Mandatory Security Information Sharing with Authorities: Implications on Investments in Internal Controls

Stefan Laube
Department of Information Systems
University of Münster
Münster, Germany
Stefan.Laube@uni-muenster.de

Rainer Böhme
Institute of Computer Science
University of Innsbruck
Innsbruck, Austria
Rainer.Boehme@uibk.ac.at

ABSTRACT

New regulations mandating firms to share information on security breaches and security practices with authorities are high on the policy agenda around the globe. These initiatives are based on the hope that authorities can effectively advise and warn other firms, thereby strengthening overall defense and response to cyberthreats in an economy. If this mechanism works (as assumed in this paper with varying effectiveness), it has consequences on security investments of rational firms. We devise an economic model that distinguishes between investments in detective and preventive controls, and analyze its Nash equilibria. The model suggests that firms subject to mandatory security information sharing 1) over-invest in security breach detection as well as under-invest in breach prevention, and 2), depending on the enforcement practices, *may* shift investment priorities from detective to preventive controls. We also identify conditions where the regulation increases welfare.

Categories and Subject Descriptors

C.2.0 [**Computer Communication Networks**]: General—*security and protection*; K.4.1 [**Computers and Society**]: Public Policy Issues—*Regulation*; K.6.0 [**General**]: Economics

Keywords

Mandatory security information sharing; security investment; detective controls; preventive controls; economics of information security; externalities; game theory; policy

1. INTRODUCTION

According to some indicators, the frequency of security breaches to information systems of firms grows rapidly [20]. Ceteris paribus this leads to higher expected costs of security breaches to firms. These costs have two components. Direct costs of breaches in firms are caused by, e. g., restoring information systems to an uninfected state. Indirect costs of breaches comprise intangible costs, including opportunity costs due to lost business. Business may be lost in particular if security breach information is publicized. Such news may damage a firm's reputation and can foster apprehension of customers to transact with firms [11]. Consequently, security breaches in firms do not only affect firms, but also (potential) customers.

The expected costs of security breaches create natural incentives for firms to invest in security [7]. By contrast, customers can only trust firms to take appropriate measures and secure their data, i. e., they fully depend on the security investment decisions of firms. This situation describes the interdependence of security between firms and customers. Similar interdependencies exist on various other levels in economies, e. g., between firms, individuals, and other market participants [16, 3]. Interdependent security may justify policy intervention with the objective to stimulate security investments up to a socially optimal level [2].

One type of regulation are specific security breach notification laws. In many countries, new breach notification laws – discussed or about to be implemented – mandate firms to share security information primarily with authorities. (Some regulations additionally require firms to share information with affected customers.) This enables the authorities to advise and warn other firms or affected customers concerning their information security. For instance, this may lead to more effective security investments of firms, and increase their customers' level of alertness concerning propagating attacks. In this paper, we study the effects of breach notification laws on the security investment strategies of firms.

1.1 Internal Controls

We regard security investments of firms as investments in internal controls. These investments can mitigate the risk of security breaches (as opposed to other instruments of risk management, such as risk avoidance, risk transfer, and risk acceptance). Risk mitigation can be interpreted as a reduction of the expected direct and indirect costs of security breaches to firms [12]. Internal controls traditionally fall into two categories: preventive and detective controls [5]. By investing in preventive controls, e. g., the proactive procurement of firewalls or the introduction of penetration tests to detect and fix security flaws, firms try to shield their information systems from attacks. Complementary, by investing in detective controls, e. g., the procurement of intrusion detection systems or the introduction of internal security audits, firms try to learn about security threats and breaches. Detective controls deserve special attention in the light of

WISCS'15, October 12, 2015, Denver, Colorado, USA.

ACM 978-1-4503-3822-6/15/10 ...$15.00.
DOI: http://dx.doi.org/10.1145/2808128.2808132.

mandatory breach disclosure because firms can only report security breaches they know about.

Detective controls, like all decision support systems, produce a certain amount of errors of two types. Type I errors occur if the controls detect violations, such as security breaches, even though nothing happened (false alarms). Type II errors occur if the controls do not detect anything, even though violations have happened (missed detection). In particular, type II errors cause significant additional direct costs of security breaches to firms. Late detection of breaches may for instance enable the attackers to exhaust vulnerabilities in information systems over time and compromise large parts of the internal network.

A common perception in the literature is that security information sharing can leverage investments in the internal controls of firms [13], i. e., reduce the expected direct and indirect costs of breaches. However, we will show that legislation mandating security information sharing may also cause negative effects in the form of misallocation of resources.

1.2 Security Breach Notification Laws

We broadly distinguish between two different types of breach notification laws. The first type stipulates security breach reporting of firms to affected individuals. This kind of mandatory breach reporting is predominantly established in different US states [18]. Its objective is to incentivize investments in internal controls of firms, and to give affected individuals the opportunity to take countermeasures against the consequences of attacks [21]. The second type of breach notification laws mandates breach reporting of firms to authorities. This kind of breach reporting is predominantly established in EU sectors [8]. The objective of those laws is to empower authorities with security information. In turn, authorities can provide the received information (possibly in aggregated form) to other firms, thereby strengthening overall defense and response to cyberthreats in an economy. In this paper, we focus on laws similar to the "Network and Information Security" Directive (NIS-Directive) [10] currently discussed in the EU. This law aims to extend breach reporting obligations to authorities by additionally requiring firms in the EU to communicate security policies and other security best practices. The enforcement of this kind of mandatory security information sharing with authorities may result in positive as well as negative effects on affected firms.

Negative effects of mandatory security information sharing with authorities arise from associated compliance and indirect costs. Consider the scenario where a firm has to report security information, including a security breach, to an authority. This firm faces bureaucratic burdens arising from the documentation and reporting of relevant information. Once an authority is informed, it may pass on the breach information to other firms or customers with the objective to strengthen overall defense and response to the propagating attack. However, the receiving firms or customers might release the security breach information to the public. This causes additional indirect costs for the firm that was obliged to report security information in the first place.

The expected costs associated with mandatory information sharing may hinder compliance of firms. To minimize non-compliance, the currently discussed NIS-Directive [10] provides for security audits combined with the threat of sanctions. For example, a German initiative anticipating this Directive includes sanctions of up to 100 000 € for firms who fail to comply with breach reporting obligations [9]. We note that it remains an open research question if combinations of audits and sanctions can indeed incentivize compliance at a socially desirable level [17].

Positive effects of mandatory security information sharing with authorities arise in two forms, but only if the information flow from firms to authorities is effectively established.

1. The authority can advise firms by providing (aggregated) information on how to effectively invest in preventive and detective controls.

2. The authority can warn firms by providing information regarding ongoing threats. This may leverage investments in preventive and detective controls of firms.

The second mechanism already indicates that security information sharing influences security investment decisions of firms. We are not aware of any prior work that analyzes this effect for investments in detective and preventive controls. This motivates our research question.

1.3 Research Question

Our primary research question asks how the outcome of the sums of all firms' locally optimal decisions (i. e., profit maximization) compares to a socially optimal situation. In this situation, an imaginary benevolent dictator – called "social planner" in the economics literature – coordinates all decision variables in order to maximize a global objective function – called "social welfare". The solution of the social planner is a benchmark to measure the efficiency of both policy regimes (i. e., with and without mandatory security information sharing).

More specifically, we are interested in how the enforcement of security breach notification laws mandating security information sharing

a) changes the total spending of firms on detective and preventive controls compared to the social planner's optimal spending (RQ 1);

b) changes the investment priorities of firms, and whether or not these priorities differ from the social planner's optimal choices (RQ 2);

c) affects the profit of firms compared to a situation without the regulation and to the profit at the social optimum (as an upper bound or benchmark) (RQ 3).

Recall that we are *not* interested in minimizing the total security breach rate because the relevant objective function in a society is welfare (in our simple symmetric model: the sum of profits). Maximizing security investments (or minimizing breaches) may lead to misallocation in individual firms as well as in a broader economy. Budget spent on security controls beyond a certain level generates lower returns than productive activity.

Answers to the questions above are relevant for security managers of firms who allocate investments on *preventive* and *detective controls*. Moreover, the answers promise important insights on the incentive mechanisms of security breach notification laws, relevant for policy makers. Eventually, they help to decide if and how mandatory security information sharing with authorities should be introduced.

1.4 Roadmap

In this paper we devise and analyze a game-theoretic model to answer the research question. The model includes two free parameters for the following properties: a parameter for the sanctions that may accrue to non-complying firms (cf. Section 1.2), and a parameter for the effectiveness of security information sharing by authorities (cf. Section 1.2). Both factors are exogenous to our analysis. They depend on technical and organizational environment and are so far unknown. To account for this uncertainty, we compare different hypothetical scenarios in this parameter space.

In Section 2 we present our model and solve it for all pure strategy equilibria. We discuss our modeling decisions in the light of related work in Section 3. Section 4 presents the scenarios and the results obtained from our model. Section 5 concludes with a discussion.

2. MODEL

The game-theoretic model consists of two components: a model for investment decisions of firms, proposed in Section 2.1, and a formalization of mandatory security information sharing with authorities, presented in Section 2.2. The second component includes all free parameters mentioned above (in Section 1.3). We determine the expected costs of firms under different policy regimes in Section 2.3. A study of the model's social optima and Nash equilibria is conducted in Section 2.4 and Section 2.5, respectively. All symbols used are summarized in Table 3 of Appendix E.

2.1 Investments of Firms

Consider for now a single rational and risk neutral firm in a larger economy. The firm has a total budget of $B = 1$. It may invest this budget in the provision of products and services $p \geq 0$ or in information security, i. e., preventive controls $x > 0$ or detective controls $d > 0$. Every dollar invested for productive activity can no longer be invested in information security. Therefore, investment in production is

$$p(x, d) = B - x - d. \tag{1}$$

Investment in production generates constant return $r \geq 1$. Expected costs of security breaches $c(x, d)$ that may happen to the firm's information system reduce the return. Thus, the overall profit of the firm is

$$o(x, d) = r \cdot p(x, d) - c(x, d). \tag{2}$$

The expected costs of security breaches $c(x, d)$ depend on the firm's investments in preventive and detective controls. Investments in preventive controls reduce the probability of security breaches to the firm's information system $P(x)$. Investments in detective controls increase the probability of finding security breaches that have happened $D(d)$. We assume that a security breach that has happened and gets detected by the firm results in direct costs q_1. By contrast, a security breach that has happened and remains undetected leads to considerably higher direct costs, as an attacker may compromise large parts of the internal network. We depict this by costs arising from undetected security breaches $q_3 \gg q_1$. Thus, the overall expected costs of security breaches in the firm are

$$c(x, d) = P(x) \cdot [D(d) \cdot q_1 + (1 - D(d)) \cdot q_3]. \tag{3}$$

We capture the probability of security breaches $P(x)$ by the realization $\alpha \in \{0, 1\}$ of the random variable A (security breach), such that $Pr(\alpha = 1) = P(x)$. Investments in preventive controls decrease this probability at a decreasing rate, i. e., $P(x)' < 0$, $P(x)'' > 0$, and $\lim_{x\to\infty} P(x) \to 0$. A functional form for the probability of security breaches is $P(x) = \beta^{-x}$. The exogenous variable $\beta > 0$ represents the productivity of investments in preventive controls. Observe that without investments in preventive controls, the firm inevitably falls victim to realized threats, i. e., $P(0) = 1$.

Moreover, we capture the probability of breach detection $D(d)$ by the realization $\hat{\alpha} \in \{0, 1\}$ of the random variable $\hat{A}$ (breach detection), such that $Pr(\hat{\alpha} = 1 | \alpha = 1) = D(d)$. Investments in detective controls increase this probability at a decreasing rate, i. e., $D(d)' > 0$, $D(d)'' < 0$, and $\lim_{d\to\infty} D(d) \to 1$. A functional form for the probability of security breach detection is $D(d) = 1 - \lambda^{-d}$. The exogenous variable $\lambda > 0$ represents the productivity of investments in detective controls. Note that we disregard type I errors of detective controls, such that $D(d)$ describes the probability of type II errors only. Observe that without investment in detective controls, the firm does not detect any security breach, not even by accident, i. e., $D(0) = 0$.

The enforcement of mandatory security information sharing with authorities may have an effect on the probability of security breaches and their detection in firms.

2.2 Mandatory Security Information Sharing

We generalize our model to $n = 2$ symmetric firms representing an economy. The firms are indexed by $i \in \{0, 1\}$. Regulators can mandate both firms to report security information to an authority, i. e., information on security breaches and best practices regarding breach prevention and detection. We capture security information sharing decisions of firm i by $t_i \in \{0, 1\}$, where $t_i = 0$ denotes that the firm does not share information at all. By contrast, if $t_i = 1$ the firm fully shares security information, i. e., it complies. Security information sharing with authorities results in both, negative and positive effects on firms.

Security information sharing with authorities causes expected indirect costs $q_2 > 0$. These indirect costs include compliance costs and losses of reputation or market share, e. g., because the security breach information leaks to the public. Consequently, firms may not have incentives to share security information. In fact, we assume that – without regulators taking additional measures – the expected indirect costs of information sharing hinder the compliance of firms. Regulators can enforce compliance by the introduction of security audits and the threat of sanctions. Specifically, we assume that regulators conduct audits at firms with a probability of $a \in [0, 1]$ to verify the compliance with breach reporting obligations. The parameter $S \geq 0$ denotes *sanctions for non-compliance*.

Security information sharing with authorities can leverage investments in preventive and detective controls of firms. A firm's reporting of best practices in security breach prevention and detection to an authority may put this authority in a position to advise other firms concerning investments in internal controls. We model the positive effect resulting from an informed authority's effective advice as an improvement of a firm's preventive or detective controls, but without additional cost for the firm. Therefore, firm i's probability

of security breaches and breach detection are, respectively,

$$P_i = P_i(x_i, x_{1-i}) = \beta^{-(x_i + b \cdot t_{1-i} \cdot x_{1-i})} , \quad (4)$$

$$D_i = D_i(d_i, d_{1-i}) = 1 - \lambda^{-(d_i + b \cdot t_{1-i} \cdot d_{1-i})} , \quad (5)$$

where $b \in [0, 1]$ is the parameter for the *sharing effectiveness* of an informed authority. Breach reporting enables the authority to draw new conclusions from these breaches. An informed authority can, e. g., provide firms with information on methods to minimize the impact of known vulnerabilities, which generates the positive effect of information sharing on preventive controls. Moreover, an authority can warn firms concerning propagating attacks, which generates the positive effect of information sharing on detective controls.

2.3 Expected Costs of Firms

Figure 1 visualizes the calculation of firm i's expected costs in a regime with mandatory security information sharing with authorities. The figure depicts all decisions of the firm and the regulator. Initially, firm i chooses whether or not to comply with security information sharing obligations. The firm simultaneous invests in preventive controls x_i, detective controls d_i, and production $p(x_i, d_i)$. Then the firm is exposed to attacks. An attack is successful with probability $P_i(x_i, x_{1-i})$. Note that in every period under consideration, there can at most be one security breach at firm i. Every security breach causes direct costs. The amount of direct costs depends on whether the firm detects the breach (q_1) or not (q_3). Once a security breach has happened, its detection probability is $D_i(d_i, d_{1-i})$. Regardless of breach detection, firm i has to report to the authority whether or not there has been a security breach to its information system. Every *reported* breach causes indirect costs q_2, which include compliance costs. If the firm does not report a security breach, the regulator conducts a security audit with probability a. The detection of a breach during a security audit results in sanctions S for non-compliance. We assume that auditors find every unreported breach and do not create false positives. Hence, audits are much more reliable than detective controls. We ignore audit costs and assume that the regulator can pay all auditors from the sum of collected sanctions.

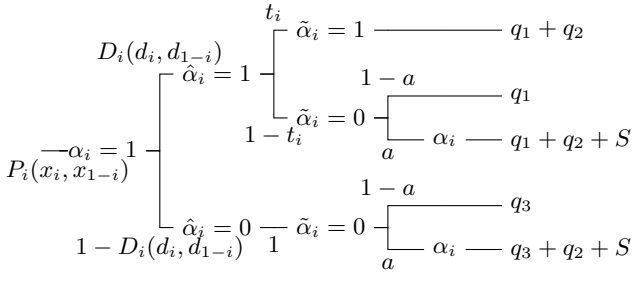


Figure 1: Decision tree used to calculate a firm's expected costs of security breaches

In order to enforce security information sharing, the regulator can adjust the audit probability a and the sanction level S based on his own cost structure. For simplicity we assume that mandatory security information sharing is always enforced with audit probability $a = 1$ and a collectable sanction level $S > 0$. Such disclosure regimes incentivize firms to fully share security information ($t = 1$). By setting the audit probability to $a = 0$, we obtain a scenario without mandatory information sharing and firms do not share security information at all ($t = 0$). We can derive firm i's expected costs due to security breaches without $c_i^{t=0}$ and with $c_i^{t=1}$ the enforcement of mandatory security information sharing from Figure 1:

$$c_i^0(x_i, x_j, d_i, d_j, 0) = P_i \cdot [D_i \cdot q_1 + (1 - D_i) \cdot q_3] , \quad (6)$$

$$c_i^1(x_i, x_j, d_i, d_j, a) = P_i \cdot [D_i \cdot (q_1 + q_2) + (1 - D_i) \cdot [(1 - a) \cdot q_3 + a \cdot (q_3 + q_2 + S)]]. \quad (7)$$

Consequently, without enforcement of information sharing, the expected profits in Eq. (2) have to be expanded to Eq. (8). With enforcement of information sharing, Eq. (2) expands to Eq. (9):

$$o_i^0(x_i, x_j, d_i, d_j, 0) = r \cdot p(x_i, d_i) - c_i^0(x_i, x_j, d_i, d_j, 0) , \quad (8)$$

$$o_i^1(x_i, x_j, d_i, d_j, a) = r \cdot p(x_i, d_i) - c_i^1(x_i, x_j, d_i, d_j, a). \quad (9)$$

2.4 Social Optima

The social optimum maximizes the sum of profits of both firms. A social planner with control over information sharing of firms does not need to incentivize sharing with audits and sanctions, i. e., $a = S = 0$. However, he does not share security information if

$$o_i^0(x_i, x_j, d_i, d_j, 0) > o_i^1(x_i, x_j, d_i, d_j, 0). \quad (10)$$

If the planner does not introduce security information sharing, he maximizes firms' profits based on Eq. (8), i. e.,

$$(x^*, d^*) = \arg\max_{x,d} 2 \cdot o_i^0(x, x, d, d, 0), \quad (11)$$

where we may substitute $x_i = x_{1-i} = x$, and $d_i = d_{1-i} = d$ for symmetry. The solution to the problem in Eq. (11) is given in Appendix A. Investments in detective controls are

$$d^*_{t=0} = \frac{\log\left(\frac{(q_1 - q_3)(\log(\beta) - \log(\lambda))}{q_1 \log(\beta)}\right)}{\log(\lambda)}. \quad (12)$$

Investments in preventive controls are

$$x^*_{t=0} = \frac{\log\left(-\frac{q_1 \log(\beta) \log(\lambda)}{r \log(\beta) - r \log(\lambda)}\right)}{\log(\beta)}. \quad (13)$$

If the planner introduces information sharing, he maximizes firms' profits based on Eq. (9) w. r. t. $a = S = 0$, i. e.,

$$(x^*, d^*) = \arg\max_{x,d} 2 \cdot o_i^1(x, x, d, d, 0). \quad (14)$$

The solution to the problem in Eq. (14) is given in Appendix B. Investments in detective controls are

$$d^*_{t=1} = \frac{\log\left(\frac{(\log(\beta) - \log(\lambda))(q_1 + q_2 - q_3)}{\log(\beta)(q_1 + q_2)}\right)}{(b+1)\log(\lambda)}. \quad (15)$$

Investments in preventive controls are

$$x^*_{t=1} = \frac{\log\left(-\frac{(b+1)\log(\beta)\log(\lambda)(q_1 + q_2)}{r(\log(\beta) - \log(\lambda))}\right)}{(1+b)\log(\beta)}. \quad (16)$$

2.5 Nash Equilibria

In practice, each firm's individual profit expectation determines its willingness to invest in internal controls. As one firm's actions affect other firms' outcomes, firms may act strategically. This requires a game-theoretic approach. We use pure strategy Nash equilibria as solution concept and analyze the existence and location of equilibria depending to whether the regulator does ($a = 1$) or does not ($a = 0$) enforce mandatory security information sharing.

A smart regulator enforces information sharing with sanctions $S > 0$ and audits $a = 1$ if this maximizes the profits of both firms. He does not introduce audits if

$$o_i^0(x_i, x_j, d_i, d_j, 0) > o_i^1(x_i, x_j, d_i, d_j, 1). \tag{17}$$

If the regulator does not introduce audits, firm i maximizes Eq. (8), i. e.,

$$(x_i^+, d_i^+) = \arg\max_{x_i, d_i} o_i^0(x_i, x_j, d_i, d_j, 0). \tag{18}$$

The solution to this equations is the best response of firm i in a regime without audits and depends on the decisions of firm $1 - i$. Nash equilibria follow from fixed points of the mutual best response of both firms. We derive these equilibria in Appendix C. In equilibrium, investments in detective controls are

$$\tilde{d}_{t=0} = \frac{\log\left(\frac{(q_1 - q_3)(\log(\beta) - \log(\lambda))}{q_1 \log(\beta)}\right)}{\log(\lambda)}, \tag{19}$$

and investments in preventive controls are

$$\tilde{x}_{t=0} = \frac{\log\left(-\frac{q_1 \log(\beta)\log(\lambda)}{r\log(\beta) - r\log(\lambda)}\right)}{\log(\beta)}. \tag{20}$$

If the regulator does introduce audits, firm i maximizes Eq. (9), i. e.,

$$(x_i^+, d_i^+) = \arg\max_{x_i, d_i} o_i^1(x_i, x_j, d_i, d_j, 1). \tag{21}$$

The solution to this equation is the best response of firm i in a regime with audits and depends on the decisions of firm $1 - i$. We derive the Nash equilibria in Appendix D. In equilibrium, investments in detective controls are

$$\tilde{d}_{t=1} = \frac{\log\left(\frac{(\log(\beta) - \log(\lambda))(q_1 - q_3 - S)}{\log(\beta)(q_1 + q_2)}\right)}{(b+1)\log(\lambda)}, \tag{22}$$

and investments in preventive controls are

$$\tilde{x}_{t=1} = \frac{\log\left(-\frac{\log(\beta)\log(\lambda)(q_1 + q_2)}{r(\log(\beta) - \log(\lambda))}\right)}{(b+1)\log(\beta)}. \tag{23}$$

If the inequality of Eq. (17) holds, only the equilibrium $(\tilde{d}_{t=0}, \tilde{x}_{t=0})$ exists. Otherwise, the equilibrium is $(\tilde{d}_{t=1}, \tilde{x}_{t=1})$.

3. RELATED WORK

This paper directly extends our prior work [17], where we analyze the economics of mandatory security breach reporting to authorities. The model in [17] assumes endogenous investment in preventive controls of firms and an exogenous probability of security breach detection. In this work, we endogenize the detection probability by explicitly allowing investments in detective controls. Furthermore, the focus of [17] is to evaluate conditions for security audits and sanctions to incentivize mandatory security breach reporting. Here we assume that the introduction of audits and sanctions always incentivizes compliance and focus on the effects of information sharing on investments in internal controls.

Another predecessor is the analytical model by Cavusoglu et al. [5]. It differentiates between investments of firms in preventive and detective controls. Their work sets out to facilitate firms to evaluate the effectiveness of real-world investment decisions in internal controls. However, the model does not consider breach reporting or information sharing.

The works in [17, 5] clearly inspired this paper's research question and modeling approach. The model in this paper consists of two components: a model for investment decisions of firms and a formalization of mandatory information sharing. In order to devise our model, we adopt widely accepted modeling assumptions for each of these components.

The first component includes assumptions on investments in preventive and detective controls. We adapt our assumptions on investments in preventive controls from Gordon and Loeb [12], which is common in the literature. Furthermore, we use a functional form to capture these assumptions which was introduced by Böhme [4]. Our assumptions and the functional form to capture investments in detective controls are adapted from Khouzani et al. [15].

The second component comprises negative and positive effects of security information sharing. The assumption that breach information sharing leads to expected indirect costs for firms, as information may leak, is commonly accepted in various economic analyses, e. g., by Gal-Or and Ghose [11] and Hausken [14]. We follow Öğüt et al. [19] and Gordon et al. [13] by using the intuition that sharing of security best practices leverages the effectiveness of investments in preventive controls. Moreover, we assume that a similar leverage effect arises from sharing best practices on breach detection. However, this assumption still lacks empirical support.

4. ANALYSIS

In this section, we apply our model to analyze implications of mandatory security information sharing with authorities on security investments. We set and justify constants in Section 4.1. The analysis of socially optimal investments is conducted in Section 4.2. Nash equilibria are analyzed in Section 4.3. We answer our research question in Section 4.4.

4.1 Constants

For the numerical analysis, we specify all exogenous model variables as constants relative to the investment budget $B = 1$ of each firm. A typical order of magnitude for our unit B would be US$ 1 billion in the real world.

4.1.1 Return on Investment

Firms can spend their budget on productive activity or internal controls. We fix the return on investment of productive activity at $r = 1.1$. This value constitutes the 10 year average of the "Dow Jones Industrial Average" – which is 8.36 % – rounded to 10 %.

4.1.2 Costs of Detected Security Breaches

We take into account the "Target breach" that has happened at the end of the year 2013 to estimate the costs of detected breaches. The Target Corporation is a firm that had a total equity of US$ 14 billion in the financial year 2014.

This total equity can be used as an estimate for the budget of Target. The security breach at Target resulted in costs of about US$ 1 billion [1]. By attributing all of these costs to the year 2014, we find that detected breaches in firms with a total budget of more than US$ 1 billion can result in costs of $q_1 + q_2 = 1/14 = .07$, relative to our model. However, as the breach at Target belongs to the worst security breaches of all time, it is reasonable to assume that the majority of security breaches in economies are not that devastating. Thus, we fix the costs of detected breaches at $q_1 + q_2 = .02$, assuming indirect costs of $q_1 = .009$ and direct costs of $q_2 = .011$. This cost ratio goes in line with previous research which concludes that, if breaches become public, their direct costs to firms are lower than the indirect costs [6].

4.1.3 Costs of Undetected Security Breaches

We assume that security breaches in firms which remain undetected for a long time are more severe than detected breaches. However, we do not find empirical studies supporting any particular cost level of such breaches. In our model, firms face an existential threat in case that they do not invest in detective controls at all, i. e., we fix the costs of undetected security breaches at $q_3 = .5$.

4.1.4 Productivity of Investments

It is notoriously hard to calibrate productivity parameters in analytical models. Acknowledging the uncertainty, we follow [4] and fix the productivity of investments in preventive controls at $\beta = 200$. This level was called "high" in an analysis with a comparable model. Furthermore, we fix the productivity of investments in detective controls at $\lambda = 250$. This productivity level is considerably higher than the productivity of investments in software vulnerability detection, as specified by the authors of [15]. Consequently, we assume that finding breaches that have happened to information systems costs (considerably) less than finding software flaws.

4.2 Decisions of the Social Planner

The two solid lines in Fig. 2 (a) show the investment decisions of the social planner as a function of the sharing effectiveness of an informed authority. The lowermost solid line describes optimal investments in detective controls d_t^*. The uppermost solid line sketches the sum of optimal investments in internal controls $x_t^* + d_t^*$. The reference point ϕ_0 in Fig. 2 (a) restricts the interval of low sharing effectiveness from above, i. e., for a sharing effectiveness of $0 \leq b < \phi_0$, Eq. (10) is fulfilled. If the sharing effectiveness is below the reference point ϕ_0, the social planner does not introduce security information sharing, and the social optimum is $(x_{t=0}^*, d_{t=0}^*)$. At the reference point ϕ_0, the planner is indifferent on introducing security information sharing. In the interval $\phi_0 \leq b \leq 1$, the sharing effectiveness justifies the introduction of information sharing, and the planner chooses the social optimum $(x_{t=1}^*, d_{t=1}^*)$.

4.2.1 No Security Information Sharing

Consider for now the interval $0 \leq b < \phi_0$ in Fig. 2 (a), where the planner does not introduce information sharing. In this interval, the social optimum $(x_{t=0}^*, d_{t=0}^*)$ does not depend on the sharing effectiveness of an informed authority b (cf. Eq. (12) and Eq. (13)). Consequently, the social planner's investments in detective and preventive controls are constant. Specifically, investments in breach prevention are $x_{t=0}^* = .013$, and investments in breach detection $d_{t=0}^* = .151$. Thus, in the interval $0 \leq b < \phi_0$, the social planner invests more in detective than in preventive controls, i. e., $x_{t=0}^* < d_{t=0}^*$. Moreover, the total security investment is constant at $x_{t=0}^* + d_{t=0}^* = .164$.

4.2.2 Security Information Sharing

The situation of constant investments changes for a sharing effectiveness of $\phi_0 \leq b \leq 1$, where the social planner introduces information sharing. In this interval, the social optimum $(x_{t=1}^*, d_{t=1}^*)$ depends on the sharing effectiveness of the authority (cf. Eq. (15) and Eq. (16)). At the reference point ϕ_0, investments in breach prevention are $x_{t=1}^* = .165$, and investments in detection are $d_{t=1}^* = .002$. Both the investments in preventive and detective controls constantly decrease with increasing sharing effectiveness b. Thus the maximum total security investment is $x_{t=1}^* + d_{t=1}^* = .167$. Fig. 2 (a) reveals that in the interval $\phi_0 \leq b \leq 1$, the social planner invests more in preventive than in detective controls, i. e., $x_{t=1}^* > d_{t=1}^*$.

4.2.3 Welfare

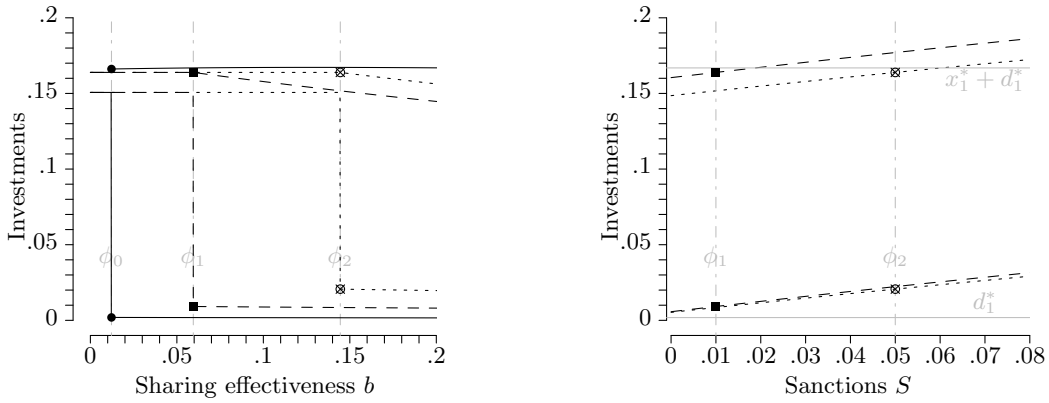
The solid line in Fig. 3 (a) depicts the profit that the social planner generates by investments at the social optimum as a function of the sharing effectiveness b of an informed authority. In the interval $0 \leq b < \phi_0$, this profit is constant at $o(x_t^*, d_t^*) = .712$, as no information sharing is introduced. However, if the sharing effectiveness renders information sharing beneficial, i. e., in the interval $\phi_0 \leq b \leq 1$, the profit increases with the sharing effectiveness (but at a decreasing rate, not visible in the figure).

4.3 Decisions of Firms

The two dashed and dotted lines in Fig. 2 (a) show the investment decisions of firms as a function of the sharing effectiveness of an informed authority. This effectiveness influences the decision of the regulator to enforce information sharing with sanctions.[1] The dashed lines represent decisions of firms if the regulator imposes sanctions of $S = .01$ to enforce sharing. We analyze this scenario subsequently. The dotted lines in Fig. 2 (a) show decisions of firms if the regulator has to impose sanctions of $S = .05$ to enforce sharing. We extend our analysis to the scenario with higher sanctions where necessary.

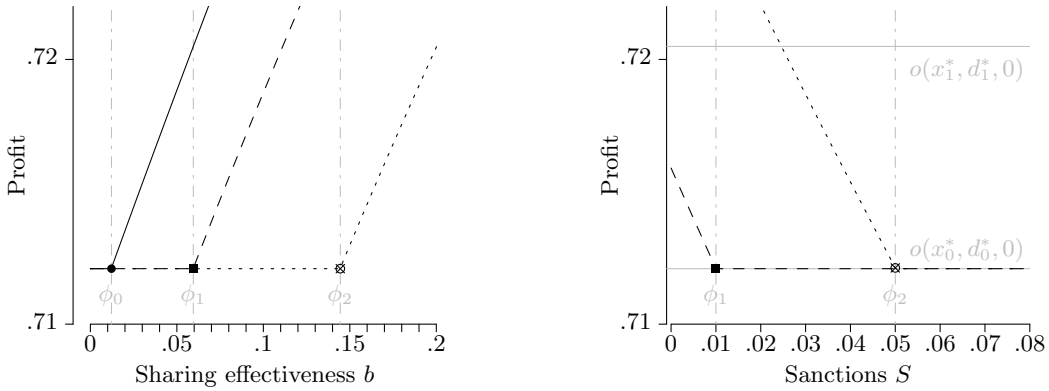
The lowermost dashed line describes the optimal investments in detective controls $\tilde{d}_t$ of firms. The uppermost dashed line shows the sum of optimal security investments $\tilde{x}_t + \tilde{d}_t$. For a sharing effectivenesses b below the reference point ϕ_1 in Fig. 2 (a), the regulator cannot effectively enforce mandatory information sharing with sanction of $S = .01$. Thus, for $0 \leq b < \phi_1$, the inequality in Eq. (17) holds and the Nash equilibrium between firms is $(\tilde{x}_{t=0}, \tilde{d}_{t=0})$. The regulator is indifferent on the enforcement of information sharing at the reference point ϕ_1. In the interval $\phi_1 \leq b \leq 1$, the sharing effectiveness is high enough to justify the enforcement of information sharing. The resulting equilibrium between firms is $(\tilde{x}_{t=1}, \tilde{d}_{t=1})$.

[1] Recall that the enforcement of information sharing is always accompanied by an audit probability of $a = 1$.



(a) $S = .01$ (dashed); $S = .05$ (dotted) (b) $b = .06$ (dashed); $b = .14$ (dotted)

Figure 2: Socially optimal investments (solid lines) and investments at the Nash equilibrium (dashed and dotted lines); lowermost lines: investments in detective controls d; uppermost lines: sum of investments $x + d$; vertical gray dashed/dotted lines: indifference points between sharing regimes



(a) $S = .01$ (dashed); $S = .05$ (dotted) (b) $b = .06$ (dashed); $b = .14$ (dotted)

Figure 3: Profit at the social optimum (solid lines) and the Nash equilibria (dashed and dotted lines); vertical gray dashed/dotted lines: indifference points between sharing regimes

4.3.1 No Security Information Sharing

Consider for now the interval $0 \leq b < \phi_1$ in Fig. 2 (a), where the regulator does not enforce information sharing. In this interval, decisions of firms are the same as the decisions of the social planner who does not introduce information sharing, i. e., $(x^*_{t=0}, d^*_{t=0}) = (\tilde{x}_{t=0}, \tilde{d}_{t=0})$ (cf. the social optimum and Nash equilibrium in Section 2.4 and Section 2.5). Thus, we refer to Section 4.2 for the explanation of the firms' optimal decisions.

4.3.2 Security Information Sharing

In the interval $\phi_1 \leq b \leq 1$ in Fig. 2 (a), the regulator enforces information sharing with sanctions of $S = .01$. Consequently, firms invest at the Nash equilibrium $(\tilde{x}_{t=1}, \tilde{d}_{t=1})$, which depends on the sharing effectiveness of the informed authority (cf. Eq. (22) and Eq. (23)). At the reference point ϕ_1, investments in security breach prevention and detection are $x^*_{t=1} = .155$ and $\tilde{d}_{t=1} = .009$, respectively. Both investments in preventive and detective controls constantly decrease with increasing sharing effectiveness b. Thus, the maximum investment in security is $\tilde{x}_{t=1} + \tilde{d}_{t=1} = .164$. In the interval $\phi_1 \leq b \leq 1$, firms invest more in preventive than in detective controls $\tilde{x}_{t=1} > \tilde{d}_{t=1}$.

We may now consider that the regulator must impose higher sanctions, $S = .05$, to enforce mandatory security information sharing. The security investment decisions of firms who are affected by these sanctions are represented by the dotted lines in Fig. 2 (a). If high sanctions are needed, the regulator cannot effectively enforce mandatory information sharing for a sharing effectiveness b below the reference point $\phi_2 > \phi_1$. Thus, in the interval $0 \leq b < \phi_2$, the inequality of Eq. (17) holds and the Nash equilibrium between firms is $(\tilde{x}_{t=0}, \tilde{d}_{t=0})$. The regulator is indifferent on the enforcement of security information sharing at the reference point ϕ_2. A high sharing effectiveness, i. e., $\phi_2 \leq b \leq 1$, enables the regulator to enforce information sharing. If information

sharing is enforced, the Nash equilibrium between firms is $(\tilde{x}_{t=1}, \tilde{d}_{t=1})$. Observe from Fig. 2 (a) that firms respond to the threat of higher sanctions with increased investments in detective controls.

The effect of sanctions on the investment decisions of firms is also visible in Fig. 2 (b). In this figure, the lowermost dashed line describes investments in detective controls as a function of the sanction level S for a sharing effectiveness of $b = .06$. The uppermost dashed line marks the resulting sum of security investments. Observe from the constance distance between both dashed lines that investments in preventive controls do not depend on the regulator's introduction of sanctions (this is also captured in Eq. (23)). Furthermore, we find that investments in detective controls increase with the sanction level (cf. Eq. (22)). Investments in detective controls by firms are always higher than the corresponding investments of the social planner (cf. the lowermost dashed line and the lowermost gray line in Fig. 2 (b), where the gray line indicates a sharing effectiveness of $b = .06$). Observe from Fig. 2 (b) that the uppermost dashed line may exceed the uppermost gray line, which shows the social planner's security investments for a sharing effectiveness of $b = .06$. Thus, high sanctions cause firms to over-invest in security. As only investments in detective controls increase with the sanction level, high sanctions may incentivize firms to invest more in detective than in preventive controls $\tilde{x}_{t=1} < \tilde{d}_{t=1}$. In general, investment decisions of firms change if security information sharing is enforced and the informed authority is effective, i. e., $b = .14$ (cf. the dotted lines in Fig. 2 (b)). Higher sharing effectiveness results in lower security investments (cf. the uppermost dashed line and the uppermost dotted line in Fig. 2 (b)). This reproduces a substitution effect of (effective) security information sharing on security investments previously observed, e. g., by Gordon et al. [13].

4.3.3 Welfare

The dashed line in Fig. 3 (a) shows the profit firms can expect at the Nash equilibrium as a function of the sharing effectiveness of an informed authority, assuming that information sharing is enforced with sanctions of $S = .01$. In the interval $0 \leq b < \phi_1$, the regulator does not enforce information sharing and the profit is constant at $o(x_t^*, d_t^*) = .712$. If sharing is enforced, i. e., in the interval $\phi_1 \leq b \leq 1$, the profit of firms increases in the sharing effectiveness b (again, at a decreasing rate). If higher sanctions are necessary to enforce mandatory security information sharing, e. g., a sanction level of $S = .05$, then the sharing effectiveness of the authority must be above a certain threshold to increase firms' profits (cf. the dotted line and the reference point $\phi_2 > \phi_1$ in Fig. 3 (a)).

The dashed line in Fig. 3 (b) shows the profit firms can expect at the Nash equilibrium as a function of the sanction level required to enforce information sharing for a sharing effectiveness of $b = .06$. Observe from this figure that the introduction of a sanction level below the reference point ϕ_1, i. e., $0 < S < \phi_1$, has a positive effect on firms' profits if they have incentives to share information. However, in this interval, no sanction level that effectively enforces information sharing results in profits greater than or equal to those of the social planner (cf. the dashed line and the uppermost solid gray line, capturing a sharing effectiveness of $b = .06$). We observe from Fig. 3 (b) that a sanction level above the reference point ϕ_1 has a negative effect on profits. Specifically, profits are maximized if the regulator sets the sanction level to the minimum required in order to (just) incentivize information sharing (cf. the dashed and the lowermost solid gray line in Fig. 3 (b), capturing a sharing effectiveness of $b = .06$). Every additional raise in the sanction level reduces profits and therefore welfare. The effect of higher sharing effectiveness, i. e., $b = .14$, is visualized by the dotted line in Fig. 3 (b). Observe that higher sharing effectiveness raises firms' profits if mandatory information sharing is effectively enforced (cf. the dotted and dashed line in Fig. 3 (b)).

Table 1: Summary of parameter effects.

Regime		Exogenous parameters	
Endogenous parameters		$b \uparrow$	$S \uparrow$
Baseline (without regulation)			
preventive controls	x_0^*	$\rightarrow$	$\rightarrow$
detective controls	d_0^*	$\rightarrow$	$\rightarrow$
Social optimum with regulation			
preventive controls	x_1^*	$\downarrow$	$\rightarrow$
detective controls	d_1^*	$\downarrow$	$\rightarrow$
Nash equilibrium with regulation			
preventive controls	$\tilde{x}_1$	$\downarrow$	$\rightarrow$
detective controls	$\tilde{d}_1$	$\downarrow$	$\uparrow$

4.4 Results

We may now answers the questions posed in Section 1.3. The effects of our model parameters on the social optimum and the Nash equilibria are summarized in Table 1. An important observation from this table is that most results depend on the sharing effectiveness. As the effectiveness of information sharing is unknown in practice, we discuss all relevant scenarios and give the intervals for the sharing effectiveness scale where specific results apply. We extend our explanation of results on the effect of sanctions where appropriate. Table 2 summarizes all results discussed in the following subsections.

4.4.1 Total Security Spending

In the interval $0 \leq b < \phi_0$, the sum of investments of firms and the social planner are equal as the social optimum corresponds to the Nash equilibrium. In the case of a high sharing effectiveness, $\phi_0 \leq b < \phi_{1,2}$, total investments of firms are lower than total investments of the social planner, who introduces information sharing. If the sharing effectiveness is in the interval $\phi_{1,2} \leq b \leq 1$, firms may over- *or* under-invest in security. We refer to the two possible scenarios as scenario 1 (S1) and scenario 2 (S2). In scenario 1, the regulator enforces information sharing with low sanctions. Consequently, firms' total investments are below the total investments of the social planner. In scenario 2, the regulator enforces information sharing with high sanctions. This may lead to security over-investments of firms.

4.4.2 Investment Priorities

In the interval $0 \leq b < \phi_0$, both the social planner and firms prioritize investments in detective controls. There is no difference in the allocation of security investments between social planner and firms. In case of a high sharing effectiveness of $\phi_0 \leq b < \phi_{1,2}$, firms have different invest-

Table 2: Answer to the research question.

Condition	**Notation**	**RQ 1**	**RQ 2**		**RQ 3**
Interval of sharing effectiveness	Social optimum, Nash equilibrium	Total security spending	Investments priorities	Preventive and detective security spending	Social welfare (sum of profits)
$0 \leq b < \phi_0$	(x_0^*, d_0^*),$(\tilde{x}_0, \tilde{d}_0)$	$x_0^* + d_0^* = \tilde{x}_0 + \tilde{d}_0$	$x_0^* < d_0^*$,$\tilde{x}_0 < \tilde{d}_0$	$x_0^* = \tilde{x}_0$,$d_0^* = \tilde{d}_0$	$o(x_0^*, d_0^*) = o(\tilde{x}_0, \tilde{d}_0)$
$\phi_0 \leq b < \phi_{1,2}$	(x_1^*, d_1^*),$(\tilde{x}_0, \tilde{d}_0)$	$x_1^* + d_1^* > \tilde{x}_0 + \tilde{d}_0$	$x_1^* > d_1^*$,$\tilde{x}_0 < \tilde{d}_0$	$x_1^* > \tilde{x}_0$,$d_1^* < \tilde{d}_0$	$o(x_1^*, d_1^*) > o(\tilde{x}_0, \tilde{d}_0)$
$\phi_{1,2} \leq b \leq 1$ (S1)	(x_1^*, d_1^*),$(\tilde{x}_1, \tilde{d}_1)$	$x_1^* + d_1^* > \tilde{x}_1 + \tilde{d}_1$	$x_1^* > d_1^*$,$\tilde{x}_1 > \tilde{d}_1$	$x_1^* > \tilde{x}_1$,$d_1^* < \tilde{d}_1$	$o(x_1^*, d_1^*) > o(\tilde{x}_1, \tilde{d}_1)$
$\phi_{1,2} \leq b \leq 1$ (S2)	(x_1^*, d_1^*),$(\tilde{x}_1, \tilde{d}_1)$	$x_1^* + d_1^* \leq \tilde{x}_1 + \tilde{d}_1$	$x_1^* > d_1^*$,$\tilde{x}_1 < \tilde{d}_1$	$x_1^* > \tilde{x}_1$,$d_1^* < \tilde{d}_1$	$o(x_1^*, d_1^*) > o(\tilde{x}_1, \tilde{d}_1)$

ment priorities than the social planner. Specifically, firms prefer to invest in detective controls while the social planner prioritizes investments in breach prevention. If the sharing effectiveness is in the interval $\phi_{1,2} \leq b \leq 1$, it depends on the scenario whether or not firms and the social planner set different investment priorities. In scenario 1, where the regulator enforces information sharing with low sanctions, firms and the social planner prioritize investments on preventive controls. In scenario 2, where sanctions are high, firms are incentivized to prioritize investments in detective controls. Hence, firms invest differently than the social planner. In both intervals, $\phi_0 \leq b < \phi_{1,2}$ and $\phi_{1,2} \leq b \leq 1$, firms over-invest in detective and under-invest in preventive controls, regardless of the sanction level.

4.4.3 *Social Welfare*

In the interval without need for security information sharing, i. e., $0 \leq b < \phi_0$, firms invest at the socially optimal level. Therefore, they gain the same profit as the social planner. If the sharing effectiveness is high, i. e., in the intervals $\phi_0 \leq b < \phi_{1,2}$ and $\phi_{1,2} \leq b \leq 1$, firms generate less profit than the social planner as they over-invest in detective and under-invest in preventive controls. However, if the regulator effectively enforces mandatory information sharing and the sharing effectiveness is in the interval $\phi_{1,2} \leq b \leq 1$, firms are more profitable than without regulatory intervention.

5. DISCUSSION

We argue that our model captures important characteristics of mandatory security information sharing between firms and authorities. However, it cannot fully represent reality. We draw some conclusions from the analysis of our model in Section 5.1 and discuss limitations in Section 5.2.

5.1 Conclusion

If authorities are ineffective in dealing with security information, regulators should not enforce mandatory information sharing with authorities. Without the enforcement of information sharing, firms make security investments at levels comparable to a social planner. Our model predicts that, without a disclosure regime, investments are focused on detective rather than preventive controls. With our exogenous parameter choice, we find that security investments of firms account for 16.4 % of their total budget.

This situation changes if the information sharing effectiveness is high, but regulators do not enforce mandatory sharing. In this scenario, firms do not deviate from their investments introduced in the last paragraph. However, a social planner establishes security information sharing and prioritizes investments in preventive over investments in detective controls. Consequently, firms and social planner have different investment priorities. Our model predicts that firms under-invest in security, as a social planner would spend more than 16.4 % of the total budget of firms on internal controls. Specifically, security investment allocations of firms reveal that they under-invest in preventive, and over-invest in detective controls. These sub-optimal investments result in profits, and hence welfare, below the social optimum.

Regulators may introduce audits and sanctions to enforce mandatory security information sharing of firms with authorities. However, the sharing effectiveness of the authorities has to justify enforcement. If the sharing effectiveness is high and regulators enforce information sharing, firms adapt their investment decisions depending on the sanction level. If regulators effectively enforce legislation with a low sanction level, firms primarily invest in preventive rather than detective controls. This matches the investment priorities of a social planner. However, in this scenario, firms under-invest in security as compared to a planner. By contrast, if regulators effectively enforce legislation with a high sanction level, investment priorities of firms and a social planner can differ, as firms may primarily invest in detective rather than preventive controls. The explanation for this investment priority is intuitive: as audits cannot differentiate firms' malicious concealment of breaches from benign nescience, firms fear the threat of high sanctions that may apply for undetected and thus unreported security breaches. Furthermore, regulators have to keep in mind that a high sanction level may incentivize firms to over-invest in internal controls.

In every case where information sharing is effectively enforced, firms under-invest in preventive and over-invest in detective controls, regardless of the level of sanctions. Nevertheless, we observe that effective enforcement of information sharing may result in higher profits for firms as compared to a situation without regulation. In general, effective enforcement of security information sharing with a low sanction level results in higher profits for firms than the effective enforcement with high sanctions.

5.2 Limitations

Beyond the general limitations of analytical models using game theory as a solution concept, our approach only considers sanctions for unreported security breaches rather than sanctions for inadequate security investment levels. Sanctions for inadequate investment levels are proposed in, e. g., the currently discussed NIS-Directive [10]. Moreover, the influence of security information sharing on internal controls of firms remains a strong assumption specific to our model. Corresponding empirical evidence is missing. Therefore, caution is needed when transferring our conclusions to the real world. At the same time these limitations call for further research.

6. ACKNOWLEDGMENTS

Parts of this research and associated travels have been funded by the German Bundesministerium für Bildung und Forschung (BMBF) under grant agreement No. 16KIS0054.

7. REFERENCES

[1] R. Abrams. Target puts data breach costs at $148 million, and forecasts profit drop, 2014. Access: http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html. Last accessed: 27.07.2015.

[2] R. Anderson, R. Böhme, R. Clayton, and T. Moore. Security economics and the internal market. Technical report, European Union Agency for Network and Information Security (ENISA), 2008.

[3] J. M. Bauer and M. van Eeten. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10):706–719, 2009.

[4] R. Böhme. Security audits revisited. In A. Keromytis, editor, *Proceedings of Financial Cryptography and Data Security*, volume 7397 of *Lecture Notes in Computer Science*, pages 129–147, Berlin, Heidelberg, 2012. Springer.

[5] H. Cavusoglu, B. Mishra, and S. Raghunathan. A model for evaluating IT security investments. *Communications of the ACM*, 47(7):87–92, 2004.

[6] H. Cavusoglu, B. Mishra, and S. Raghunathan. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1):70–104, 2004.

[7] H. Cavusoglu, B. Mishra, and S. Raghunathan. The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, 16(1):28–46, 2005.

[8] D. M. Dekker, C. Karsberg, and B. Daskala. Cyber incident reporting in the EU – An overview of security articles in EU legislation. Technical report, European Union Agency for Network and Information Security (ENISA), 2012.

[9] Deutscher Bundestag. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). *Bundesgesetzblatt*, I(31):1324–1331, 2015.

[10] European Commission. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. *COM (2013) 48 final*, 2013.

[11] E. Gal-Or and A. Ghose. The economic incentives for sharing security information. *Information Systems Research*, 16(2):186–208, 2005.

[12] L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, 2002.

[13] L. A. Gordon, M. P. Loeb, and W. Lucyshyn. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22(6):461–485, 2003.

[14] K. Hausken. Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26(6):639–688, 2007.

[15] M. Khouzani, V. Pham, and C. Cid. Strategic discovery and sharing of vulnerabilities in competitive environments. In R. Poovendran and W. Saad, editors, *Decision and Game Theory for Security*, volume 8840 of *Lecture Notes in Computer Science*, pages 59–78, Berlin, Heidelberg, 2014. Springer.

[16] H. Kunreuther and G. Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2/3):231–249, 2003.

[17] S. Laube and R. Böhme. The economics of mandatory security breach reporting to authorities. In *Workshop on the Economics of Information Security (WEIS)*, Delft, 2015.

[18] National Conference of State Legislatures. State security breach notification laws, 2014. Access: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Last accessed: 27.07.2015.

[19] H. Öğüt, N. Memon, and S. Raghunathan. Cyber insurance and IT security investment: Impact of interdependent risk. In *Workshop on the Economics of Information Security (WEIS)*, Harvard, 2005.

[20] PricewaterhouseCoopers. Managing Cyber risks in an interconnected world: Key findings from the global state of information security survey 2014. Technical report, PricewaterhouseCoopers, 2014.

[21] S. Romanosky, R. Sharp, and A. Acquisti. Data breaches and identity theft: When is mandatory disclosure optimal? In *Workshop on Economics of Information Security (WEIS)*, Harvard, 2010.

APPENDIX

A. SOCIAL PLANNER'S INVESTMENTS IN CONTROLS WITHOUT SHARING

The first derivates of Eq. (11) w. r. t. d and x are

$$\frac{\partial o}{\partial d} = \lambda^{-d}\log(\lambda)(q_3 - q_1)P(x) - r \ ,$$
$$\frac{\partial o}{\partial x} = \beta^{-x}\log(\beta)((q_1 - q_3)D(d) + q_3) - r.$$

The roots of the conditions $\partial o/\partial d = 0$ and $\partial o/\partial x = 0$ are

$$d = \frac{\log\left(\frac{\log(\lambda)(q_3 - q_1)P(x)}{r}\right)}{\log(\lambda)} \ ,$$
$$x = \frac{\log\left(\frac{\log(\beta)((q_1 - q_3)D(d) + q_3)}{r}\right)}{\log(\beta)}.$$

Solving these two equations simultaneously results in

$$d^* = \frac{\log\left(\frac{(q_1 - q_3)(\log(\beta) - \log(\lambda))}{q_1\log(\beta)}\right)}{\log(\lambda)} \ ,$$
$$x^* = \frac{\log\left(-\frac{q_1\log(\beta)\log(\lambda)}{r\log(\beta) - r\log(\lambda)}\right)}{\log(\beta)}.$$

These equations correspond to Eq. (12) and Eq. (13).

B. SOCIAL PLANNER'S INVESTMENTS IN CONTROLS WITH SHARING

The first derivates of Eq. (14) w. r. t. d and x are

$$\frac{\partial o}{\partial d} = \frac{-(1+b)(q_1 + q_2 - q_3)\log(\lambda)P(x) - r\lambda^{bd+d}}{\lambda^{(1+b)d}} \ ,$$
$$\frac{\partial o}{\partial x} = \frac{(1+b)(q_3\log(\beta) + (q_1 + q_2 - q_3)\log(\beta)D(d)) - r\beta^{bx+x}}{\beta^{(1+b)x}}.$$

The roots of the conditions $\partial o/\partial d = 0$ and $\partial o/\partial x = 0$ are

$$d = \frac{\log\left(-\frac{(b+1)(q_1+q_2-q_3)\log(\lambda)P(x)}{r}\right)}{(b+1)\log(\lambda)} \ ,$$
$$x = \frac{\log\left(-\frac{(b+1)\log(\beta)(-q_3-(q_1+q_2-q_3)D(d))}{r}\right)}{(b+1)\log(\beta)}.$$

Solving these two equations simultaneously results in

$$d^* = \frac{\log\left(\frac{(\log(\beta)-\log(\lambda))(q_1+q_2-q_3)}{\log(\beta)(q_1+q_2)}\right)}{(b+1)\log(\lambda)} \ ,$$
$$x^* = \frac{\log\left(-\frac{(b+1)\log(\beta)\log(\lambda)(q_1+q_2)}{r(\log(\beta)-\log(\lambda))}\right)}{(1+b)\log(\beta)}.$$

These equations correspond to Eq. (15) and Eq. (16).

C. AGENTS' INVESTMENTS IN CONTROLS WITHOUT SHARING

The first derivates of Eq. (18) w. r. t. d_i and x_i are

$$\frac{\partial o}{\partial d_i} = \lambda^{-d_i}\log(\lambda)(q_3 - q_1)P - r \ ,$$
$$\frac{\partial o}{\partial x_i} = \beta^{-x_i}\log(\beta)((q_1 - q_3)D + q_3) - r.$$

The roots of the conditions $\partial o/\partial d_i = 0$ and $\partial o/\partial x_i = 0$, i. e., the best response of agent i, are

$$d_i^+(x_i, x_{1-i}) = \frac{\log\left(\frac{\log(\lambda)(q_3 - q_1)P}{r}\right)}{\log(\lambda)} \ ,$$
$$x_i^+(x_{1-i}, d_i) = \frac{\log\left(\frac{\log(\beta)((q_1 - q_3)D + q_3)}{r}\right)}{\log(\beta)}.$$

Solving these two equations simultaneously results in the Nash equilibrium

$$\tilde{d} = \frac{\log\left(\frac{(q_1 - q_3)(\log(\beta) - \log(\lambda))}{q_1\log(\beta)}\right)}{\log(\lambda)} \ ,$$
$$\tilde{x} = \frac{\log\left(-\frac{q_1\log(\beta)\log(\lambda)}{r\log(\beta) - r\log(\lambda)}\right)}{\log(\beta)}.$$

These equations correspond to Eq. (19) and Eq. (20).

D. AGENTS' INVESTMENTS IN CONTROLS WITH SHARING

The first derivates of Eq. (21) w. r. t. d_i and x_i are

$$\frac{\partial o}{\partial d_i} = \frac{\log(\lambda)(q_3 - q_1 + S)P_i}{\lambda^{bd_{1-i}+d_i}} - r \ ,$$
$$\frac{\partial o}{\partial x_i} = \frac{\log(\beta)(q_2 + q_3 + S - (q_3 - q_1 + S)D_i)}{\beta^{bx_{1-i}+x_i}} - r.$$

The roots of the conditions $\partial o/\partial d_i = 0$ and $\partial o/\partial x_i = 0$, i. e., the best response of agent i, are

$$d_i^+(x_i, x_{1-i}, d_{1-i}) = \frac{\log\left(\frac{(\log(\beta)-\log(\lambda))(q_1-q_3-S)}{\log(\beta)(q_1+q_2)}\right)}{\log(\lambda)} - bd_{1-i} \ ,$$
$$x_i^+(x_{1-i}, d_i, d_{1-i}) = \frac{\log\left(\frac{\log(\beta)\left((q_1+q_2)\lambda^{bd_{1-i}+d_i} - q_1 + q_3 + S\right)}{r\lambda^{bd_{1-i}+d_i}\beta^{bx_{1-i}}}\right)}{\log(\beta)}.$$

Based on the mutual best response $\tilde{x}(\tilde{d}) = x_i^+(\tilde{x}, \tilde{d}, \tilde{d})$ and $\tilde{d}(\tilde{x}) = d_i^+(\tilde{x}, \tilde{x}, \tilde{d})$, the Nash equilibrium has to satisfy

$$\tilde{d}(\tilde{x}) = \frac{\log(P(\tilde{x})) + \log(\log(\lambda)) + \log(q_3 - q_1 + S) - \log(r)}{(b+1)\log(\lambda)} \ ,$$
$$\tilde{x}(\tilde{d}) = \frac{\log(q_2 + q_3 + S - D(\tilde{d})(q_3 - q_1 + S))}{(b+1)\log(\beta)} + \frac{\log(\log(\beta)) - \log(r)}{(b+1)\log(\beta)}.$$

Solving these two equations simultaneously results in the Nash equilibrium

$$\tilde{d} = \frac{\log\left(\frac{(\log(\beta)-\log(\lambda))(q_1-q_3-S)}{\log(\beta)(q_1+q_2)}\right)}{(b+1)\log(\lambda)} \ ,$$
$$\tilde{x} = \frac{\log\left(-\frac{\log(\beta)\log(\lambda)(q_1+q_2)}{r(\log(\beta)-\log(\lambda))}\right)}{(b+1)\log(\beta)}.$$

These equations correspond to Eq. (22) and Eq. (23).

E. SYMBOLS

Table 3: List of Symbols.

Symbol	Type	Meaning	Constraint or value
x	choice variable	investments in preventive controls	$x > 0$
d	choice variable	investments in detective controls	$d > 0$
b	parameter	sharing effectiveness of an authority	$b \in [0, 1]$
S	parameter	sanction level	$S \geq 0$
B	constant	budget	$B = 1$
β	constant	security productivity	$\beta = 200$
λ	constant	security breach detection productivity	$\lambda = 250$
r	constant	return on investment	$r = 1.1$
q_1	constant	direct costs of a detected security breach	$q_1 = .009$
q_2	constant	indirect costs of a security breach	$q_2 = .011$
q_3	constant	direct costs of an undetected security breach	$q_3 = .5$
n	constant	number of firms	$n = 2$
c	function	expected costs	
o	function	profit of firms	
p	function	productive part of investments	
P	function	security breach probability	
D	function	security breach detection probability	
A	random variable	security breach	
$\hat{A}$	random variable	security breach detection	
α	realization	realization of A	$\alpha \in \{0, 1\}$
$\hat{\alpha}$	realization	realization of $\hat{A}$	$\hat{\alpha} \in \{0, 1\}$
a	realization	realization of security audits	$a \in \{0, 1\}$
t	realization	realization of security information sharing	$t \in \{0, 1\}$