The Economics of Mandatory Security Breach Reporting to Authorities

Stefan Laube*[1], Rainer Böhme[2]

[1] Department of Information Systems, University of Münster, Germany
Stefan.Laube@uni-muenster.de
[2] Institute of Computer Science, University of Innsbruck, Austria
Rainer.Boehme@uibk.ac.at

Abstract. Regulators in many countries enact security breach notification laws to address a lack of information security in their economies. Some of these laws designate authorities to handle reported security breaches and advise firms. We devise a principal–agent model to analyze the economic effect of mandatory security breach reporting to authorities. In practice, it is hard to enforce such laws as firms (agents) have little incentive to unilaterally report security breaches. In response, regulators (principals) may introduce security audits and impose sanctions. However, security audits cannot differentiate between malicious concealment and benign nescience of the agents. Even under optimistic assumptions about the effect of mandatory security breach reporting to authorities on reducing losses, our model predicts that it may be difficult to adjust the level of sanctions such that security breach notification laws are socially beneficial.

Keywords: Mandatory security breach reporting, interdependent security, information asymmetry, principal–agent theory, security audits

1 Motivation

Confidentiality, integrity and availability are the canonical protection goals of information systems. Security breaches are violations of one or more of these protection goals [15]. They may concern data protection or data security [10]. Over the past years, both the attack rate against information systems and the number of security breaches has increased, causing high costs to affected firms [36].

Cavusoglu et al. [5], among others, remark that security breaches may cause direct and indirect costs. Direct costs include for instance the costs of cleaning systems from malware. Indirect costs comprise intangible costs, which include costs from security breach announcements to the public coming along with, e. g., potential reputation loss [11]. Quantifying indirect costs of security breaches is generally hard. One approach suggested by the authors of [5] is to analyze the impact of published breaches on the stock market value of affected firms. The results show that security breaches create losses (on average) of 2.1 % of the market value within the first two days of their announcement. Cavusoglu et al. [5]

attribute this negative effect to a loss of confidence and trust of customers. They argue that when security breaches of firms become public, the indirect costs of these breaches exceed their direct costs.

Security breaches do not only generate costs at firms which are directly affected, but interdependence between information systems allows breaches to spread and negatively effect others [21]. In other words, lack of information security of firms causes negative externalities in an economy. For a number of reasons, critical national infrastructures are in a particularly exposed position [2]. The presence of negative externalities justifies government intervention, for instance in the form of laws with the prospect to decrease the costs to society [3, 18].

One particular approach is the introduction of security breach notification laws. In general, these laws differ in their design as:

1. they may *require* firms to *report security breaches to affected individuals*, via direct or mass communication (implemented in several US states [27]), or
2. they may *require* firms to *report security breaches to authorities* (implemented for firms of selected sectors in the EU [7]).

In essence, breach notification laws try to establish transparency on breaches such that firms (individuals) are able to protect themselves from propagated attacks, and to incentivize firms to effectively invest in information security. But as security information sharing and security investments are costly [11], the effectivity of security breach notification laws in decreasing costs to society has to be rigorously analyzed. We are aware of some empirical work on the economic effects of obliging firms to report security breaches to individuals (e. g., [1, 30, 31, 33]), and also find a theoretical model which examines this scenario [32]. Moreover, several models have been proposed which analyze the economic incentives for voluntary security information sharing between firms (e. g., [16, 11, 17]), and one model discusses the effects of security information sharing between firms and authorities [29]. However, we observe a lack of scientific investigations on the effectiveness of mandatory security breach reporting to authorities. As a starting point to close this research gap, we devise and analyze a principal–agent model which captures the conflicting interests between regulators and affected firms.

This paper is structured as follows: Section 2 provides a qualitative introduction to the object of research, and motivates our research question. Section 3 discusses relations of our work to prior art. We describe our principal–agent model and present social optima and Nash equilibria in Section 4. Section 5 concludes with a critical discussion and an outlook for future research.

2 Background and Research Question

Section 2.1 introduces prominent security breach notification laws, implemented in the US and the EU, and identifies problems that may lead to non-compliance of firms. Direct regulation is a tool to counter these problems. In Section 2.2, we discuss the effects of security breach notification laws, enforced by direct regulation, on natural incentives of firms to reduce security breach related costs. Our research question, proposed in Section 2.3, concerns the effectiveness of such laws.

2.1 Security Breach Notification Laws

Table 1 summarizes superficial characteristics of prominent US and EU security breach notification laws, presented in this Section. We observe that all of these laws have the objective to incentivize firms to take precautions against security or privacy breaches. This observation goes in line with previous discussions of such laws (e. g., [3]).

Table 1: Characteristics of prominent US and EU security breach notification laws

Country	Law	Obliged	Report	Address	Objective	Economics
US	State Laws [27]	Firms controlling personal data	P	I or A&I	IP&R	C or F&C
US	HIPAA & HITECH	Firms in the health care sector	P	A&I	IP&R	F&C
US	GLBA	Firms in the financial sector	P	I or A&I	IP&R	F&C
EU	Telecom Reform [7]	Firms in the telecom sector	S or P	A or A&I	IP&D or IP&D&R	F or F&C
EU	Regulation No 611/2013	Firms in the telecom sector & service providers	P	A or A&I	IP&D or IP&D&R	C
EU	Data Protec. Regulation* [8]	Data controllers and processors	P	A or A&I	IP&D or IP&D&R	F or F&C
EU	NIS-Directive* [9]	Market operators & public administrations	S&P	A	IP&D or IP&D&R	F or F&C

S	Security breaches	IP	Incentivize firms to take precautions
P	Privacy breaches	D	Dissemination of knowledge to firms
A	Authorities	R	Improve rights of affected individuals
I	Affected individuals	F	Imposes fines on firms
*	Proposed, not yet enacted	C	Potential of indirect costs for firms

Situation in the US. The first implemented security breach notification law in the US was the California Civil Code Section § 1798.29. This law requires private and public firms, conducting business in California, to report privacy breaches to affected individuals. Additionally, firms are obliged to report these breaches to authorities in the event that more than 500 data records are affected. The intention of this law is twofold: firstly, the provision of knowledge on breaches to affected individuals enables them to take mitigating actions – such as monitoring of credit card reports or filing of individual or class action lawsuits [32] – which improves their rights; secondly, the law incentivizes firms to encrypt data, as only privacy breaches of unencrypted data have to be reported.

The Californian law led to a high amount of privacy breach reporting, as firms only had to fear few compensation claims because affected individuals in

the US are not protected by a general right of information privacy [38].[3] Consequently, other US States enacted similar laws [27]. However, only few studies confirm their effectivity [30, 33]. Besides these state laws, there are sector specific breach notification laws in the US. Prominent examples are the HIPAA – with its amendments (HITECH) – and the GLBA, which oblige firms in the health care and financial sector, respectively, to report privacy breaches. In general, some of the breach notification laws in the US stipulate privacy breach reporting to individuals *only*, others *additionally* require firms to notify authorities. Moreover, many of these laws provide for fines, applicable in case of non-compliance of firms. However, as privacy breach announcements can result in considerable indirect costs [1], a lack of incentives for firms to report breaches may persist.

In January 2015, US President Barack Obama announced legislation with the objective to solve challenges of security information sharing amongst the US private sector and between the private sector and the government. This legislation will summarize the existing patchwork of US state security breach notification laws into one federal statute. Moreover, it will provide targeted liability protection for firms that share information about breaches with the DHS [37]. In this context, the House of Representatives (H.R.) passed two bills in April 2015, i. e., the "H.R.1560 – Protecting Cyber Networks Act" and the "H.R.1731 – National Cybersecurity Protection Advancement Act". (Note that both bills must still be passed by the Senate and signed by the President to get enacted.) Related to these two H.R. bills, the Senate (S.) introduced the "S.754 – Cybersecurity Information Sharing Act" to congress lately. Simultaneously to these legislative efforts, the Obama administration discusses the creation of a "Cyber Threat Intelligence Integration Center". This new authority will be responsible for the integration of available information on breaches from the private sector and other authorities, e. g., the NSA, DHS, and the FBI [35]. Efforts to coordinate information exchange on breaches are also observable in the EU.

Situation in the EU. In the EU, there are only sector specific security breach notification laws which *all* require firms to report to "Competent Authorities" [7, 18]. Most of these laws can be referred to as legislation in the context of the "Telecom reform", which passed into law in 2009. A prominent example of a law that stipulates breach reporting to authorities is the framework Directive 2009/140/EC, which has been enacted during the reform and affects firms of the telecommunication sector only. More extensive reporting obligations are formalized in the e-Privacy Directive. This Directive obliges telecoms firms to report privacy breaches to authorities, and, under some circumstances, *additionally* notify affected individuals. To clarify and detail the requirements of the e-Privacy Directive, the European Commission introduced Regulation No. 611/2013 in 2013.

As to the narrow definition of these EU security breach notification laws, they have a smaller coverage than the US laws. Specifically, reporting obligations of EU firms to authorities in the first instance – rather than to affected

[3] Affected individuals may be able to prove a causal relationship between harm and a privacy breach, such that their class actions might be successful.

individuals – stand in contrast to most of the US laws. Reporting to authorities has the objective to establish an economy wide transparency on security breaches [7]: informed authorities can disseminate conclusions drawn from security breaches (subsequently referred to as "dissemination of knowledge to firms"), i. e., provide affected firms with information on methods to minimize the impact of breaches or inform non-affected firms on how to protect against propagating attacks [29]. Some of the EU authorities are also authorized to announce information on accrued security breaches to the public or impose fines for non-compliance with the law. These latter two measures are intended to incentivize firms to take precautions against security breaches. However, they may fail to incentivize breach reporting in case that the expected fines and indirect costs of firms exceed their expected costs of malicious concealment.

Currently, two fundamental legislative proposals are discussed in the EU, which both intend to expand existing security breach notification laws:

- A "EU Data Protection Regulation" [8], which requires "data controllers and processors" in the EU[4] to report privacy breaches to authorities. Additionally, once authorities are notified and in case that adverse impact is determined, this law obliges to inform affected individuals. The Regulation has the objective to harmonize and unify existing EU privacy breach reporting obligations, and will supersede the data protection Directive 95/46/EC.
- A "Network and Information Security" Directive (NIS-Directive) [9], which requires EU "market operators and public administrations"[5] to report security breaches to authorities *only*. This Directive has the objective to reduce security breach related costs in the EU by overcoming information asymmetries and increasing the overall level of information security. It extends the already implemented sector specific security breach notification laws.

Legislation similar to the NIS-Directive motivates an economic analysis of mandatory security breach reporting to authorities *only*. The NIS-Directive has already passed the EU-Parliament in March 2014, but the Council's endorsement is still pending. Its novelty is the provision of direct regulation, i. e., security audits, and sanctions to address issues like free riding and opportunism of firms, which have been identified with other US and EU notification laws. A legal analysis of Winn [38] supports that direct regulation is likely to be necessary in security breach notification laws, as firms may seek to exploit alternative, weaker, enforcement mechanisms. However, questions on the practical implementation of the NIS-Directive remain open. Our working-hypothesis is that firms get sanctioned in case that non-reported breaches are discovered during a security audit. This may change the natural incentives of firms to reduce breach related costs.

[4] The Regulation will also apply for firms based outside the EU, processing data of EU residents.

[5] Note that "market operators and public administrations" are broad terms in [9]. In the context of the NIS-Directive, we refer to "market operators and public administrations" as firms.

2.2 Incentives of Firms

Cavusoglu et al. [6] find that the economy wide increase in the number of security breaches [36] incentivizes firms to extensively invest in internal control mechanisms. The authors distinguish between two categories of these mechanisms: preventive and detective controls. Preventive controls, such as firewalls, try to shield information systems in order to secure them from security beaches. We interpret a firm's investment in preventive controls as *security investment*. Detective controls, such as intrusion detection systems (IDS), try to detect security breaches that already happened. However, detective controls may result in type I errors (alerts, even though there is no security breach) and type II errors (absence of alerts, even though there is a security breach). In order to protect against propagating attacks [29] or to leverage security investment [24], firms may also have some natural incentives to voluntarily share security information with each other [11]. "Security Based Information Sharing Organizations" (SB/ISOs), such as "Information Sharing Analysis Centers" (ISACs), facilitate a platform for this purpose. Relevant security information that can be shared in SB/ISOs include knowledge on security breaches, security breach attempts, or methods to minimize the impact of breaches [16].

Laws with the prospect to enforce mandatory security breach reporting to authorities, similar to the NIS-Directive [9], affect these natural incentives of firms:

- They may incentivize firms to report security breaches to authorities, as non-reported breaches may lead to sanctions in the event of security audits.
- They may incentivize firms to invest in detective controls, as non-detected breaches inevitably result in non-reporting, which may lead to sanctions in the event of security audits.
- They may incentivize firms to increase their security investments, i. e., reduce the number of security breaches and therefore reporting obligations.
- Authorities can announce information on reported security breaches to the public, which may result in indirect costs for firms [5]. This may foster security investments of firms to prevent breaches and reporting obligations.
- Authorities can advise firms by dissemination of knowledge on reported breaches. This can reduce interdependence between firms or leverage their security investments [29], but may also result in free riding behavior [16].

Overall, enforced security breach notification laws may incentivize firms to internalize negative externalities. Simultaneously, these laws may cause free riding and opportunism. Compliance costs of firms include additional security investments. Moreover, in the event of a security breach, firms do not only have to bear direct costs, but compliance results in what we may call "disclosure costs", i. e., expected indirect costs and expenses emerging from bureaucratic burdens. In case of non-compliance, firms also have to expect sanctions.

We are not aware of previous research analyzing the potential economic benefits and barriers of mandatory security breach reporting to authorities, enforced by direct regulation. This leads to our research question.

2.3 Research Question

The objectives of the NIS-Directive [9] motivate our research question:

> *Mandatory security breach reporting to authorities (cf. Section 2.1), enforced by audits and sanctions, may change the natural incentives of firms to reduce security breach related costs (cf. Section 2.2). Does this change of incentives result in an increase in (a) the overall level of information security, and (b) a decrease in social costs?*

The response to this question is relevant for security managers of firms, who decide on the *reporting of security breaches* and *security investments*. Moreover, it is relevant for regulators who enforce security breach notification laws with the use of direct regulation, i. e., *security audits*, and *sanctions*.

In this paper, we devise and analyze a principal–agent model to answer our research question. The model includes free parameters for the following properties: interdependence of information security (cf. Section 1), an informed authority's effectiveness in dissemination of knowledge to firms (cf. Section 2.1), the error rate of detective controls (cf. Section 2.2), and the disclosure costs associated with security breach reporting of firms (cf. Section 2.2).

3 Related Work

Two streams of theoretical literature are closely related to our work: papers on the effectiveness of audits in the context of principal–agent problems (cf. Section 3.1), and papers on the economics of security information sharing. The second stream of literature can be further divided in papers that discusses the economic incentives for

- *voluntary* information sharing *between firms* (cf. Section 3.2);
- *mandatory* information sharing *between firms and individuals* (cf. Section 3.3);
- *mandatory* information sharing *between firms and authorities* (cf. Section 3.4).

3.1 Effectiveness of Audits in Principal–Agent Setups

Ng and Stoeckenius [28] were among the first to analyze the effectiveness of audits to solve a principal–agent problem. They identify a moral hazard problem between an owner (principal) and the management (agent) of a firm, and discuss how audits can incentivize the agent to truthfully report to the principal. Their seminal work in 1979 has triggered lots of research on principal–agent problems with moral hazard and adverse selection (e. g., [26, 39]). Much of this research has in common that audits are contractually agreed upon [22], i. e., to overcome information asymmetries, the principal proposes a *contract* to the agent which includes audits as a credible signal. By contrast, we analyze the design of *legislation* which includes audits and sanctions to incentivize compliance.

3.2 Voluntary Information Sharing between Firms

There is substantial work on *voluntary* information sharing *between firms*. All of the consecutively introduced papers assume security information sharing to be conducted in SB/ISOs. Moreover, most of these papers use a model with two interdependent [21] firms representing an economy, where both firms may invest in information security to decrease the probability of security breaches to their information systems. To capture security investment decisions of firms, the authors usually base their model on the assumptions of Gordon and Loeb [14].

Gordon et al. [16] evaluate the cost side effects of security breaches and security information sharing. They assume that information sharing between firms has a leverage effect on their security investments, and show that information sharing reduces information security expenditures of firms. Thus, the authors find that security investment and security information sharing can act as strategic substitutes. By contrast, Gal-Or and Ghose [11] analyze demand-side effects of security investment and information sharing. According to them, information sharing between firms, e. g., security vendors in IT-ISACs, has a positive effect on the demand of their IT security products. However, information sharing may also result in indirect costs. The authors find that security investment and information sharing can act as strategic complements. Similar to [11, 16], Hausken [17] proposes a model for information sharing between firms, but adds a strategic attacker. He assumes that information sharing may have a positive effect on a firm's profit, and is accompanied by indirect costs. His analysis shows that individual information sharing of firms increases with the interdependence in SB/ISOs, and is zero in case of no or negative interdependence. Liu et al. [24] show that the nature of information assets, possessed and secured by firms, plays a crucial role for decisions on information sharing and security investment. Consistent with [16], Liu et al. [24] assume that information sharing can leverage security investments. They find that in case of complementary assets, firms have a natural incentive to share security information. By contrast, when firms possess substitutable assets, they do not share. Either way, investments of firms are sub-optimal without the introduction of a coordination mechanisms. Gao et al. [12, 13] propose two different papers on information sharing, inspired by [24] and [17], respectively. Among other things, they analyze the effects on social welfare in case that a social planner controls information sharing of firms, their security investments, or both. In [12], the authors demonstrate that the intervention of a social planner can be – but not necessarily is – preferable to the case where firms choose individually. Contrarily, in [13], they show that the intervention of a social planner always has positive implications on social welfare.

Khouzani et al. [19] proposes a model on security information sharing that differs from the approaches introduced before: it respects the investments of firms in discovery of security vulnerabilities, and sharing of their findings. The authors consider that knowledge on vulnerabilities has a positive effect on the utility of firms. They find that firms share information on detected vulnerabilities in case that information security behaves as a common good – and vice versa.

Our model setup in this paper is closely related to the above-cited works.

3.3 Mandatory Information Sharing between Firms and Individuals

Considerably less work addresses *mandatory* information sharing *between firms and individuals*, although there are corresponding security breach notification laws in several US States [27]. Romanosky et al. [32] are the first – and to our knowledge only – ones to specifically focus on this research topic. Their model captures a firm which may suffer from a data breach. The authors assume that if the firm is breached, and breach disclosure is not mandatory, not only the firm but also affected customers suffer losses. The losses to affected customers result from their inability to take mitigating actions. Romanosky et al. [32] find that costs of firms are higher under disclosure regimes. However, as mandatory disclosure may incentivize firms to invest in security, and enables actions of customers to reduce losses, corresponding security breach notification laws may decrease the social costs. Furthermore, the authors argue that some political instruments may be necessary for social planners to optimally reduce social costs.

Our model in this paper does not stand in the tradition of the work by Romanosky et al. [32] as we do not consider costs of individuals.

3.4 Mandatory Information Sharing between Firms and Authorities

Öğüt et al. [29] are – to our knowledge – the only ones that discuss the economics of security information sharing *between firms and authorities*. However, they do not analyze *mandatory* information sharing. The authors primarily investigate the effects of security interdependence between firms on their incentives to invest in information security and cyber insurance. Their findings suggest that interdependence of firms can lead to reduced incentives to invest in security. However, security information sharing between firms and authorities may change this situation and mitigate negative effects of security interdependence, given that information sharing either reduces the direct attack probability on firms or interdependence in the economy. The authors conclude that information sharing can result in positive welfare effects. Our model builds up on these findings.

In what follows, we will devise a principal–agent model composed of established modeling assumptions. Our work is primarily inspired by theoretical literature on voluntary information sharing between firms. Motivated by this literature, our model comprises two firms, representing an economy. We combine security investment assumptions [14] with a model of security interdependence [21] to derive the expected costs due to security issues of firms. Additionally, we adopt the assumption that security information sharing between firms and authorities may reduce security interdependence [29]. Our model also respects disclosure costs of firms, comprising indirect costs [11], which may hinder information sharing. Regulators can counter suboptimal information sharing and security investments of firms with the enforcement of a security breach notification law [9]. The conflict of interest between firms, which have to report to an authority acting on behalf of regulators, and regulators can be interpreted as a principal–agent problem with moral hazard [22].

4 Model

Our principal–agent model consists of three different components: a model for security investment and interdependent security, a formalization of mandatory security breach reporting to an authority, and a formalization of security audits. These components will be described in Section 4.1, 4.2, and 4.3, respectively. Each component includes at least one of the free parameters specified in Section 2.3. We will study the model's social optima in Section 4.4 and its Nash equilibria in Section 4.5. Table 2 in Appendix A summarizes all symbols used.

4.1 Security Investment and Interdependence

Consider for now a single rational firm belonging to a larger economy. This firm invests the amount $x \geq 0$ in information security to decrease the probability P of security breaches of its information system. Gordon and Loeb [14] characterize this relationship as $P(x)$. With an increase in the security investment x, the probability of a security breach decreases $P'(x) < 0$, but at a decreasing rate $P''(x) > 0$, i. e., $\lim_{x\to\infty} P(x) \to 0$. Following Böhme [4], a simple way to capture this relationship in a functional form is $P(x) = \beta^{-x}$. The parameter β represents the security productivity of the firm, which we subsequently assume to be "moderate", i. e., $\beta = 20$. Furthermore, we assume that each attack on an unprotected information system $x = 0$ results in a security breach and causes direct costs q_1. We define the direct cost of a security breach as $q_1 = 1$ to normalize the monetary scale. The firm's expected costs due to security issues are given by

$$c(x) = P(x) \cdot q_1 + x. \tag{1}$$

We generalize this model setup to an economy with $n = 2$ symmetric, a priori homogenous and rational firms. Both firms $i \in \{0, 1\}$ individually choose their security investment x_i. According to Öğüt et al. [29], who introduce a *parameter for the security interdependence* $\gamma \in [0, 1]$ *between two firms*, we can express the security breach probability at firm i as

$$P_i(x_i, x_{1-i}) = 1 - (1 - P(x_i)) \cdot (1 - \gamma \cdot P(x_{1-i})). \tag{2}$$

4.2 Detective Controls and Security Breach Notification Laws

Let $\alpha_i \in \{0, 1\}$ denote the realization of the random variable B (breach). Consequently, the security breach probability at firm i is $Pr(\alpha_i = 1) = P_i(x_i, x_{1-i})$. We assume that both firms have a self-interest to detect security breaches and denote the realization of the random variable D (security breach detected) as $\hat{\alpha}_i \in \{0, 1\}$. Therefore, the success probability of detective controls is $Pr(\hat{\alpha}_i = 1 | \alpha_i = 1) = 1 - \epsilon$, where $\epsilon \in]0, 1]$ is the *parameter for the error rate of detective controls*. We assume that, as an exemplary detective control, firms use IDS. However, we ignore potential costs of such systems to restrict the number of parameters in our model. Moreover, as a further simplification,

consider that the type I error rate of IDS is 0 %. A study of Lippmann et al. [23] shows that even the best IDS only detect about 80 % of attacks that have happened. Therefore, we optimistically assume a type II error rate of $\epsilon = 20\,\%$ in subsequent figures.

Once a security breach is detected, breach notification laws require firms to decide on breach reporting $\tilde{\alpha}_i \in \{0, 1\}$ to an authority. We indicate a firm's decision to report the information that no security breach has been detected as $\tilde{\alpha}_i = 0$. Accordingly, $\tilde{\alpha}_i = 1$ indicates that a firm reports a detected security breach to an authority. Thus, compliance with security breach notification laws is $Pr(\tilde{\alpha}_i = 1 | \hat{\alpha}_i = 1 \wedge \alpha_i = 1) = t_i$. For the sake of simplicity, we assume that nobody has an interest in reporting feigned incidents that did not happen.

In case that a firm reports breach information to an authority, this authority can disseminate conclusions drawn from this breach to other firms with the objective to decrease social costs. According to Öğüt et al. [29], the positive effect from such dissemination of knowledge may be interpreted as a reduction of the interdependence between firms (when information on the protection against propagating attacks is exchanged) or an enhancement in their efficiency of security investments (when security best practices are exchanged). Subsequently, we assume that an authority's disseminated knowledge reduces interdependence, denoted by the function $1 \geq \eta(t) \geq 0$. Thus, the breach probability at firm i is

$$P_i(x_i, x_{1-i}, t_{1-i}) = 1 - (1 - P(x_i)) \cdot (1 - \gamma \cdot \eta(t_{1-i}) \cdot P(x_{1-i})). \tag{3}$$

Observe from Eq. (3) that truthful reporting t_i of firm i does not contribute to a reduction of its interdependence to firm $1 - i$: for $n \to \infty$, a single firm's contribution to the reduction of interdependence is insignificant. Let $b \in [0, 1]$ denote the *parameter for an informed authority's effectiveness in dissemination of knowledge to firms*. Hence, we can define $\eta(t_{1-i})$ as

$$\eta(t_{1-i}) = 1 - b \cdot (1 - \epsilon) \cdot t_{1-i}. \tag{4}$$

4.3 Disclosure Costs and Security Audits

If regulators pass breach notification laws, firms do not only respect direct costs of security breaches, but also disclosure costs associated with breach reporting. These disclosure costs may, e. g., arise because of bureaucratic burdens or an authority's announcement of reported breaches to the public. Let $q_2 \in [0, \infty[$ denote the *parameter for a firm's disclosure costs associated with security breach reporting*. As truthful reporting t_i affects a firm's sum of breach related costs $L_i(t_i)$, expected costs due to security issues $c_i(x_i, x_{1-i}, t_i, t_{1-i})$ are

$$c_i(x_i, x_{1-i}, t_i, t_{1-i}) = P_i(x_i, x_{1-i}, t_{1-i}) \cdot L_i(t_i) + x_i \tag{5}$$

$$L_i(t_i) = (1 - \epsilon) \cdot t_i \cdot q_2 + q_1. \tag{6}$$

Disclosure costs associated with security breach reporting lead to a conflict of interest between firms and regulators, hereinafter interpreted as a principal–agent problem with moral hazard. A representative regulator (principal) introduces a security breach notification law. Firms (agents) invest in information

security and may possess knowledge on security breaches that have happened to their information system. However, agents may only have little incentives to unilaterally report these breaches, because of associated disclosure costs. Thus, they may take precautions against security breaches based on their self-interests. In response, the principal introduces audits of the information systems of agents, and imposes sanctions for non-compliance with the law.

Let $\psi \in \{0, 1\}$ denote the realization of the random variable A (audit), such that $Pr(\psi = 1) = a$ depicts the probability for an agent's information system to get audited. We assume that any realized security audit detects every security breach that has happened with certainty, i. e., per definition, audits are more reliable than detective controls.

The decision tree in Fig. 1 summarizes the security breach related costs of agent i under such a disclosure regime. The figure comprises all decisions of both agent and principal. Dashed lines represent uncertainty because of nature's decisions. At first, the agent invests x_i in information security. Thereafter, an attack on his information system takes place. This attack is successful with probability $P_i(x_i, x_{1-i}, t_{1-i})$. We assume that, per period under consideration, there can only be one security breach to an agent's information system at most. After a security breach has happened, the agent detects it with the probability $1-\epsilon$. Moreover, regardless of the agent's detection, he faces a reporting decision. In case that the agent does not report a security breach, the principal conducts security audits at random. If the principal detects an unreported security breach during a security audit, the agent is penalized with sanctions $S \in [0, \infty[$.

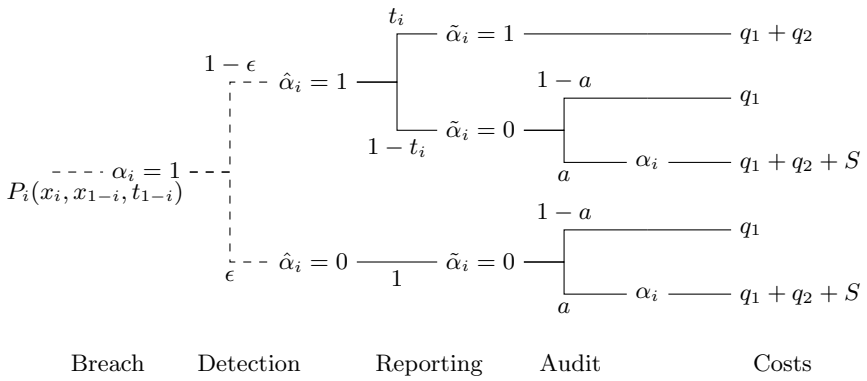


Fig. 1: Decisions of agent i, principal, and nature

We can derive the expected costs due to security issues of agent i, given mandatory security breach reporting to an authority, from Fig. 1:

$$c_i(x_i, x_{1-i}, t_i, t_{1-i}, a) = P_i(x_i, x_{1-i}, t_{1-i}) \cdot L_i(t_i, a) + x_i \tag{7}$$

$$L_i(t_i, a) = (1 - \epsilon) \cdot [t_i \cdot q_2 + (1 - t_i) \cdot a \cdot (q_2 + S)] + \epsilon \cdot a \cdot (q_2 + S) + q_1. \tag{8}$$

Observe from Eq. (8) that the principal can substitute the audit probability a with the sanction level S. If the principal introduces infinitely high sanctions, and given a positive audit probability, agents always have incentives to report security breaches. This result is trivial and prevents a comparison of alternative incentive schemes. Therefore, we follow Khouzani et al. [20], and fix the sanctions to an assumed to be collectable level $S = 1$. (Note that this level is equal to the direct costs of a security breach $S = q_1 = 1$.) Consequently, the choice on the security audit probability constitutes the principal's only decision.

4.4 Social Optima

Social costs are defined as the sum of the expected costs of all agents. A social planner with control over security breach reporting, security investments, and security audits (note that a social planner does not require audits, as their purpose is to incentivize truthful reporting and security investments of the agents only), has the following minimization problem, based on the costs of an agent in Eq. (7):

$$(x^*, t^*) = \arg\min_{x,t} 2 \cdot c(x, x, t, t, 0). \tag{9}$$

We may substitute x_i by x and t_i by t because of our symmetry assumption. The solution to the problem in Eq. (9), proposed in Appendix B, consists of extreme and boundary values.

Security investment is

$$x^*(t^*) = -\frac{\log\left(\frac{\gamma\cdot\eta(t^*)+1}{4\cdot\gamma\cdot\eta(t^*)} - \sqrt{\frac{(\gamma\cdot\eta(t^*)+1)^2}{16\cdot\gamma^2\cdot\eta(t^*)^2} - \frac{1}{2\cdot\gamma\cdot\log(\beta)\cdot\eta(t^*)\cdot L(t^*,0)}}\right)}{\log(\beta)}. \tag{10}$$

Security breach reporting is

$$t^*(x^*(t^*)) = \begin{cases} 1, \text{ if } c(x^*(0), x^*(0), 0, 0, 0) > c(x^*(1), x^*(1), 1, 1, 0) \\ 0, \text{ else.} \end{cases} \tag{11}$$

The case distinction in Eq. (11) can be interpreted as the implementation of a security breach notification law under the assumption of honest agents.

Proposition 1. *Given that $b > 0$, $\gamma > 0$, $q_2 > 0$, $\epsilon > 0$ and for any x^*, a truthfulness of $0 < t < 1$ is not socially optimal. Under these conditions, the socially optimal truthfulness $t^*(x^*(t^*))$ depends on a threshold value.*

Proof. The proof is in Appendix B.2.

Fig. 2 illustrates regions for social optima depending on different situations in the (q_2,γ,b)-parameter space. The three lines, each starting in the origin of the coordinate system, indicate a social planner's indifference in security breach reporting $c(x^*(0), x^*(0), 0, 0, 0) = c(x^*(1), x^*(1), 1, 1, 0)$ for three different types of effectiveness b of an authority. In the region below each line, security breaches are reported, i. e., the social optimum is $(x^*(1), 1)$, and vice versa. Observe that

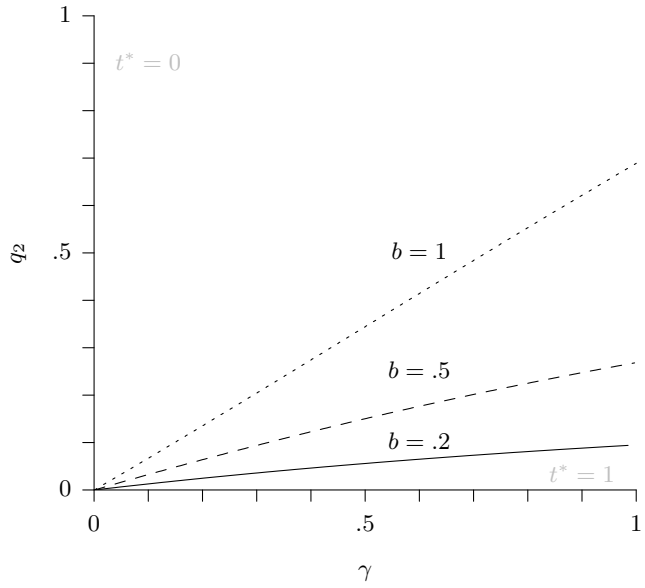


Fig. 2: Social planner's case distinction in (q_2,γ,b)-parameter space

the regions below the lines get larger for a more effective authority. In contrast to this, with an increase in the error rate of detective controls ϵ, all lines in Fig. 2 decline to the abscissa, ceteris paribus. The reason for this is that an increase in the probability of undetected breaches leads to a reduced amount of security breach reporting. Thus, as an authority can only disseminate less knowledge, there is a negative effect on the reduction of security interdependence $\eta(t)$.

By comparing Fig. 3 (a) with Fig. 3 (b) (change in +), we observe that a social planner's optimal security investment increases with an increase in interdependence γ between the two agents.

4.5 Nash Equilibria

In practice, there is no social planner and incentives determine the willingness of agents to minimize expected costs due to security issues. A game-theoretic approach is needed to analyze these incentives. In what follows, we search for the pure strategy Nash equilibria of the devised principal–agent game, i. e., the fixed points of the best response of principal and agents. According to Macho-Stadler and Pérez-Castrillo [25], Nash equilibria of a principal–agent game with moral hazard can be derived by the following steps: (1) determination of the Nash equilibria between agents, disregarding the best response of the principal, and (2) backwards induction to determine the principal's best response.

(1) Agents. After a security breach notification law is implemented, agents simultaneously and independently decide on security investments and security breach reporting with the objective to minimize their expected costs, specified in Eq. (7). Consequently, agent i has the following minimization problem:

$$(x_i^+, t_i^+) = \underset{x_i, t_i}{\arg\min}\, c_i(x_i, x_{1-i}, t_i, t_{1-i}, a) \quad \text{s. t. } x_i \geq 0. \tag{12}$$

Solving the problem in Eq. (12) results in the best response of agent i, given decisions of agent $1-i$. Nash equilibria follow from the mutual best response of the two symmetric agents. The derivation of equilibria between agents is proposed in Appendix C.

Security investment is

$$\tilde{x}_{1,2}(\tilde{t}, a) = -\frac{\log\left(\frac{1}{2\cdot\gamma\cdot\eta(\tilde{t})} \pm \sqrt{\frac{1}{4\cdot\gamma^2\cdot\eta(\tilde{t})^2} - \frac{1}{\gamma\cdot\log(\beta)\cdot\eta(\tilde{t})\cdot L(\tilde{t},a)}}\right)}{\log(\beta)} \tag{13}$$

$$\tilde{x}_3(\tilde{t}, a) = 0. \tag{14}$$

Lemma 1. *Given that $\tilde{x}_1(\tilde{t}, a)$ exists, the equilibrium $\tilde{x}_3(\tilde{t}, a)$ exists simultaneously. Moreover, there are parameter settings where only $\tilde{x}_2(\tilde{t}, a)$ or $\tilde{x}_3(\tilde{t}, a)$ persist. If all equilibria $\tilde{x}_{1,2,3}(\tilde{t}, a)$ exist, we find that $\tilde{x}_{1,3}(\tilde{t}, a) \leq \tilde{x}_2(\tilde{t}, a)$.*

Proof. The proof is in Appendix C.2.

Security breach reporting is

$$\tilde{t}(\tilde{x}, a) = \begin{cases} 1, \text{ if } a \geq a_{min} \vee q_2 = 0 \\ 0, \text{ else.} \end{cases} \tag{15}$$

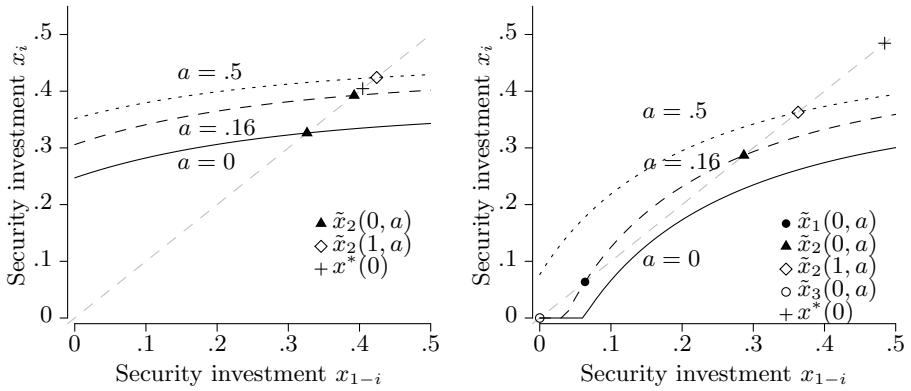
Lemma 2. *Given that no disclosure costs are associated with security breach reporting, $q_2 = 0$, marginal risk averse agents voluntarily report security breaches $t = 1$. Otherwise, in case that $q_2 > 0$, marginal risk averse agents do not report breaches unless an audit probability of $a \geq a_{min} = q_2/(q_2 + S)$ is introduced.*

Proof. The proof is in Appendix C.3.

Proposition 2. *In case of low interdependence, only the Nash equilibrium $(a, \tilde{t}, \tilde{x}_2(\tilde{t}, a))$ exists. Otherwise, with high interdependence, the Nash equilibrium $(a, \tilde{t}, \tilde{x}_3(\tilde{t}, a))$, or the Nash equilibria $(a, \tilde{t}, \tilde{x}_{1,2,3}(\tilde{t}, a))$, or $(a, \tilde{t}, \tilde{x}_2(\tilde{t}, a))$ exist, depending on the audit probability and the other free model parameter.*

Proof. Follows from Lemma 1 and Lemma 2. □

Fig. 3 (a) and (b) demonstrate all interesting cases of an agent's best response in security investment. Note that reporting strategies in these figures depend on the principal's introduced audit probability. Both figures each include the socially optimal security investment $x^*(0)$ as a reference point (indicated by +).



(a) Best response of agent i ($\gamma = .3$) (b) Best response of agent i ($\gamma = .8$)

Fig. 3: Best response in security investment of agent i, cf. Eq. (24), given security investment of agent $1 - i$; reporting strategies depend on the principal's audit probability; Nash equilibria and social optima are depicted on the angle bisector ($b = .2; q_2 = .2; a_{min} = .166$)

If agents expect disclosure costs associated with security breach reporting to an authority, a security breach notification law without security audits is ineffective (cf. Lemma 2). In this scenario, up to three Nash equilibria may exist ($a = 0, \tilde{t} = 0, \tilde{x}_{1,2,3}(0,0)$), depending on all free model parameters (cf. Lemma 1). These Nash equilibria include security investments which are below the social optima (cf. Fig. 3), given that $x^*(t^*) \neq 0$. Audits with a probability of $0 < a < a_{min}$ may establish incentives for higher security investments of the agents (cf. Fig. 3). Yet, as long as the audit probability does not reach the threshold a_{min}, marginal risk averse agents do not report breaches (cf. Lemma 2).

In case of low interdependence γ, a security breach notification law without security audits results in the Nash equilibrium $(0, 0, \tilde{x}_2(0,0))$ (cf. Fig. 3 (a) and Proposition 2). An audit probability $a \geq a_{min}$ incentivizes marginal risk averse agents to report breaches and increase security investments. However, if the principal introduces a very high audit probability $a \gg a_{min}$, investments of the agents exceed the socially optimal level (cf. + and □ in Fig. 3 (a)).

In case of high interdependence γ, a security breach notification law without security audits results in the Nash equilibrium $(0, 0, \tilde{x}_3(0,0))$, where agents do not invest in information security at all (cf. Fig. 3 (b) and Proposition 2). In this scenario, security audits are most effective. An increase in the audit probability $0 < a < a_{min}$ eventually leads to two additional equilibria $(a, 0, \tilde{x}_{1,2}(0,a))$. An audit probability $a \geq a_{min}$ incentivizes marginal risk averse agents to report security breaches, and only the Nash equilibrium $(a, 1, \tilde{x}_2(1,a))$ persists (cf. Fig. 3 (b) and Proposition 2).

(2) Principal. The principal choses the audit probability. He has to observe the maximum security investment $\tilde{x}_2(\tilde{t}, a)$ of the agents as incentive compatibility constraint. Moreover, since an implemented security breach notification law is legally binding, the principal does not have to consider participation constraints. His objective is to minimize social costs:

$$\tilde{a} = \arg\min_{a} 2 \cdot c(\tilde{x}_2(\tilde{t}, a), \tilde{x}_2(\tilde{t}, a), \tilde{t}(\tilde{x}, a), \tilde{t}(\tilde{x}, a), a). \tag{16}$$

Lemma 3. *Given a positive sanction level $S > 0$, and disregarding the case where a marginal increase in audit probability has a positive net effect on social cost by inciting $t = 1$, the social costs always increase in the audit probability.*

Proof. The proof is in Appendix D.1.

Based on Lemma 3, a high audit probability has to be avoided. However, based on Lemma 2, audits may incentivize security breach reporting. Consequently, the principal introduces an audit probability which just breaks even to incentivize reporting of marginal risk averse agents, i. e., a_{min}, and at the same time reduces the social costs. Otherwise, audits are ineffective. This leads to

$$\tilde{a} = \begin{cases} a_{min}, \text{ if } c(\tilde{x}_2(0,0), \tilde{x}_2(0,0), 0, 0, 0) > c(\tilde{x}_2(1, a_{min}), \tilde{x}_2(1, a_{min}), 1, 1, a_{min}) \\ 0, \quad \text{else.} \end{cases} \tag{17}$$

Lemma 4. *Given that $q_2 > 0$, $S > 0$, and a_{min} is the audit probability in equilibrium, the optimal audit probability a_{min} decreases with the sanction level S and increases with the disclosure costs q_2 of the agents.*

Proof. The proof is in Appendix D.2.

Proposition 3. *The optimal audit probability $\tilde{a}$ depicts a threshold value. Given that audits with the probability $\tilde{a} = a_{min}$ result in lower social costs than audits with the probability $\tilde{a} = 0$, and given marginal risk averse agents, the Nash equilibrium $(\tilde{a} = a_{min}, \tilde{t} = 1, \tilde{x}_2(1, a_{min}))$ exists. Otherwise, the optimal audit probability is $\tilde{a} = 0$, and all Nash equilibria from Proposition 2 may exist.*

Proof. Follows from Eq. (17). □

Fig. 4 illustrates regions for Nash equilibria, given marginal risk averse agents and depending on different situations in the (q_2,γ,b)-parameter space. In the regions below the lines in Fig. 4, the principal introduces audits which just break even to incentivize security breach reporting a_{min}, and the Nash equilibrium $(\tilde{a} = a_{min}, \tilde{t} = 1, \tilde{x}_2(1, a_{min}))$ exists (cf. Proposition 3). In these regions, a security breach notification law with security audits decreases social costs. We conclude that **the enforcement of mandatory security breach reporting to an authority is effective in case of high interdependence between agents, low disclosure costs associated with security breach reporting, a high effectiveness of an informed authority in dissemination of knowledge to agents, and a low error rate of detective controls**.

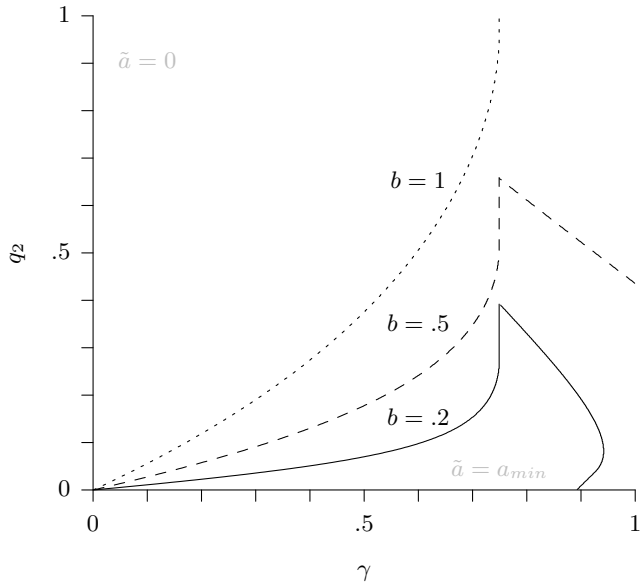


Fig. 4: Principal's case distinction in (q_2,γ,b)-parameter space

Observe that audits can stimulate security investments of agents in case of high interdependence (cf. the heavy slope of the lines at $\gamma = .749$ in Fig. 4).

In the regions above the lines in Fig. 4, a security breach notification law with audits increases social costs. Consequently, the principal does not introduce security audits, and up to three Nash equilibria may exist (cf. Proposition 3). With an increase in the error rate of detective controls ϵ, ceteris paribus, the lines in Fig. 4 decline to the abscissa. The reason for this is that an increasing error rate results in fewer security breach detection and reporting of the agents (cf. Fig. 1). Hence, expected sanctions of the agents rise. This results in a reduction of the effectiveness of a security breach notification law with security audits.

5 Discussion

The devised principal–agent model covers important characteristics of the conflict of interest between regulators, who enforce security breach notification laws, and firms. However, it cannot fully represent reality. Nevertheless, we can draw new conclusions from the analysis of our model with four parameters. We present these conclusions in Section 5.1. Finally, we discuss possible model extensions as an outlook for future research in Section 5.2.

5.1 Conclusions

Security breach notification laws *without* security audits, regardless of the level of sanctions, cannot incentivize firms to report security breaches to authorities, given positive disclosure costs. In turn, authorities cannot disseminate knowledge to other firms. In this scenario, firms realize security investments based on their natural incentives. These investments are below the socially optimal level. Under such disclosure regimes, the few firms in an economy which report security breaches in the absence of security audits internalize negative externalities.

Security breach notification laws *with* security audits *and* sanctions may incentivize firms to report security breaches to authorities, regardless of disclosure costs. In turn, authorities can disseminate knowledge to other firms. In this scenario, breach notification laws incentivize firms to conduct additional security investments. However, misadjustments of the security audit probability and sanction level can lead to over-regulation, which results in security over-investments of firms. If security audits and sanctions incentivize addressed firms to report security breaches, all of these firms internalize negative externalities.

In order to demonstrate the difficulty in adjusting the audit probability and the sanction level, consider the following scenario: assume that regulators imposes a sanction level equal to the direct costs of security breaches. Consequently, the optimal audit probability to incentivize security breach reporting depends on the disclosure costs of firms. If the disclosure costs, direct costs, and the sanction level are all equal, regulators have to introduce an audit probability of 50 % to enforce mandatory security breach reporting to authorities. The situation in Germany fits to examine the practical implications of this scenario. In 2012, the "Statistisches Bundesamt" recorded 80,000 german firms employing more than 50 people [34]. In the event that a security breach notification law affects all of these firms, more than 40,000 security audits are required – in a period to be defined – to incentivize their compliance. However, an introduction of more that 40,000 audits, or a considerable increase in the sanction level, ceteris paribus, results in over-regulation. A tradeoff between security audits and sanctions may be conceivable in order to enact a politically feasible security breach notification law. Regulators may, e. g., increase the level of sanctions to decrease the amount of security audits. But this harms firms which do not report security breaches because of benign nescience. Consequently, the enforcement of mandatory security breach reporting to authorities does not always result in social benefits.

Based on our devised model, laws that enforce mandatory security breach reporting to authorities are most reasonable in case of low disclosure costs associated with the compliance of firms, high security interdependence, and a low error rate of detective controls. Moreover, we observe that such laws are only justified under optimistic assumptions on the effectiveness of informed authorities in drawing conclusions from reported security breaches, and the dissemination of this knowledge to other firms in the economy. However, such assumptions lack empirical evidence, and further research is needed. Without this empirical evidence, legislative approaches stipulating security breach reporting to authorities are questionable.

5.2 Outlook

We presented a simple economic model, in which regulators introduce security audits and impose sanctions on firms to enforce mandatory security breach reporting to authorities. The proposed NIS-Directive [9] motivates this approach.

Our results call for reality checks on the adjustments of audit probabilities and sanction levels which effectively incentivize security breach reporting of firms. These reality checks may provide insights on the political feasibility of direct regulation in the context of security breach notification laws.

Moreover, different extensions of our model are conceivable. It is possible to interpret effective knowledge dissemination of authorities as a reduction in the attack probability on firms, rather than a reduction of interdependence between firms [29]. This could be modeled via an effect of information sharing on the economy-wide security productivity. Besides that, one could respect over-reporting of firms in the model, which has been identified in the context of other notification laws and can harm information quality. Furthermore, an analysis of endogenous investments in detective controls and security audits promises interesting results. Specifically, such an analysis would facilitate a theoretical comparison of welfare effects associated with security breach notification laws and the costs of supervisory programs introduced by governments.

With regard to future models on security breach notification laws, it is possible to incorporate government strategies that increase voluntary compliance and self-regulation of firms [38]. These models may, e. g., regard political instruments such as subsidies, liabilities, and taxes. One could utilize the currently discussed bills on cybersecurity in the US, providing for liability protection of firms that share information about security breaches with authorities, as a starting point for the construction of such models.

References

1. Acquisti, A., Friedman, A., Telang, R.: Is there a cost to privacy breaches? An event study. In: Proceedings of the International Conference on Information Systems (ICIS). Milwaukee (2006)
2. Anderson, R.: Security engineering: A guide to building dependable distributed systems. 2 edn. Wiley (2008)
3. Anderson, R., Böhme, R., Clayton, R., Moore, T.: Security economics and the internal market. Technical report, European Network and Information Security Agency (ENISA) (2008)
4. Böhme, R.: Security audits revisited. In Keromytis, A., ed.: Proceedings of the Financial Cryptography and Data Security (FC). Volume 7397 of Lecture Notes in Computer Science. Berlin, Heidelberg, Springer (2012) 129–147
5. Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. IJEC **9**(1) (2004) 70–104
6. Cavusoglu, H., Mishra, B., Raghunathan, S.: The value of intrusion detection systems in information technology security architecture. ISR **16**(1) (2005) 28–46
7. Dekker, D.M., Karsberg, C., Daskala, B.: Cyber incident reporting in the EU – An overview of security articles in EU legislation. Technical report, European Network and Information Security Agency (ENISA) (2012)
8. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM (2012) 11 final (2012)
9. 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)
10. Fischer-Hübner, S.: IT-Security and privacy. Springer, Berlin et al. (2001)
11. Gal-Or, E., Ghose, A.: The economic incentives for sharing security information. ISR **16**(2) (2005) 186–208
12. Gao, X., Zhong, W., Mei, S.: A game-theoretic analysis of information sharing and security investment for complementary firms. JORS **65**(11) (2013) 1682–1691
13. Gao, X., Zhong, W., Mei, S.: Security investment and information sharing under an alternative security breach probability function. Inf Syst Front (2013) 1–16
14. Gordon, L., Loeb, M.P.: The economics of information security investment. ACM TISSEC **5**(4) (2002) 438–457
15. Gordon, L., Loeb, M., Zhou, L.: The impact of information security breaches: Has there been a downward shift in costs? JCS **19**(1) (2011) 33–56
16. Gordon, L.a., Loeb, M.P., Lucyshyn, W.: Sharing information on computer systems security: An economic analysis. JAPP **22**(6) (2003) 461–485
17. Hausken, K.: Information sharing among firms and cyber attacks. JAPP **26**(6) (2007) 639–688
18. Hiller, J.S., Russell, R.S.: The challenge and imperative of private sector cybersecurity: An international comparison. CLSR **29**(3) (2013) 236–245
19. Khouzani, M., Pham, V., Cid, C.: Strategic discovery and sharing of vulnerabilities in competitive environments. In Poovendran, R., Saad, W., eds.: Decision and game theory for security. Volume 8840 of Lecture Notes in Computer Science. Berlin, Heidelberg, Springer (2014) 59–78
20. Khouzani, M., Pham, V., Cid, C.: Incentive engineering for outsourced computation in the face of collusion. In: Workshop on the Economics of Information Security (WEIS). Pennsylvania (2014)

21. Kunreuther, H., Heal, G.: Interdependent security. J Risk Uncertain **26**(2/3) (2003) 231–249
22. Laffont, J., Martimort, D.: The theory of incentives: The principal-agent model. Princeton University Press, Princeton (2002)
23. Lippmann, R., Haines, J., Fried, D., Korba, J., Das, K.: The 1999 DARPA off-line intrusion detection evaluation. Computer networks **34**(4) (2000) 579–595
24. Liu, D., Ji, Y., Mookerjee, V.: Knowledge sharing and investment decisions in information security. DSS **52**(1) (2011) 95–107
25. Macho-Stadler, I., Pérez-Castrillo, D. In: Principal-agent models. Volume 1. Springer, New York (2009) 6977–6990
26. Nalebuff, B., Scharfstein, D.: Testing in models of asymmetric information. The Review of Economic Studies **54**(2) (1987) 265–277
27. 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: 04.05.2015.
28. Ng, D., Stoeckenius, J.: Auditing: Incentives and truthful reporting. JAR **17**(1979) (1979) 1–24
29. Ogut, H., Memon, N., Raghunathan, S.: Cyber insurance and IT security investment: Impact of interdependent risk. In: Workshop on the Economics of Information Security (WEIS). Harvard (2005)
30. Romanosky, S., Telang, R., Acquisti, A.: Do data breach disclosure laws reduce identity theft? In Johnson, M.E., ed.: Proceedings of the Workshop on the Economics of Information Security (WEIS). Hanover, New Hampshire, Springer (2008)
31. Romanosky, S., Hoffman, D., Acquisti, A.: Empirical analysis of data breach litigation. In Böhme, R., ed.: Proceedings of the Workshop on Economics of Information Security (WEIS). Berlin, Springer (2012)
32. Romanosky, S., Sharp, R., Acquisti, A.: Data breaches and identity theft: When is mandatory disclosure optimal? In: Workshop on Economics of Information Security (WEIS). Harvard (2010)
33. Samuelson Law, Technology & Public Policy Clinic: Security breach notification laws: Views from chief security officers. Technical report, University of California-Berkeley School of Law (2007)
34. Statistisches Bundesamt: Statistisches Jahrbuch Deutschland und Internationales. Statistisches Bundesamt, Wiesbaden (2013)
35. Strobel, Warren: U.S. creates new agency to lead cyberthreat tracking (2015) Access: http://www.reuters.com/article/2015/02/10/us-cybersecurity-agency-idUSKBN0LE1EX20150210. Last accessed: 04.05.2015.
36. Symantec Corporation: Internet security threat report 2014. Technical report, Symantec Corporation (2014)
37. White House: Securing cyberspace – President Obama announces new cybersecurity legislative proposal and other cybersecurity efforts (2015) Access: http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat. Last accessed: 04.05.2015.
38. Winn, J.: Are 'better' security breach notification laws possible? BTLJ **24**(3) (2009) 1–33
39. Zhou, L.: The value of security audits, asymmetric information and market impacts of security breaches. PhD thesis, University of Maryland (2004)

A Symbols

Table 2: List of Symbols.

Symbol	Type	Meaning	Constraint
x	choice variable	security investment	$x \geq 0$
t	choice variable	probability of truthful reporting	$t \in [0,1]$
a	choice variable	audit probability	$a \in [0,1]$
S	choice variable	sanction level	$S \geq 0$
q_2	parameter	security breach disclosure costs	$q_2 \geq 0$
γ	parameter	security interdependence	$\gamma \in [0,1]$
ϵ	parameter	error rate of detective controls	$\epsilon \in]0,1]$
b	parameter	effectiveness of an authority	$b \in [0,1]$
n	constant	number of firms	$n = 2$
q_1	constant	direct costs of a security breach	$q_1 = 1$
β	constant	security productivity	$\beta = 20$
L	function	sum of security breach related costs	
η	function	reduction of interdependence	
P	function	security breach probability	
c	function	expected costs due to security issues	
B	random variable	security breach	
D	random variable	security breach detection	
A	random variable	security audit	
α	realization	realization of B	$\alpha \in \{0,1\}$
$\hat{\alpha}$	realization	realization of D	$\hat{\alpha} \in \{0,1\}$
$\tilde{\alpha}$	realization	choice on security breach reporting	$\tilde{\alpha} \in \{0,1\}$
ψ	realization	realization of A	$\psi \in \{0,1\}$

B Social Planner controls both, Security Breach Reporting and Security Investments (cf. Section 4.4)

The first derivates of Eq. (9), w. r. t. t and x, are

$$\frac{\partial c}{\partial x} = [\gamma \cdot \eta(t^*) \cdot (1 - P(x)) + (1 - \gamma \cdot \eta(t^*) \cdot P(x))] \cdot L(t^*, 0) \cdot P'(x) + 1 \quad (18)$$

$$\frac{\partial c}{\partial t} = (1 - \epsilon) \cdot P(x^*) \cdot ((1 - P(x^*)) \cdot (\gamma \cdot q_2 \cdot \eta(t) - b \cdot \gamma \cdot L(t)) + q_2). \quad (19)$$

B.1 Optimal Security Investment

The root of the first-order condition $\partial c / \partial x = 0$ is

$$x^*(t^*) = -\frac{\log\left(\frac{\gamma \cdot \eta(t^*)+1}{4 \cdot \gamma \cdot \eta(t^*)} - \sqrt{\frac{(\gamma \cdot \eta(t^*)+1)^2}{16 \cdot \gamma^2 \cdot \eta(t^*)^2} - \frac{1}{2 \cdot \gamma \cdot \log(\beta) \cdot \eta(t^*) \cdot L(t^*,0)}}\right)}{\log(\beta)}. \quad (20)$$

This expression corresponds to Eq. (10).

B.2 Optimal Security Breach Reporting and Proof of Proposition 1

Proof. The second derivate $\partial^2 c/\partial t^2$ is

$$\frac{\partial^2 c}{\partial t^2} = -2 \cdot b \cdot \gamma \cdot q_2 \cdot (1-\epsilon)^2 \cdot (1 - P(x^*)) \cdot P(x^*). \tag{21}$$

Based on Eq. (21), we observe that, for $b > 0$, $\gamma > 0$, $q_2 > 0$, $\epsilon > 0$ and any x^*, $\partial^2 c/\partial t^2 < 0$. Given these conditions, the cost function in Eq. (9) is concave in t, and $t^*(x^*) \in \{0, 1\}$ is a boundary value. □

C Agents control both, Security Breach Reporting and Security Investment (cf. Section 4.5)

The first derivates of Eq. (12), w. r. t. t_i and x_i, are

$$\frac{\partial c_i}{\partial x_i} = (1 - \gamma \cdot \eta(t_{1-i}) \cdot P(x_{1-i})) \cdot L_i(t_i, a) \cdot P'(x_i) + 1. \tag{22}$$

$$\frac{\partial c_i}{\partial t_i} = P_i(x_i, x_{1-i}, t_{1-i}) \cdot (1-\epsilon) \cdot (q_2 - a \cdot (q_2 + S)). \tag{23}$$

C.1 Security Investment

The root of the first-order condition $\partial c_i/\partial x_i = 0$, i. e., the best response of agent i, is

$$x_i^+(x_{1-i}, t_i, t_{1-i}, a) = \sup \left\{ -\frac{\log\left(\frac{1}{\log(\beta) \cdot L(t_i,a) \cdot \left(1-\gamma \cdot \eta(t_{1-i}) \cdot \beta^{-x_{1-i}}\right)}\right)}{\log(\beta)}, 0 \right\}. \tag{24}$$

The mutual best response $\tilde{x}(\tilde{t}, a) = x_i^+(\tilde{x}, \tilde{t}, \tilde{t}, a)$ leads to the Nash equilibria:

$$\tilde{x}_{1,2}(\tilde{t}, a) = -\frac{\log\left(\frac{1}{2 \cdot \gamma \cdot \eta(\tilde{t})} \pm \sqrt{\frac{1}{4 \cdot \gamma^2 \cdot \eta(\tilde{t})^2} - \frac{1}{\gamma \cdot \log(\beta) \cdot \eta(\tilde{t}) \cdot L(\tilde{t},a)}}\right)}{\log(\beta)} \tag{25}$$

$$\tilde{x}_3(\tilde{t}, a) = 0. \tag{26}$$

These equilibria correspond to Eq. (13) and Eq. (14). (Note that the constraint in Eq. (12) motivates the corner equilibrium $x_i^+(0, t_i, t_{1-i}, a) = 0$ in Eq. (26).)

C.2 Proof of Lemma 1

Proof. The existence of $\tilde{x}_{1,2}(\tilde{t}, a)$ depends on the discriminant in Eq. (25). In case of a negative discriminant, $\tilde{x}_3(\tilde{t}, a)$ is the only equilibrium. Moreover, note

that the equilibria $\tilde{x}_{1,3}(\tilde{t}, a)$ may only exist under the following conditions:

$$-\frac{\log\left(\frac{1}{2\cdot\gamma\cdot\eta(\tilde{t})}+\sqrt{\frac{1}{4\cdot\gamma^2\cdot\eta(\tilde{t})^2}-\frac{1}{\gamma\cdot\log(\beta)\cdot\eta(\tilde{t})\cdot L(\tilde{t},a)}}\right)}{\log(\beta)}\geq 0 \tag{27}$$

$$-\frac{\log\left(\frac{1}{\log(\beta)\cdot L(t_i,a)\cdot(1-\gamma\cdot\eta(t_{1-i})\cdot\beta^{-0})}\right)}{\log(\beta)}\leq 0. \tag{28}$$

Both conditions are fulfilled in case that, e. g.,

$$\gamma \geq \frac{\log(\beta)\cdot L(\tilde{t},a)-1}{\log(\beta)\cdot\eta(\tilde{t})\cdot L(\tilde{t},a)}. \tag{29}$$

Eq. (29) can also be solved for all other free model parameter and the audit probability: all free model parameter and the audit probability influence the existence of $\tilde{x}_{1,3}(\tilde{t}, a)$.

As a consequence of Eq. (27) and Eq. (28), $\tilde{x}_3(\tilde{t}, a)$ always exists simultaneously with $\tilde{x}_1(\tilde{t}, a)$, and $\tilde{x}_2(\tilde{t}, a)$ may exist alone. Observe from Eq. (25) that $\tilde{x}_1(\tilde{t}, a) \leq \tilde{x}_2(\tilde{t}, a)$. This leads to Lemma 1. □

C.3 Security Breach Reporting and Proof of Lemma 2

Proof. Based on the first derivative $\partial c_i/\partial t_i$, we observe that

$$\frac{\partial c_i}{\partial t_i} = \underbrace{P_i(x_i, x_{1-i}, t_{1-i})}_{>0}\cdot\underbrace{(1-\epsilon)\cdot(q_2 - a\cdot(q_2+S))}_{\text{depends on } a,\ S \text{ and } q_2}. \tag{30}$$

In case that $a = 0 \wedge q_2 > 0$, an agent does not have an incentive to report security breaches: $\partial c_i/\partial t_i > 0$. Consequently, we find that $\tilde{t}(\tilde{x}, 0) = 0$ is a Nash equilibrium. Otherwise, when $a = 0 \wedge q_2 = 0$, agents are indifferent to security breach reporting $\partial c_i/\partial t_i = 0$. In this case, marginal risk averse agents voluntarily report security breaches. A principal can incentivize agents to report security breaches with the introduction of audits $a > 0 \wedge q_2 > 0$, as these can lead to $\partial c_i/\partial t_i \leq 0$. In order to determine a principal's minimum audit probability $a = a_{min}$ to incentivize security breach reporting of marginal risk averse agents, we use the second part of Eq. (30):

$$0 = (1-\epsilon)\cdot(q_2 - a_{min}\cdot(q_2+S)) \Leftrightarrow a_{min} = \frac{q_2}{q_2+S}. \tag{31}$$

A principal can incentivize marginal risk averse agents to report breaches with the introduction of an audit probability $a \geq a_{min} = q_2/(q_2+S)$. Consequently, $\tilde{t}(\tilde{x}, a) = 1$ is a Nash equilibrium. This leads to the case distinction in Eq. (15) and Lemma 2. □

D Principal controls Audit Probability (cf. Section 4.5)

The first derivative of Eq. (16), w. r. t. a, is

$$\frac{\partial c}{\partial a} = 2 \cdot P_i(x_i, x_{1-i}, t_{1-i}) \cdot ((1 - t_i) \cdot (1 - \epsilon) \cdot (q_2 + S) + \epsilon \cdot (q_2 + S)). \quad (32)$$

D.1 Proof of Lemma 3

Proof. Given a positive sanction level $S > 0$, and disregarding the case where a marginal increase in audit probability has a positive net effect on social cost by inciting $t = 1$, we find that

$$\frac{\partial c}{\partial a} > 0. \quad (33)$$

This leads to Lemma 3. □

D.2 Proof of Lemma 4

Proof. In Appendix C.3, we derived the audit probability to incentivize reporting of agents $a_{min} = q_2/(q_2 + S)$. Based on Eq. (17), this may be the equilibrium audit probability. The first derivates of a_{min}, w. r. t. S and q_2, are

$$\frac{\partial a_{min}}{\partial S} = -\frac{q_2}{(q_2 + S)^2} \quad (34)$$

$$\frac{\partial a_{min}}{\partial q_2} = \frac{S}{(q_2 + S)^2}. \quad (35)$$

Given $q_2 > 0$ and $S > 0$, we find that $\partial a_{min}/\partial S < 0$ and $\partial a_{min}/\partial q_2 > 0$. This leads to Lemma 4. □