more effectively utilized before, or at least in conjunction with, considering new government incentives/regulations concerning cybersecurity investments. Two such actions of particular note are the Sarbanes-Oxley Act of 2002 and the 2011 SEC Disclosure Guidance on Cybersecurity Risks and Cyber Incidents (Although these actions pertained only to publicly traded firms, such firms include virtually all of the firms that own an element of the nation’s critical infrastructure). Before examining these two government actions, we highlight some other government actions that are closely aligned with our analysis of incentives and regulations of cybersecurity inputs.

Regulations that specify security processes to be followed are, in essence, regulations on a set of inputs. For example, the 1999 Gramm-Leach-Bliley Act [47] “... obliges banks to protect the security and confidentiality of customer information by ... specifying processes that banks must comply with, such as adopting a written information security program and establishing programs to assess and manage operational risks ([42], p. 106).” Our emphasis on regulating inputs is consistent with regulation security processes, providing that the regulation on security processes does not include regulating all inputs. That is, our analysis provides insights to any situation where some, but not all, inputs are regulated.

Another example of a direct government regulation on inputs is the de facto regulation of firms by having them comply with a cyber regulation, so that they can avoid the imposition of a penalty. For example, some states do not require firms to make notifications of breaches if the data are encrypted [48]. A final example is the proposed mandatory strong authentication of identity requirement for critical infrastructures proposed in a Commission Report chaired by US Representatives Langevin and McCaul, Scott Charney and Lt. General Raduige [49].

**Sarbanes-Oxley Act**

The Sarbanes-Oxley Act (SOX) of 2002 requires firms to have strong internal control systems in place, where internal control systems are defined in terms of reliable financial reports (see Sections 302 and 404 of SOX). In a modern computer-based information system environment, firms cannot produce reliable financial reports results without having secure computer systems. For accelerated filers, SOX (Section 404) requires external auditors to attest to the quality, or lack thereof, of the firm’s internal controls of their financial information reporting systems. SOX, as modified by the Dodd-Frank Act of 2010, requires only accelerated firms to have external auditors attest to the quality of internal controls. Generally speaking, accelerator firms are large firms, with revenues over $75 million per year (see [50]). As indicated in various empirical studies, one category of market weaknesses (MW) in internal control systems identified by managers and auditors has to do with the security of computer-based information systems (e.g. [51]). More generally, it has been shown that MW in internal control systems have a negative impact on the cost of equity firms [52, 53].

Presumably, the SOX reporting requirements have been accompanied by an increase in cybersecurity investments. Unfortunately, since firms in the private sector do not disclose the level of expenditures on cybersecurity activities as a separate category on their financial reports filed with the SEC, the presumption that the passage of SOX had a positive impact on the cybersecurity investments of firms has never been verified. Furthermore, since SOX only applies to financial reporting systems (With the increasing use of integrated enterprise systems, an increasing percentage of a firm’s IT systems affect the financial reporting systems of firms), its ability to motivate firms to make the appropriate level of cybersecurity investments is limited. The above notwithstanding, the fact that firms are required to report their MW in their 10-K reports filed with the SEC (which include MW related to the security of their computer-based information systems) leads us to conjecture that SOX has motivated corporate executives to increase their expenditures on at least one cybersecurity input beyond what they would be without SOX. More to the point, we believe that SOX is already operating as a government incentive for firms to allocate additional investments to their internal control system, which is clearly an important input to cybersecurity. In terms of our model, this additional investment in the cybersecurity input of internal control would essentially shift the expenditure level toward some unspecified higher level (i.e. moving the expenditures on $x_1$ toward what our model calls $x_2$).

Gordon et al. [54] provide evidence that is consistent with this conjecture. They show that firms listed on the US Stock Exchanges have significantly increased their voluntary disclosures of
cybersecurity related activities. The fact that these voluntary disclosures are associated with a statistically significant increase in the stock market returns of the disclosing firms (see [55]) provides additional support for this conjecture.

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

SEC Disclosure Guidance

The SEC Disclosure Guidance on Cybersecurity Risks and Cyber Incidents [3] is another government action that is particularly germane to the issue of cybersecurity investments by private sector firms. Although the SEC Disclosure Guidance related to cybersecurity is technically speaking not a binding requirement, the fact that the disclosure is voluntary will provide a poor defense in the event of a suit by investors. Unlike SOX, which is focused on the inputs to cybersecurity via its emphasis on computer-based information systems, the SEC Disclosure Guidance focuses on the cybersecurity output in terms of cybersecurity risks and incidents. As stated in the SEC Disclosure Guidance:

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

Many firms have reacted to the SEC Disclosure Guidance with an extensive discussion of the cybersecurity risks facing their firms in Item 1A of their 10K as well as the Management Discussion Section of the firm’s 10K, filed with the SEC. In Appendix B, we present the Risk Factors reported by Lockheed Martin in their 10-K for 2013 as a representative example of a rapidly growing trend by firms to voluntarily report information concerning cybersecurity activities on the 10-K reports. In fact, since the SEC’s Disclosure Guidance was published in 2011, one is hard pressed to find a major corporation that does not voluntarily report some sort of information concerning its cybersecurity activities. This trend notwithstanding, we are still only able to conjecture that the increased reporting of cybersecurity related activities are accompanied by an increase in cybersecurity investments. In other words, while it seems reasonable to assume that corporate executives are increasing their level of investments in cybersecurity related activities as a result of the SEC Disclosure Guidance, hard evidence supporting this conjecture does not currently exist (As noted earlier in the article, there is scant information on the actual level of investments in cybersecurity activities by firms. The information that does exist is based largely on survey data which is of questionable reliability due to such problems as nonresponse bias, difficulty in verifying the actual respondent, and difficulty in verifying the amounts reported. Thus, it is difficult, if not impossible, to prove or disprove the accuracy of this statement). In fact, there have been calls for changing the SEC’s Disclosure Guidance on cybersecurity risks and incidences to a more formal regulation that requires firms to disclose more detailed information than currently is taking place. A leading advocate of this latter position is Senator John Rockefeller. In a letter to the SEC Chairperson (Ms. Mary Jo White) on 9 April 2013, Senator Rockefeller wrote [56]:

In October 2011, the SEC responded to my request and announced that it was issuing staff guidance on disclosure obligations regarding cybersecurity risks and cyber incidents. I applauded this decision as an important first step in the right direction, and it certainly made a positive impact on disclosures. However, given the growing significance of cybersecurity on investors’ and stockholders’ decisions, the SEC should raise the guidance to the level of a Commission rule.

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

Other examples of government actions affecting cybersecurity investments

Besides SOX and the SEC Disclosure Guidance, there are many industry-specific government regulations that are likely to offset the tendency by private sector firms to underinvest in cybersecurity inputs. Two such regulations that have presumably had a significant effect on increasing cybersecurity investments in private sector firms are the Gramm-Leach-Bliley Act (GLB) of 1999 [47] and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [57]. GLB and HIPAA impose stringent privacy and information security rules on financial institutions and health providers, respectively. As a result, both of these Acts provide strong incentives for firms in the private sector to increase their investments in cybersecurity inputs [58]. Presumably, the firms affected by these laws are investing enough in cybersecurity to cover the private costs and at least some of the externalities resulting from cybersecurity breaches. Anecdotal evidence provided to the authors, by a variety of firms in both of these industries, confirms this presumption. Unfortunately, we have no way of knowing if this anecdotal evidence is generalizable because private sector firms do not provide public information on the...
actual expenditure level of investments in cybersecurity activities. However, the significant penalties associated with noncompliance to these Acts suggest that this evidence about increased cybersecurity investments is likely to be true.

The above noted industry-specific regulations only apply to two specific sectors of the nation’s critical infrastructure. There are other regulations that apply to a specific subset of firms or sectors. For example, in 2003 California enacted the Notice of Security Breach Act [59] which requires that any company that maintains personal information of California citizens and has a security breach threatening the confidentiality of that information must disclose the details of the event. Clearly, this regulation motivates firms to increase their investments in a variety of cybersecurity inputs in an effort to avoid the likelihood of disclosing of a security breach. However, unless government agencies were to come up with regulations for each and every sector of the critical infrastructure (a very unlikely scenario), general incentives/regulations to encourage firms to make the appropriate level of cybersecurity investments are required. The reporting of MW under SOX, and the SEC’s guideline on cybersecurity risks and cyber incidences, represent two examples of the types of general incentives/regulations that can help accomplish the goal of increasing cybersecurity investments among a broad array of private sector firms that own US critical infrastructure assets.

Concluding comments

President Obama has recognized the importance of cybersecurity to the US national security (e.g. [1]). Recognizing the importance of cybersecurity is a necessary first step in resolving the challenges associated with cybersecurity risks and incidents. The next step, however, is to find solutions to these challenges. One such challenge, which has been the focus of this article, has to do with the tendency by firms in the private sector to underinvest in cybersecurity. Thus, it is appropriate for governments to consider the use of incentives and regulations to offset this tendency. Based on an input–output analysis, this article has examined the conditions under which incentives/regulations are likely to be most effective in encouraging a more appropriate level of cybersecurity investments by private sector firms.

Two examples of existing US federal government actions affecting cybersecurity investments were also discussed in this article. These examples are the Sarbanes-Oxley Act of 2002 and the 2011 SEC Disclosure Guidance on Cybersecurity Risks and Incidents. As pointed out in this discussion, the government would be wise to examine existing incentives/regulations before, or at least in conjunction with, initiating new ones. In particular, we believe that even as other incentives/regulations are being considered, a more effective utilization of SOX and the SEC Disclosure Guidance could go a long way toward resolving the problem associated with underinvestment in cybersecurity activities by a large subset of private sector firms.

It should be noted that private sector firms do not make cybersecurity investments in isolation of other firm-related investment decisions (e.g. new product investments). A limitation of this article is that we did not consider these other investment decisions in our discussion. In other words, cybersecurity investments need to compete for scarce organizational resources. Thus, no matter how carefully one tries to analyze the impact of government regulations and/or incentives related to cybersecurity investments on private sector firms, the ultimate impact will be determined by a variety of interactive concerns, many of which are unrelated to cybersecurity issues. In addition, government policies are often considered and adopted as a set of policies. As a result of this integrative process of government policies, the productivity of information security could also be changed by policies concerning other factors. Thus, looking at individual government policies directed at information security in isolation of other government policies could lead to misleading conclusions concerning the impact of the changes in the information security policy.

It is important to monitor the derivative effect of any incentives/ regulations directed at improving cybersecurity investments by private sector firms. One component of such monitoring is the gathering of data on the level of investments in cybersecurity activities by private sector firms vis-a-vis other firm-level investments (e.g. capital investments unrelated to cybersecurity). Unfortunately, at the present time, reliable empirical data on the actual level of cybersecurity investments is unavailable. Thus, one recommendation suggested in this article is for the US federal government to consider the development of a national database that tracks cybersecurity investments by private sector firms. A database on the level of investments in cybersecurity activities (and their effectiveness) by private sector firms could be maintained by a government agency and/or a research center within a university. The mere collection of such data could (and most likely would) serve to provide an incentive, via the marketplace, for firms to invest more into cybersecurity-related activities.

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

Funding

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 (NCS); and Sweden MSB (Myndigheten för samhällsskydd och beredskap) – Swedish Civil Contingencies Agency.

Appendix A

Proof of Proposition 1 First, we prove by contradiction that \( x^* = x_R \) (i.e. \( x \geq x_R \) is a binding constraint). Assume \( x \geq x_R \) is not binding. The firm’s problem then becomes \( \max_{x,y} [v - S(x,y)]L - x - y \), subject to \( x + y = B_1 \). The optimal solution to this problem is \((x_1, y_1)\), which contradicts the regulatory requirement \( x \geq x_R > x_1 \). Hence, \( x \geq x_R \) must be binding, i.e. \( x^* = x_R \).

We, therefore have \( S(x^*, y_R, v) = S(x_R, y_R, v) \). Given that \( x^* + y_R = x_R + y_R = B_1 = x_1 + y_1 \) and \( x_R > x_1 \), it follows that \( y_R < y_1 \). Thus, we have \( S(x_R, y_R, v) > S(x_R, y_1, v) \), so \( S(x^*, y_R, v) > S(x_R, y_1, v) \). Since \((x_1, y_1)\) is the optimal input mix under budget constraint \( B_1 \), it follows that \( S(x_R, y_1, v) \geq S(x_1, y_1, v) \). Combining the
last two inequalities, we have $S(x^*, y_R, v) > S(x_1, y_1, v)$. Hence, by the definitions of $S_R$ and $S_1$, we have $S_R > S_1$. Q.E.D.

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

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

Proof of Proposition 4 We first show that $\hat{y} \geq y_1$.

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

\[
\begin{align*}
\frac{dS_1}{dx} + \frac{dS_y}{dy} &= 0, \\
\frac{dS_y}{dx} + \frac{dS_y}{dy} &= 0.
\end{align*}
\] (A.1)

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

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

First-order conditions are as follows:

\[
\begin{align*}
\frac{dS_1}{dx} + \frac{dS_y}{dy} &= 0, \\
\frac{dS_y}{dx} + \frac{dS_y}{dy} &= 0.
\end{align*}
\] (A.3)

From equations (A.4) and (A.2), we have $S_1(x, y, v) = S_1(x_1, y_1, v)$. Given $x_R > x_1$, with $S_{\gamma_2} \leq 0$, it follows that $S_1(x_1, y_1, v) = S_1(x_1, y_1, v)$. Combined with $S_{\gamma_2} > 0$, we have $\hat{y} \geq y_1$. Since we also have $x = x_R > x_1$, $S_1 < 0$, and $S_2 < 0$, it follows that $S(x, \hat{y}, v) < S(x_1, y_1, v)$. In addition, $\hat{x} + \hat{y} > x_1 + y_1$. Q.E.D.

Proof of Proposition 5 Recall that the unregulated probability of a cybersecurity breach occurring was denoted as $S_1 = S(x_1, y_1, v)$, and now define $\gamma$ as the level of input $Y$ achieving the same probability of a cybersecurity breach occurring when $x = x_R$, i.e. $S(x_R, \gamma, v) = S(x_1, y_1, v)$. In other words, input mixes $(x_1, y_1)$ and $(x_R, \gamma)$ are on the same ISOSEC curve and $\gamma(x_R)$ can be described with the slope of

\[
\frac{d\gamma(x_R)}{dx_R} = -\frac{S_x}{S_{\gamma_2}}.
\] (A.5)

Hence, $\gamma(x_R)$ is decreasing in $x_R$ with the slope of marginal rate of technical substitution (MRTS) of the security breach function.

The firm’s optimal post-regulation investment in input $\hat{y}$ can also be viewed as a function of $x_1$, i.e. $\hat{y}(x_1)$ and can be described by taking the total differentiation of the first order condition $-S_1(x_R, \hat{y}, v) L = 1$ (equation (A.4)):

\[
\frac{d\hat{y}}{dx_R} = -\frac{S_{\gamma_2}}{S_{\gamma_1}},
\] (A.6)

when $x_R = x_1$, $\hat{y} = \gamma(x_R)$. This means that when the regulation requires the firm to spend at least $x_1$, the firm will choose the optimal mix $(x_1, y_1)$, and the regulation would not change the probability of a cybersecurity breach (i.e. the cybersecurity level remains the same). When the regulation requires the firm to increase spending on input $X$, imposing $x > x_R > x_1$, the firm needs to spend at least $\gamma_R$ to maintain the pre-regulation cybersecurity level. Therefore, by comparing $\hat{y}$ with $\gamma_R$, we can draw a conclusion on the regulation induced cybersecurity level. When $S_{\gamma_2} < 0$, $\hat{y}(x_R)$ is weakly increasing in $x_R$, the firm would not decrease spending on input $Y$, and the firm will always have a higher post regulation security level (i.e. Proposition 4). When $S_{\gamma_2} > 0$, $\hat{y}(x_R)$ is decreasing with the slope of $\frac{S_x}{S_{\gamma_2}}$. If $\hat{y}(x_R)$ is steeper than the ISOSEC curve $(-\frac{S_{\gamma_2}}{S_{\gamma_2}} = -\frac{S_x}{S_{\gamma_2}})$, the firm would not invest enough to maintain the same cybersecurity level and the regulation would result in lower cybersecurity level, on the other hand, if $\hat{y}(x_R)$ is flatter than the ISOSEC curve ($-\frac{S_x}{S_{\gamma_2}} < -\frac{S_{\gamma_2}}{S_{\gamma_2}}$), the firm would invest more than enough to maintain the same cybersecurity level and the regulation would result in higher cybersecurity level. Q.E.D.


I. For $S(x, y, v) = \frac{a_1}{(x+y+1)^2} + \frac{a_2}{(x+y+1)^2}$, we calculate the following derivatives:

\[
\begin{align*}
S_x &= -\frac{a_1}{(x+y+1)^2}(2x+1), \\
S_y &= -\frac{a_1}{(x+y+1)^2}(2y+1), \\
S_{\gamma_2} &= \frac{a_2}{(x+y+1)^2}(2x+1), \\
S_{\gamma_1} &= \frac{a_2}{(x+y+1)^2}(2y+1).
\end{align*}
\]

The above calculations show that for this class of breach function, $-\frac{S_x}{S_{\gamma_2}} < -\frac{S_y}{S_{\gamma_1}}$, which implies the regulation leads to an improved cybersecurity level.
II. For $S^{II}(x, y, v) = n(x + 1)(y + 1)\ln v$, we have:

$$S_x = 2(2x + 1)\left(2y + 1\right)\ln v, \quad S_y = 2(2x + 1)\left(2y + 1\right)\ln v, \quad S_{xy} = 2(2x + 1)\left(2y + 1\right)\ln v$$

$$S_{xy} = 2(2x + 1)\left(2y + 1\right)\ln v$$

(When $S_{xy} \leq 0$, $-\frac{S_x}{S_{xy}} < -\frac{S_y}{S_{xy}}$ holds. When $S_{xy} > 0$, it follows that $2x + 1 > 0$ and $y + 1 > 0$. Hence, $\frac{x}{y + 1} > 1$, and we have $-\frac{S_x}{S_{xy}} < -\frac{S_y}{S_{xy}}$ again.)

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

Appendix B

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

- Our business could be negatively affected by cyber or other security threats or other disruptions.
- As a U.S. defense contractor, we face cyber threats, insider threats, threats to the physical security of our facilities and employees, and terrorist acts, as well as the potential for business disruptions associated with information technology failures, natural disasters, or public health crises.

We routinely experience cyber security threats, threats to our information technology infrastructure and unauthorized attempts to gain access to our company sensitive information, as do our customers, suppliers, subcontractors and venture partners. We may experience similar security threats at customer sites that we operate and manage as a contractual requirement.

Prior cyber attacks directed at us have not had a material impact on our financial results, and we believe our threat detection and mitigation processes and procedures are adequate. The threats we face vary from attacks common to most industries to more advanced and persistent, highly organized adversaries who target us because we protect national security information. If we are unable to protect sensitive information, our customers or governmental authorities could question the adequacy of our threat mitigation and detection processes and procedures. Due to the evolving nature of these security threats, however, the impact of any future incident cannot be predicted.

Although we work cooperatively with our customers, suppliers, subcontractors, venture partners, and acquisitions to seek to minimize the impact of cyber threats, other security threats or business disruptions, we must rely on the safeguards put in place by these entities, which may affect the security of our information.

These entities have varying levels of cyber security expertise and safeguards and their relationships with government contractors, such as Lockheed Martin, may increase the likelihood that they are targeted by the same cyber threats we face.

The costs related to cyber or other security threats or disruptions may not be fully insured or indemnified by other means. Additionally, some cyber technologies we develop, particularly those related to homeland security, may raise potential liabilities related to intellectual property and civil liberties, including privacy concerns, which may not be fully insured or indemnified by other means. Occurrence of any of these events could adversely affect our internal operations, the services we provide to our customers, our future financial results, our reputation or our stock price; or such events could result in the loss of competitive advantages derived from our research and development efforts or other intellectual property, early obsolescence of our products and services, or contractual penalties (see: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/2013-Annual-Report.pdf, p. 16, accessed 26 October 2015).

References

52. Li C, Peters GF, Richardson VJ, Watson MW. The consequences of information technology control weaknesses on management information systems: the case of Sarbanes-Oxley internal control reports. MIS Quart (2012); 36: 179–204.