JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2(1), 2016, 29–41
doi: 10.1093/cybsec/tyw002
Advance Access Publication Date: 22 December 2016
Research paper

Research paper

The economics of mandatory security breach reporting to authorities

Stefan Laube[1,*] and Rainer Böhme[2]

[1]Department of Information Systems, Westfälische Wilhelms-Universität Münster, Leonardo-Campus 3, 48149 Münster, Germany and

[2]Department of Computer Science, Universität Innsbruck, Technikerstraße 21A, 6020 Innsbruck, Austria

*Corresponding author: E-mail: Stefan.Laube@uni-muenster.de

Received 17 September 2015; revised 10 July 2016; accepted 21 July 2016

Abstract

Legislators in many countries enact security breach notification regulation to address a lack of information security. The laws designate authorities to collect breach reports and advise firms. We devise a principal–agent model to analyze the economic effect of mandatory security breach reporting to authorities. The model assumes that firms (agents) have few incentives to unilaterally report breaches. To enforce the law, regulators (principals) can introduce security audits and sanction noncompliance. However, audits cannot differentiate between concealment and nescience of the agents. Even under optimistic assumptions regarding the effectiveness of mandatory security breach reporting to authorities in reducing individual losses, our model predicts that it may be difficult to adjust the sanction level such that breach notification laws generate social benefit.

Motivation

Confidentiality, integrity, and availability are the canonical protection goals for information systems. Security breaches are violations of at least one of these protection goals [1]. They may concern data protection or security [2]. In the past years, the intensity of attacks against information systems and the number of observed security breaches has increased, causing high costs for firms [3].

Firms incur two types of costs due to security breaches: direct and indirect. Direct costs are, e.g., the costs of cleaning systems from malware. Indirect costs include intangible costs, which materialize, for instance, in reputation loss if security breaches are publicly announced. Quantifying, in particular, the indirect costs of security breaches is hard. One approach suggested by Cavusoglu *et al.* [4], among others, is to analyze the impact of breach publications on the stock market value of breached firms. Firms in their sample lost (on average) 2.1% of their market value within the first 2 days after a breach announcement. (Cavusoglu *et al.* [4] also find cross-sectional variations in indirect costs of firms and explain them by firms' size, type, and the year in which the breach occurred.) The authors attribute this negative effect to shareholders' anticipation of losses of confidence and trust by customers. They argue that when security breaches 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. Interdependence between information systems allows breaches to propagate and negatively affect others [5]. In the language of economics, a lack of firms' information security causes negative externalities in an economy. The presence of negative externalities justifies government intervention, for instance, in the form of laws aiming at reducing the costs of insecurity to society [6, 7].

One specific approach is the introduction of security breach notification laws. Such laws differ in their design, as

1. they may oblige firms to report security breaches to affected individuals, via direct or mass communication (implemented in several US states [8]), or
2. they may oblige firms to report security breaches to authorities (implemented for firms of selected sectors in the EU [9]).

In essence, breach notification laws try to establish some transparency on breaches such that firms or individuals are able to protect themselves from propagating attacks. Furthermore, they shall incentivize effective investment in information security. But as breach reporting and security investments are costly [10], the effectivity of these laws in decreasing the costs to society has to be analyzed. We are aware of empirical work on the economic effects of

Table 1. Characteristics of selected US and EU breach notification laws

Region	Law	Obliged	Report	Address	Objective	Effect
USA	State laws	Firms controlling personal data	P	I or A&I	IP&R	C or F&C
USA	HIPAA & HITECH	Firms in the health care sector	P	A&I	IP&R	F&C
USA	GLBA	Firms in the financial sector	P	I or A&I	IP&R	F&C
EU	Telecoms package	Firms in the telecoms sector	S or P	A or A&I	IP&D or IP&D&R	F or F&C
EU	Regulation 2016/679	Data controllers and processors	P	A or A&I	IP&D or IP&D&R	F or F&C
EU	NIS Directive[a]	Market operators	S&P	A	IP&D or IP&D&R	F or F&C

S, Security breaches; P, Privacy breaches; A, Authorities; I, Affected individuals; IP, Incentivize firms to take precautions; D, Dissemination of knowledge to firms; R, Improve rights of affected individuals; F, Fines; C, Indirect costs.

[a] Proposed, not yet enacted.

obliging firms to report security breaches to individuals (e.g., [11, 12, 13, 14]), and also find a theoretical model which examines this scenario [15]. Moreover, several scholars analyze the economic incentives for voluntary security information sharing between firms (e.g., [16, 10, 17]). And two studies discuss the effects of security information sharing between firms and authorities [18, 19]. However, we observe a lack of scientific investigations on the conditions under which mandatory security breach reporting to authorities is effective in reducing social cost. 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 breached firms.

This article is structured as follows: Section "Background and research question" provides a qualitative introduction to the research topic and motivates our research question. Section "Related work" discusses relations to prior art. We describe our principal–agent model and present solutions for social optima and Nash equilibria in Section "Model." The last section concludes with a discussion and an outlook for future research.

Background and research question

Security breach notification laws are on the policy agenda around the globe for over a decade. Section "Security breach notification laws" introduces selected laws implemented or discussed in the USA and EU along with inherent mechanisms that are expected to incentivize firms' compliance. In Section "Incentives of firms," we discuss how a particular mechanism can alter incentives of firms to reduce breach related costs. Our research question proposed in Section "Research question" concerns the effectiveness of laws that make use of this mechanism.

Security breach notification laws

Table 1 summarizes key characteristics of selected breach notification laws. All of these laws lead to additional expected cost for breached firms. Firms can reduce these costs if they prevent breaches *a priori*, and thereby evade breach reporting. From a review of legal texts and official justifications we conclude that this is in fact an important objective of breach notification laws in the USA and EU besides improving the rights of the individuals affected by a breach.

Situation in the USA

State and federal laws mandate firms to notify affected individuals about breaches. The first implemented state breach notification law was the California Civil Code Section §1798.29. It obliges private and public firms conducting business in California to report privacy breaches to affected individuals. Additionally, the law stipulates breach reporting to authorities if more than 500 data records are affected. The intention of this law is 2-fold: first, informing individuals about breaches enables them to take mitigating actions [15]; second, the law incentivizes firms to encrypt personal data, as only breaches of unencrypted records have to be reported. From the start, the Californian law led to a high number of privacy breach reports [12]. Because of this success, other US states enacted similar laws [8]. Besides these state laws, there are two prominent federal breach notification laws. They are formalized in the "Health Insurance Portability and Accountability Act" (HIPAA)—amended by the "Health Information Technology for Economic and Clinical Health Act" (HITECH)—and the "Gramm–Leach–Bliley Act" (GLBA), respectively. The HIPAA mandates firms in the health care sector to report breaches of health information to affected individuals, the Department of Health & Human Services, and under some circumstances the media. The GLBA differs from the HIPAA in that it obliges firms in the financial sector to inform their primary federal regulator on privacy breaches, and in some cases notify affected individuals. In summary, some state and federal breach notification laws stipulate privacy breach reporting to individuals only, while others additionally require firms to inform authorities. In order to incentivize firms' compliance, most of the laws provide for fines in cases of violations.

The 114th Congress has introduced new federal legislation on security information sharing. The House of Representatives (H.R.) proposed "H.R.1770 – Data Security and Breach Notification Act of 2015," which intends to replace the existing patchwork of state laws. Furthermore, US President Barack Obama submitted an "Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing" with the objective to improve security information sharing within the private sector and between the private sector and the government. The order shall pave the way for new legislation on security information sharing, formalized in different bills: the H.R. introduced "H.R.234 – Cyber Intelligence Sharing and Protection Act," and passed "H.R.1560 – Protecting Cyber Networks Act" in the Congress; Senate submitted "S.456 – Cyber Threat Sharing Act of 2015," and passed "S.754 – Cybersecurity Information Sharing Act." Most of this legislation limits firms' liability if they not only share security information with each other, but also with an authority, e.g., the Department of Homeland Security (DHS).

Situation in the EU

Union laws (i.e., regulations and directives) and national laws of EU Member States mandate firms to report breaches. All Member States have to transpose directives into national law. Union laws in the form of regulations are directly binding. Enforced union laws that mandate breach reporting predominantly affect the telecoms sector. Most of them were introduced with the "Telecoms Package" in 2009. A prominent example is Directive 2009/136/EC, amending

Directive 2002/58/EC. It has the objective to protect the privacy of users' data handled by electronic communications service providers. The directive obliges providers to report breach information to authorities and, under specific circumstances, also notify affected individuals. All of the enforced union breach notification laws that we reviewed require firms to report breaches to "Competent Authorities" in the first instance, rather than affected individuals—as it is common in US laws. The declared objective is to establish union-wide transparency on breaches [9]: informed authorities can disseminate conclusions drawn from breach information (subsequently referred to as "dissemination of knowledge"). For instance, they can offer guidance to breached firms and individuals on how to minimize impact, or inform non-breached firms and individuals on how to protect against propagating attacks. In addition to union law, some EU Member States have enacted national security breach notification laws. A non-exhaustive list of these laws is reported in [20]. Our review indicates that almost all union and national breach notification laws use fines as an incentive mechanism to ensure firms' compliance.

Two complementary legislative proposals intend to expand existing union breach notification laws in the future:

- Regulation (EU) 2016/679. This regulation is referred to as the "General Data Protection Regulation" (GDPR), and aims to harmonize and unify existing EU privacy breach reporting obligations. It requires "data controllers and processors" in the EU to report privacy breaches to authorities. (The GDPR will also apply to firms based outside the EU who process personal data of Europeans.) The authorities may then inform affected individuals, e.g., when a breach is likely to violate rights and freedoms. Regulation (EU) 2016/679 entered into force in May 2016, and repeals the data protection Directive 95/46/EC in May 2018.
- Proposal COM/2013/048 final [21]. The proposed directive is referred to as the "Network and Information Security Directive" (NIS Directive). Its declared objective is to establish a high level of information security in the EU. Selected "market operators" will have to report breaches to authorities only. (In the context of the NIS Directive, we use "firms" as shorthand for the legal term "market operators") The NIS Directive is expected to enter into force in the course of 2016.

In the tradition of other union breach notification laws, both the GDPR and the proposed NIS Directive provide for fines to ensure firms' compliance.

Possibilities to enhance compliance

Breach notification laws in the USA and the EU all pose enforcement challenges as regulators must verify if firms comply. The threat of fines may incentivize some firms. But others, who expect higher costs, e.g., because of reported breaches becoming public, will rather refrain from reporting and speculate that their concealment remains undetected. Thus, the laws' objectives may fail without mechanism verifying compliance.

In order to incentivize firms' compliance, some form of direct regulation may be necessary. Winn [22] analyzes US state notification laws and argues that these laws are likely ineffective, as they do not directly regulate how compliance is verified. The EU laws also suffer from this issue, but national implementations of the NIS Directive may change the situation. This Directive mentions security audits that can be used to check whether firms' reporting obligations to authorities have been fulfilled. Yet, many practical questions remain open. Our working hypothesis is that firms undergo spontaneous security audits, initiated by regulators. If unreported breaches are discovered during these audits, sanctions are imposed. The prospect of sanctions can incentivize firms to report breaches, which entails indirect costs as authorities may publish corresponding information. In order to reduce expected sanctions and indirect costs, firms can increase their investments into security. Thus, direct regulation may change firms' incentives.

Incentives of firms

In a situation without breach notification laws, the expected impact of security breaches establishes incentives for firms to invest in internal control mechanisms and to share security information with each other [10]. Cavusoglu *et al.* [23] distinguish between two categories of control 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. But preventive controls are no panacea. Thus, many firms complement them with detective controls, trying to detect breaches that already happened. For instance, firms can make use of intrusion detection systems (IDS). However, such systems can result in type I errors (alerts, even though there are no breaches) and type II errors (absence of alerts, even though there are breaches). In order to reduce the probability of these errors, and leverage security investments in general, firms can share security information with each other [24]. This includes information on how to prevent or detect breaches, and methods to minimize their impact [16]. Platforms for information sharing are provided by "Security Based Information Sharing Organizations" (SB/ISOs), e.g., "Computer Emergency Response Teams" (CERTs) or "Information Sharing Analysis Centers" (ISACs).

Laws similar to the NIS Directive [21], which has the prospect to enforce mandatory security breach reporting to authorities by means of direct regulation, affect these incentives of firms:

- They can incentivize firms to report breaches to authorities even though reporting entails "disclosure costs," i.e., expenses emerging from bureaucratic burdens and indirect costs due to authorities' publication of obtained information. This is because non-reported breaches may lead to sanctions in the event of audits.
- They can incentivize firms to increase investments in controls. The reason is that investment in security reduces the number of breaches at firms, and therefore reporting obligations. Furthermore, remaining breaches have to get detected before they can be reported, requiring detective controls.
- They can incentivize firms to abstain from investments in controls. The rationale is that informed authorities' advise can be utilized by firms to leverage investments. Thus, optimal security levels may be reached at lower costs [16].

Overall, the enforcement of laws mandating breach reporting to authorities may incentivize firms to internalize negative externalities of their insecurity. Specifically, they can incentivize firms to enhance their security levels, leading to a reduction of breach probabilities in the economy. Thus, less breaches propagate and negatively affect others. However, this internalization of negative externalities may be accompanied by substantial security investment costs and sanctions at firms.

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.

Research question

The objectives of the NIS Directive [21] motivate our research question:

Mandatory security breach reporting to authorities (cf. Section "Security breach notification laws"), enforced with audits and sanctions, may change the incentives of firms to invest in security and share breach information (cf. Section "Incentives of firms"). Under what circumstances does this change lead to (i) a higher overall level of information security, and (ii) lower social costs?

The response to this question is relevant for firms who decide on security investments and breach reporting. Moreover, it is relevant for regulators enforcing security breach notification laws by means of security audits and sanctions.

In this article, we devise and analyze a principal–agent model to answer our research question. The model includes parameters for the following properties: interdependence of information security (cf. Section "Motivation"), an informed authority's effectiveness in dissemination of knowledge to firms (cf. Section "Security breach notification laws"), and disclosure costs (cf. Section "Incentives of firms").

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 "Effectiveness of audits in principal–agent setups"), and papers on the economics of security information sharing. The second stream of literature can be further divided in papers that discuss the economic incentives for

- voluntary information sharing between firms (cf. Section "Voluntary information sharing between firms");
- mandatory information sharing between firms and individuals (cf. Section "Mandatory information sharing between firms and individuals");
- mandatory information sharing between firms and authorities (cf. Section "Mandatory information sharing between firms and authorities").

Effectiveness of audits in principal–agent setups

Ng and Stoeckenius [25] were among the first to analyze the effectiveness of audits in solving a principal–agent problem. They identify a moral hazard problem in the reporting of performance from the management (agent) to the owner (principal) of a firm, and discuss how audits can incentivize the agent to comply with reporting obligations. Their seminal work from 1979 has triggered a lot of research on principal–agent problems with moral hazard and adverse selection (e.g., [26, 27]). Much of this research has in common that audits are contractually agreed upon [28].

In contrast to this literature, we analyze the design of legislation which includes audits and sanctions to establish incentives for an agent to comply.

Voluntary information sharing between firms

There is substantial work on voluntary information sharing between firms. All of the papers discussed in the following assume security information sharing to be conducted in SB/ISOs. Moreover, most of the papers use a model with two interdependent firms [5] representing an economy. Both firms can invest in information security, decreasing the probability of breaches to their information systems. To capture security investment decisions of firms, authors usually base their models on the assumptions of Gordon and Loeb [29].

Gordon *et al.* [16] evaluate the effects of security investment and security information sharing on firms' costs due to security breaches. They argue that information sharing between firms has a leverage effect on security investments. Their findings indicate that investment and sharing can act as strategic substitutes in decreasing breach-related costs. By contrast, Gal-Or and Ghose [10] analyze the effects of firms' investments and security information sharing on customers' demand for products. According to them, a firm's publication of security investment decisions or participation in a sharing arrangement, e.g., an ISAC, both establish confidence with customers that security efforts are successful. This is interpreted as a positive effect on the demand of this firm's products. Additionally, private security information sharing between firms leverages their security investments. However, if information that is shared between firms leaks, this can result in indirect costs. The authors' results indicate that if sharing has large positive implications on product demand, firms naturally share security information. They observe that investment and information sharing may act as strategic complements. Hausken [17] proposes a model of information sharing between firms similar to the authors of [16, 10]. He argues that in the presence of strategic attackers, firms' sharing can have positive or negative effects on their profits—depending on prevailing interdependence. His analysis reveals that firms' information sharing increases with their interdependence, and is zero in case of no or negative interdependence. Liu *et al.* [24] argue that firms' logical interdependence plays a key role for their investment and information sharing decisions. They find that if firms possess complementary assets, i.e., assets that have to get combined in order to provide value to an attacker, sharing incentives exist. By contrast, if firms possess substitutable assets, they do not share. Either way, investment decisions are suboptimal in case that the firms do not coordinate their choices.

The authors of [30, 31] propose models on security information sharing that differ from those introduced before. Khouzani *et al.* [30] analyze two firms' incentives to invest in the discovery of vulnerabilities to their (homogenous) information systems, and to share vulnerability information. Both firms operate on the same market, and private knowledge about vulnerabilities has a positive effect on each firm's own utility. Though, under the assumption that breaches result in loss of customers' confidence and trust in industries, vulnerability exploitation at any firm leads to overall market shrinkage. The authors find that firms are willing to share vulnerability information if the loss from market shrinkage exceeds individual gains from private information on vulnerabilities—and vice versa. In extension to all previously introduced works, Naghizadeh and Liu [31] propose a model to analyze incentives for information sharing considering repeated interactions of two firms. Thereby, each firm's sharing improves the other's payoff, and is associated with disclosure costs. The authors show that if both firms interact only once, they abstain from sharing even though this could improve their payoffs. By contrast, if firms repeatedly interact, they are able to condition future sharing decisions on past interactions. This can enable firms to coordinate sharing decisions, and improve their payoffs.

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

Mandatory information sharing between firms and individuals

Considerably less theoretical work addresses mandatory information sharing between firms and individuals, although there are corresponding breach notification laws in several US states [8]. Romanosky *et al.* [15] are the first—and to our knowledge only—ones to analyze this research topic using an economic model. They argue that breach publication to affected individuals leads to two types of costs for firms. First, firms have to expect some disclosure tax, e.g., regulatory fines and indirect costs. Second, firms bear some losses from individuals. Specifically, they can get held liable for harm resulting from breaches, e.g., because of individuals' class action lawsuits. The authors' analysis reveals that even though firms are affected by both types of costs, mandatory sharing between firms and individuals can be socially beneficial. This is because it establishes incentives for firms to increase investments, reducing the probability of security breaches, and enables individuals to take care. However, some political instruments may be necessary for regulators to optimally reduce the overall social costs.

Our model in this article does not stand in the tradition of the work by Romanosky *et al.* [15] as we do not consider individuals' actions, though we also respect that firms fear the costs associated with breach publication. In fact, some firms even try to offset these costs by the release of positive news simultaneous to a breach publication [32].

Mandatory information sharing between firms and authorities

Öğüt *et al.* [18] are the first to discuss the economics of security information sharing between firms and authorities. However, they do not analyze mandatory 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 reduces firms' investment incentives. This leads to overall suboptimal security levels. Breach information sharing between firms and an authority may oppose the effect of security interdependence. The reason is that an informed authority can draw conclusions from reported breaches, and disseminate knowledge on derived countermeasures. This information may then be used by firms to lower their breach probabilities. In turn, this results in a reduction of the number of breach propagations in an economy, and therefore interdependence. Thus, the authors conclude that information sharing between firms and authorities can result in positive welfare effects.

In previous work [19], we analyze the implications of firms' mandatory security information sharing with authorities on their investments in internal controls. The proposed model assumes that information sharing leverages controls. However, firms do not share information voluntarily because of associated disclosure costs. Thus, a regulator considers to enforce sharing by the introduction of an incentive mechanism. The analysis reveals that if a weak incentive mechanism is introduced by the regulator to enforce sharing, this incentivizes firms to prioritize investments in preventive rather than detective controls. In this situation, positive welfare implications are conceivable due to the sharing's leverage effect on security investments. In contrast, a strong incentive mechanism reverses firms' priorities, and can lead to economy-wide security over-investments. These over-investments may negatively affect welfare as they are associated with substantial costs at firms. Though, the analysis does not provide for parameter settings in which regulators should abstain from enforcement because of these costs.

In what follows, we will devise a principal–agent model that can be used to evaluate parameter settings where the enforcement of firms' security breach reporting to authorities is socially beneficial. This model is primarily inspired by the theoretical literature on voluntary information sharing between firms. It comprises two firms that represent an economy. Both are affected by attacks on their information systems. A firm's security investment can reduce the number of successful attacks, i.e., breaches, according to the assumptions in [29]. However, the firm's breach probability is also affected by the other firm's investment, because security is interdependent [5]. Consequently, security underinvestment of one firm leads to negative externalities on the other. In order to reduce negative externalities, firms can share information on detected security breaches with each other [18]. But privately shared information may leak and thus result in disclosure costs, as argued by the authors of [10]. Therefore, both firms base their sharing decision on a cost–benefit tradeoff, and it is conceivable that they abstain from sharing altogether. Regulators can counter a lack of sharing incentives by enforcing a law mandating firms to report breaches to an authority [21]. Thereby, a conflict arises that can be interpreted as a principal–agent problem with moral hazard [28]: the regulator (principal) cannot be sure that firms (agents) comply with the law. Thus, he requires security audits to detect and sanction unreported breaches at agents. However, agents can only comply with reporting obligations if they detect breaches. And as audits cannot differentiate between nescience and concealment of breaches, it may be difficult for the principal to decide on the security audit probability and sanction level enforcing the law.

Model

Our principal–agent model consists of three different components: a model for security investment and firms' interdependence, a formalization of mandatory security breach reporting to an authority, and a formalization of security audits. These components will be described in Sections "Security investment and interdependence," "Detective controls and security breach notification laws," and "Disclosure costs and security audits," respectively. Each component includes one of the free parameters specified in Section "Research question." We will study the model's social optima in Section "Social optima" and its Nash equilibria in Section "Nash equilibria." Table A1 summarizes all symbols used.

Security investment and interdependence

Consider for now a single rational firm belonging to a larger economy. This firm has a choice on investment in information security $x \geq 0$, which can decrease the probability P of security breaches to its information system. We model realizations of the random variable B (breach) as $\alpha \in \{0,1\}$, and follow Gordon and Loeb [29] by characterizing the relationship between breach probability and investment as $Pr(\alpha=1)=P(x)$. With an increase in investment x, the probability of a security breach decreases $\partial P/\partial x < 0$, but at a decreasing rate $\partial^2 P/\partial x^2 > 0$, i.e., $\lim_{x\to\infty} P(x) \to 0$. According to Böhme [33], 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 fix the direct costs of a security breach on $q_1 = 1$ to normalize the monetary scale. Overall, the firm's expected costs due to security issues are given by

$$c(x) = P(x) \cdot q_1 + x\,. \quad (1)$$

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.* [18], who introduce a parameter for security interdependence $\gamma \in [0, 1]$ between two firms, we can express the security breach probability at firm i as

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

The intuition of Equation (2) is that firm i can only evade a loss if itself does not get breached and no breach propagates from firm $1 - i$ due to interdependence. Without interdependence, i.e., $\gamma = 0$, we find that the security breach probability is $Pr(\alpha_{\mathrm{i}}{=}1){=}\ P_i(x_i, x_{1-i}) = P(x_i)$.

Detective controls and security breach notification laws

We acknowledge that both firms have a self-interest in detecting security breaches and denote the realization of the random variable D (security breach detected) as $\hat{\alpha}_i \in \{0, 1\}$. The success probability of detecting a breach is given by $Pr(\hat{\alpha}_i = 1 | \alpha_i = 1) = 1 - \epsilon$, where ϵ is 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. As a further simplification, we consider that the type I error rate of IDS is 0%. A study of Lippmann *et al.* [34] shows that the best IDS detect about 80% of attacks that have happened. Thus, we subsequently (optimistically) fix the type II error rate at $\epsilon = 20\,\%$.

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. Therefore, compliance with reporting obligations is $Pr(\tilde{\alpha}_i = 1 | \hat{\alpha}_i = 1) = t_i$. For the sake of simplicity, we assume that nobody has an interest in reporting incidents that did not happen.

If a firm reports security breach information, the authority can draw conclusions from the breach and advise other firms with the objective of decreasing social costs. We denote the parameter for an informed authority's effectiveness in dissemination of knowledge to firms by $b \in [0, 1]$. According to Öğüt *et al.* [18], the positive effect from such dissemination can be interpreted as an enhancement in firms' efficiency of security investments or a reduction of their security interdependence. Note that if all firms in an economy invest into security, an economy-wide increase in security productivity reduces breach probabilities, and thus interdependence, *ceteris paribus*. Subsequently, we assume that an authority's dissemination of knowledge can reduce interdependence according to

$$\eta(t) = 1 - b \cdot (1 - \epsilon) \cdot t \,, \text{ such that} \tag{3}$$

$$P_i(x_i, x_{1-i}, t_{1-i}) = 1 - (1 - P(x_i)) \cdot (1 - \gamma \cdot \eta(t_{1-i}) \cdot P(x_{1-i})) \,. \tag{4}$$

The function in Equation (3) is bound to the interval $0 \le \eta(t) \le 1$. Furthermore, it monotonically decreasing in the effectiveness of an authority and firms' compliance, i.e., $\partial\eta/\partial b < 0$ and $\partial\eta/\partial t < 0$. According to Equation (4), this reflects the intuition that information sharing with an effective authority reduces security interdependence, given that disseminated knowledge is effectively used by firms.

Furthermore, observe from Equation (4) 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. Though, truthful reporting entails disclosure costs.

Disclosure costs and security audits

If regulators pass breach notification laws, firms do not only consider the direct costs of security breaches, but also disclosure costs associated with breach reporting. Disclosure costs may arise, e.g., because of bureaucratic burdens or an authority's breach publication. Let $q_2 \in [0, \infty[$ denote the parameter for a firm's disclosure costs. As truthful reporting t_i inevitably leads to these costs, a firm's sum of breach related costs are given by

$$L_i(t_i) = (1 - \epsilon) \cdot t_i \cdot q_2 + q_1, \text{ such that} \tag{5}$$

$$c_i(x_i, x_{1-i}, t_i, t_{1-i}) = P_i(x_i, x_{1-i}, t_{1-i}) \cdot L_i(t_i) + x_i \,. \tag{6}$$

Disclosure costs lead to a conflict of interest between firms and regulators, hereinafter interpreted as a principal–agent problem with moral hazard. A regulator (principal) introduces a security breach notification law. But firms (agents) may only have few incentives to unilaterally report detected breaches because of disclosure costs. We assume that agents only report breaches if this does not make them worse off than concealing them. (Thus, agents which are indifferent to compliance with the law act law-abiding. In economic terms, one could consider such agents as "marginal risk averse.") To overcome a potentially evolving moral hazard problem where agents do not comply with the law, the principal can introduce audits and imposes sanctions for non-reported breaches.

We model realizations of the random variable A (security audit) as $\psi \in \{0, 1\}$. The principal abstains from audits if a breach is reported by an agent, i.e., $Pr(\psi = 1 | \tilde{\alpha}_i = 1) = 0$. Otherwise, he conducts security audits with probability $Pr(\psi = 1 | \tilde{\alpha}_i = 0) = a$. We assume that every realized audit detects every security breach that has happened with certainty, i.e., audits are more reliable than detective controls per definition. For the sake of simplicity, we do not model the costs associated with security audits. Rather, we assume that sanctions collected from noncomplying agents fully compensate these costs.

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. Then, an attack on his information system takes place. This attack results in a breach with probability $P_i(x_i, x_{1-i}, t_{1-i})$. We assume that, per period under consideration, there can at most be one security breach to an agent's information system. After a security breach has happened, the agent detects it with probability $Pr(\hat{\alpha}_i = 1 | \alpha_i = 1) = 1 - \epsilon$. If the agent does not detect the breach, he will not report it to the authority. Otherwise, he can strategically choose whether he commits to reporting or not. In cases where the agent does not report a breach, the principal conducts audits at random. If the principal detects an unreported breach, the agent is penalized with sanctions $S \in [0, \infty[$. Additionally, the agent has to expect disclosure costs q_2 as the principal can publish the detected breach.

From Fig. 1, we can derive the expected costs due to security issues of agent i if mandatory security breach reporting to an authority is enforced, i.e.,

$$\begin{aligned} c_i(x_i, x_{1-i}, t_i, t_{1-i}, a) &= P_i(x_i, x_{1-i}, t_{1-i}) \cdot L_i(t_i, a) + x_i \,, \text{ with} \\ L_i(t_i, a) &= (1 - \epsilon) \cdot [t_i \cdot q_2 + (1 - t_i) \cdot a \cdot (q_2 + S)] \\ &\quad + \epsilon \cdot a \cdot (q_2 + S) + q_1 \,. \end{aligned} \tag{7}$$

Observe from Equation (8) that if the principal introduces infinitely high sanctions, and given a positive audit probability, agents always have incentives to report detected security breaches. Yet, agents cannot find any breach that has to be reported because of the

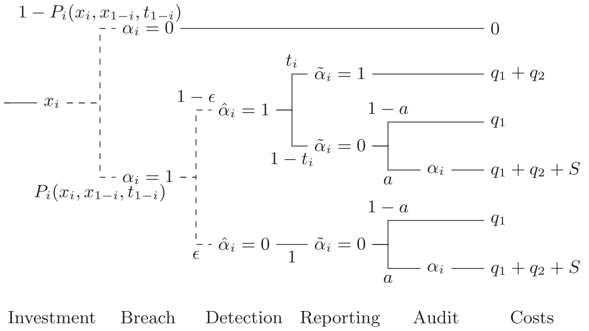

Figure 1. Decisions of agent *i*, nature, and the principal.

error probability of detective controls. Thus, they will be burdened with sanctions eventually. In practice, unreasonably high sanctions are uncollectible, as they lead to agents' bankruptcy. This renders an incentive mechanism with infinitely high sanctions infeasible, as also acknowledged by Khouzani *et al.* [35]. We are interested in evaluating practically feasible incentive mechanism, and therefore 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 principal's decision on the audit probability is his only choice variable.

Social optima

Social costs are defined as the sum of all agents' expected costs. A social planner with control over agents' investments, breach reporting, and a principal's audits, has a minimization problem based on the agents' costs in Equation (7), i.e.,

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

Observe from this equation that the social planner does not require audits. This is because investments and truthful reporting do not have to get stimulated, but are in control of the planner. Furthermore, we may substitute x_i by x and t_i by t because of agents' symmetry. The solution to the problem in Equation (9), derived in Appendix 2, consists of extreme and boundary values.

The social planner's optimal security investment is

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

Lemma 1. If $b > 0$, $\gamma > 0$, $q_2 > 0$, $\epsilon > 0$ and for any x^*, a reporting strategy $0 < t < 1$ is not socially optimal. Under these conditions, the socially optimal reporting strategy is a boundary value, i.e., $t^*(x^*) \in \{0, 1\}$.

The proof is in Appendix 2.2.

A social planner will either introduce full reporting of all detected security breaches, or abstain from reporting altogether. Consequently, optimal security breach reporting is

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

This case distinction can be interpreted as the implementation of a security breach notification law under the assumption of fully complying agents.

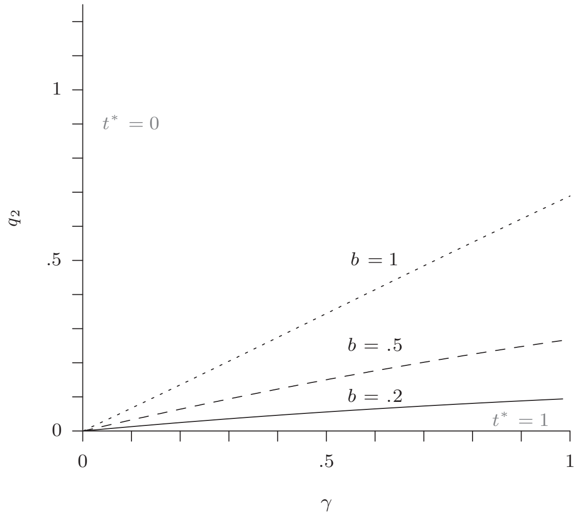

Figure 2. Social planner's case distinction in (γ, *b*, q_2)-parameter space.

Proposition 1. If $c(x^*(0), x^*(0), 0, 0, 0) > c(x^*(1), x^*(1), 1, 1, 0)$, the social planner introduces breach reporting, and the social optimum is $(t^* = 1, x^*(1))$. Otherwise, the social optimum is $(t^* = 0, x^*(0))$.

Proof. Follows from Lemma 1 and Equation (11).

Figure 2 illustrates regions for social optima depending on different situations in the (γ, b, q_2)-parameter space. The three lines each starting in the origin of the coordinate system indicate a social planner's indifference in security breach reporting, following from Equation (11), for three different types of an authority's effectiveness b. On and above the lines, the social optimum is $(t^* = 0, x^*(0))$. In the region below each line, breaches get reported, i.e., the social optimum is $(t^* = 1, x^*(1))$. Observe that the region below a line is larger for a more effective authority. This leads to the conclusion that the introduction of breach reporting to a large extend depends on an authority's effectiveness.

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 [36], Nash equilibria of a principal–agent game with moral hazard can be derived by the following steps: (i) determination of the Nash equilibria between agents, disregarding the best response of the principal, and (ii) backwards induction to determine the principal's best response.

Agents

If a security breach notification law is implemented, agents simultaneously and independently decide on security investments and breach reporting with the objective to minimize their expected costs specified in Equation (7), i.e.,

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

Solving the problem in Equation (12) results in the best response of agent i, given decisions of agent $1 - i$. Nash equilibria follow

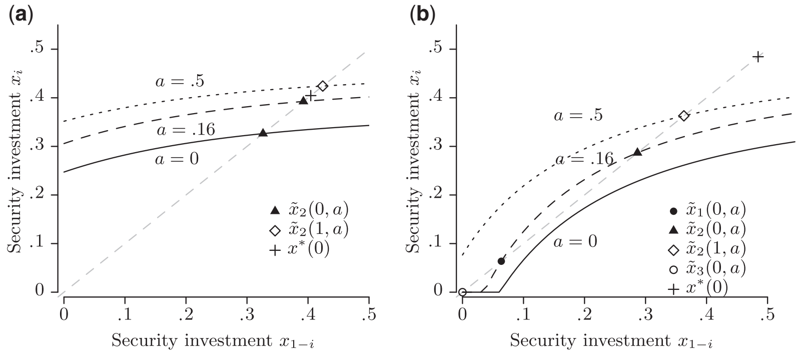

Figure 3. Best response in security investment and breach reporting of agent i, given decisions of agent $1 - i$ and the principal's audit probability (a) Best response of agent i ($\gamma = 0.3$); (b) Best response of agent i ($\gamma = 0.8$). Nash equilibria and social optima are depicted on the angle bisector (Common assumptions: $b = .2, q_2 = .2, S = 1$, leading to an equilibirum audit probability of $a_{\min} = .166$).

from the mutual best response of the two symmetric agents. The derivation of these equilibria is proposed in Appendix 3.

Depending on the parameter setting, up to three equilibria can exist simultaneously. These equilibria imply the security investments

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

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

Lemma 2. If the equilibrium implying $\tilde{x}_1(\tilde{t},a)$ exists, then two other equilibria that contain the investments $\tilde{x}_{2,3}(\tilde{t},a)$ exist simultaneously, where $\tilde{x}_3(\tilde{t},a) = 0 \leq \tilde{x}_1(\tilde{t},a) \leq \tilde{x}_2(\tilde{t},a)$. Moreover, there are settings where only the equilibrium with investment $\tilde{x}_2(\tilde{t},a)$ or $\tilde{x}_3(\tilde{t},a) = 0$ persist.

The proof is in Appendix 3.2.

Three categories of model parameter settings have to be distinguished, each resulting in equilibria implying different security investments. These categories can, for instance, be illustrated based on security interdependence between agents, *ceteris paribus*. If interdependence is low, only an equilibrium where agents choose to extensively invest in security $\tilde{x}_2(\tilde{t},a)$ exists. With moderate security interdependence, two additional equilibria implying the investment strategies $\tilde{x}_{1,3}(\tilde{t},a)$ evolve. If there is high interdependence, only the equilibrium where agents abstain from any investment $\tilde{x}_3(\tilde{t},a) = 0$ exists.

Lemma 3. If no disclosure costs are associated with security breach reporting $q_2 = 0$, only equilibria where agents voluntarily report breaches exist $\tilde{t} = 1$. Otherwise, if $q_2 > 0$, equilibria implying that agents do not report breaches exist $\tilde{t} = 0$, unless an audit probability $a \geq a_{\min} = q_2/(q_2 + S)$ is introduced.

The proof is in Appendix 3.3.
Nash equilibria imply the security breach reporting strategy

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

Agents' reporting decision depends on associated disclosure costs and the introduction of audits by the principal. If there are no disclosure costs, agents will always comply with reporting obligations regardless of audits. This is because in Section "Disclosure costs and security audits," we assume that agents act law-abiding in cases where reporting does not make them worse off than non-reporting. Otherwise, the principal requires audits and sanctions to incentivize compliance. For this mechanism to work, the audit probability has to be adapted to agents' disclosure costs and the sanction level.

Figure 3 (a) and (b) demonstrate all interesting cases of agents' best responses to different audit probabilities introduced by the principal, assuming disclosure costs $q_2 > 0$. Both figures include the computed social optimum ($t^* = 0, x^*(0)$) as a reference point (indicated by +).

First we discuss best responses of agents who expect audits with probability $0 \leq a < a_{\min}$, depicted by solid and dashed lines in Fig. 3 (a) and (b). (See the next paragraph for a discussion of the dotted lines.) This audit probability does not incentivize agents' reporting to an authority, i.e., compliance. Yet, differences in the audit probability and interdependence alter evolving equilibria. Figure 3 (a) depicts a setting with low interdependence $\gamma = .3$. In this setting, only one Nash equilibrium $(a, 0, \tilde{x}_2(0,a))$ exists that implies investments increasing in the audit probability, but which are always below the socially optimal investment. By contrast, Fig. 3 (b) depicts a setting with high interdependence $\gamma = .8$. Here, if no security audits are conducted $a = 0$, only the Nash equilibrium $(0, 0, \tilde{x}_3(0,0))$ where agents do not invest in information security at all exists. An increase in the audit probability $0 < a < a_{\min}$ eventually leads to two additional equilibria $(a, 0, \tilde{x}_{1,2}(0,a))$. These equilibria imply the security investments $\tilde{x}_1\,(0,a)$ and $\tilde{x}_2\,(0,a)$, which are decreasing and increasing in the audit probability, respectively. However, they always stay below the socially optimal investment.

Figure 3 (a) and (b) also show best responses of agents who expect audits with probability $a \geq a_{\min}$ by dotted lines. This probability incentivizes agents' compliance. Moreover, differences in the audit probability and interdependence alter equilibrium strategies. In a setting with low interdependence, depicted in Fig. 3 (a), agents have an incentive to introduce very high security investments. Here only one Nash equilibrium $(a, 1, \tilde{x}_2(1,a))$ exists that implies investments increasing in the audit probability, and exceeding the socially optimal investment. Consequently, agents over-invest in security, leading to high social costs. These costs may surpass the benefits from enforced sharing, which can render mandatory security breach reporting to an authority as ineffective from a welfare point of view. In contrast, if there is high security interdependence in an economy, as depicted in Fig. 3 (b), the introduction of a high audit probability enforcing agents' breach reporting can be very effective. This is because audits may create incentives to invest in security. In the depicted scenario, only the Nash equilibrium $(a, 1, \tilde{x}_2(1,a))$ exists. At this equilibrium, agents' investments are below the socially optimal investment and increase in the audit probability. Thus, a notification law enforced by the principal can be socially beneficial.

Principal

The principal chooses the audit probability. To decide on this probability, he observes the maximum security investment $\tilde{x}_2(\tilde{t}, a)$ of the agents as incentive compatibility constraint. The principal does not have to consider participation constraints, as security breach notification laws are legally binding. Thus, his objective is to minimize social costs according to:

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

Lemma 4. If the sanction level is positive $S > 0$, social costs always increase in the audit probability except for the case where this probability incites $\tilde{t} = 1$.

The proof is in Appendix 4.1.

Following Lemma 4, a high audit probability has to be avoided. However, according to Lemma 3, audits may incentivize security breach reporting. Consequently, the principal introduces an audit probability which just breaks even to incentivize reporting, i.e., $a_{\min}$, and at the same time reduces social costs. This leads to the case distinction

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

Lemma 5. If $q_2 > 0$, $S > 0$, and $\tilde{a} = a_{\min}$, the audit probability at all equilibria $\tilde{a}$ decreases with the sanction level S and increases with agents' disclosure costs q_2.

The proof is in Appendix 4.2.

The principal can substitute the audit probability and sanction level to maintain the power of his incentive mechanism. If high disclosure costs result in disincentives for agents against reporting breaches, the principal can counter this issue by raising the expected sanctions. This can be done by increasing the audit probability or sanction level, *ceteris paribus*.

Proposition 2. All equilibria imply an audit probability $\tilde{a}$ that constitutes a threshold value. If audits with the probability $\tilde{a} = a_{\min}$ decrease social costs as compared to the situation without audits $\tilde{a} = 0$, the principal chooses the audit probability $\tilde{a} = a_{\min}$. Thus, only the equilibrium $(\tilde{a} = a_{\min}, \tilde{t} = 1, \tilde{x}_2(1, a_{\min}))$ exists. Otherwise, the principal chooses the audit probability $\tilde{a} = 0$, and up the three equilibria $(\tilde{a} = 0, \tilde{t}, \tilde{x}_{1,2,3}(\tilde{t}, 0))$ may exist simultaneously.

Proof. According to Equation (17), the principal either enforces reporting with an audit probability $\tilde{a} = a_{\min}$ or abstains from enforcement. If the principal enforces reporting, he uses the incentive compatibility constrain $x = \tilde{x}_2(\tilde{t}, a)$ such that the only existing Nash equilibrium is $(\tilde{a} = a_{\min}, \tilde{t} = 1, \tilde{x}_2(1, a_{\min}))$. Otherwise, if he abstains from enforcement, up to three Nash equilibria $(\tilde{a} = 0, \tilde{t}, \tilde{x}_{1,2,3}(\tilde{t}, 0))$ may exist. At these equilibria, agents introduce investments analogous to Lemma 2. Furthermore, agents' willingness to report breaches is in accordance with Lemma 3.

Figure 4 illustrates regions for the Nash equilibria introduced in Proposition 2, depending on different situations in the (γ, b, q_2)-parameter space. The three lines each starting in the origin of the coordinate system indicate a principal's indifference in enforcing breach reporting with audits, following from Equation (17), for three different types of an authority's effectiveness b. On and above the lines, the principal does not introduce audits. This is because the introduction of audits may only increase social cost, and is thus detrimental. Consequently, up to three Nash equilibria can exist simultaneously, i.e., $(\tilde{a} = 0, \tilde{t} = 0, \tilde{x}_{1,2,3}(0, 0))$. In the regions below the lines, the principal introduces audits which just break even to incentivize security breach reporting. This decreases social costs, and only the Nash equilibrium $(\tilde{a} = a_{\min}, \tilde{t} = 1, \tilde{x}_2(1, a_{\min}))$ exists. We conclude that the enforcement of mandatory security breach reporting to an authority is effective in case of high interdependence between agents, a high effectiveness of an informed authority in dissemination of knowledge, and low disclosure costs. If interdependence is high, audits can even stimulate agents' investments (cf. the regions below the lines starting from their slope at $\gamma = .749$). However, in case that disclosure costs exceed the direct costs of a security breach $q_2{>}q_1{=}1$, enforcement is likely to be detrimental.

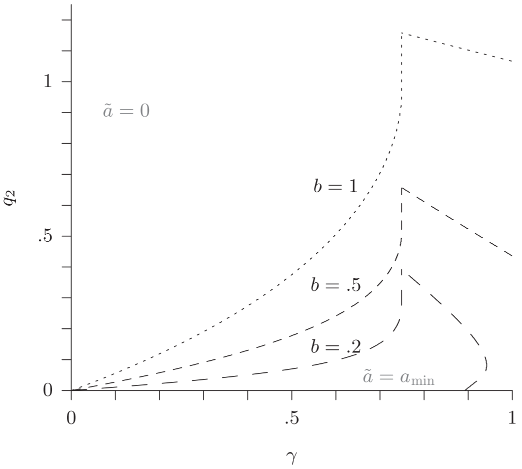

Figure 4. Principal's case distinction in (γ, b, q_2)-parameter space.

On the abscissa in Fig. 4, we find the special case where agents always report breaches voluntarily. Therefore, the introduction of audits to incentivize reporting is useless, and the three Nash equilibria $(\tilde{a} = 0, \tilde{t} = 1, \tilde{x}_{1,2,3}(1, 0))$ may exist.

Conclusion

Our 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 three parameters. We discuss inferences in Section "Discussion". Finally, we propose possible model extensions as an outlook for future research and lessons learned for national implementations of the NIS Directive in Section "Outlook."

Discussion

If disclosure costs are not negligible, a security breach notification law without security audits, regardless of the sanction level, cannot incentivize firms to report security breaches to authorities. Thus, authorities are unable to advise other firms by disseminating knowledge drawn from reported breaches. In turn, firms cannot use such knowledge to leverage their security investments. Rather, they make investments based on their self-interests. These investments are below the socially optimal level.

In contrast, a breach notification law with security audits and sanctions can incentivize firms to report breaches to authorities, regardless of accompanied disclosure costs. With such a law in place, firms face sanctions for noncompliance with reporting obligations, and indirect cost associated with information sharing. Therefore, firms conduct additional security investments to reduce their breach probabilities, and thus the number of reporting obligations. Furthermore, authorities can draw conclusions from firms' reported breaches and disseminate advice. This advice may help other firms to leverage their security investments. An overall increase in firms' security level reduces the negative effects of security interdependence in the economy. Consequently, the law potentially decreases social costs as compared to a situation without mandatory breach reporting. However, if there is a misadjustment of the audit probability and sanction level, it can happen that firms over-invest in security. Thus, the costs associated with the enforcement of the law may exceed the benefits from established breach reporting.

In order to demonstrate the difficulty in adjusting the audit probability and sanction level, consider the following scenario: assume that regulators impose a sanction level equal to the direct costs of breaches. Consequently, the optimal audit probability to incentivize breach reporting depends on the disclosure costs of firms. If the disclosure costs, direct costs, and the sanction level are all equal, regulators would have to introduce an audit probability of 50% to enforce mandatory security breach reporting to authorities. Regard the situation in Germany to examine the practical implications of this scenario. In 2012, the "Statistisches Bundesamt" recorded about 80 000 German firms employing more than 50 people [37]. In the event that a breach notification law affects all of these firms, about 40 000 security audits are required—in a period to be defined—to incentivize their compliance. However, an introduction of more than 40 000 audits, or a considerable increase in the sanction level, *ceteris paribus*, can lead to security over-investments. A tradeoff between audits and sanctions may be conceivable in order to enact a politically feasible security breach notification law. Regulators can, e.g., increase the sanction level to decrease the amount of security audits. But this harms firms which do not report breaches because they cannot detect them. Consequently, the enforcement of mandatory security breach reporting to authorities is not always socially beneficial.

Laws that enforce mandatory security breach reporting to authorities are most reasonable in case of high security interdependence between firms, and low disclosure costs. In fact, if disclosure costs exceed the direct costs associated with breaches, enforcement will almost always be detrimental. 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 others. However, we lack quantifications of the parameter in our model, and thus require further empirical evidence. Without evidence on where in the parameter space economies stand, legislative approaches stipulating breach reporting to authorities should be called into question.

Outlook

We have presented a simple economic model, in which regulators introduce security audits and impose sanctions on firms to enforce mandatory breach reporting to authorities. In particular, the proposed NIS Directive [21] motivates this approach. As a next step, our results on the adjustments of audit probabilities and sanction levels which effectively incentive firms' breach reporting should undergo a feasibility check.

Furthermore, different extensions of our model are conceivable. It is possible to interpret effective knowledge dissemination of authorities as a reduction in the breach probability at firms, rather than a reduction of interdependence between firms [18]. This could be modeled via an effect of information sharing on the economy-wide security productivity. Besides, one could consider over-reporting of firms, which has been identified in the context of other notification laws and can harm information quality. Additionally, the modeling of security audits' inaccuracy and entailed costs promises interesting results.

With regard to future models on breach notification laws, it is possible to incorporate government strategies fostering voluntary compliance and self-regulation of firms [22]. These models may, e. g., regard political instruments such as subsidies, liabilities, and taxes. One could utilize the currently discussed US legislation, providing for liability protection of firms that share information about breaches with authorities, as a starting point for the construction of such models.

We can also learn some lessons for national implementations of the NIS Directive. The benefit to society of its implementation depends on economy-wide interdependence, though we could not find any empirical quantification of interdependence. Thus, regulators should place this on their research agenda. Additionally, regulators have to be cautious when adjusting the audit probability and sanctions level to incentivize firms' breach reporting. Such adjustments must respect disclosure costs associated with reporting, which may differ between firms of different size and type. Therefore, regulators should not implement a "one-size-fits-all" solution, but have to adapt different incentive mechanism to groups of "similar" firms. It remains an open question if the established breakdown by sectors is the best classification for this purpose.

Acknowledgements

Parts of this research have been funded by the German Bundesministerium für Bildung und Forschung (BMBF) under grant agreement No. 16KIS0054. Furthermore, we acknowledge support by the Open Access Publication Fund of the Westfälische Wilhelms-Universität Münster.

References

1. Gordon L, Loeb M, Zhou L. The impact of information security breaches: Has there been a downward shift in costs? *J Comput Secur* 2011;**19**:33–56.
2. Fischer-Hübner S. IT-Security. In: Goos G, Hartmanis J, van Leeuwen J (ed). *IT-Security and Privacy: Design and Use of Privacy-enhancing Security Mechanisms, Vol. 1958, Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, 2001, 35–105.
3. PwC. Managing cyber risks in an interconnected world Key–findings from The Global State of Information Security Survey 2015. Technical report. PricewaterhouseCoopers (PwC), 2015.
4. 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. *Int J Electron Commerce* 2004;**9**:69–104.
5. Kunreuther H, Heal G. Interdependent security. *J Risk Uncertainty* 2003;**26**:231–49.
6. Anderson R, Böhme R, Clayton R, *et al*. Security economics and the internal market. Technical report. European Network and Information Security Agency (ENISA), 2008.
7. Hiller J, Russell R. The challenge and imperative of private sector cybersecurity: An international comparison. *Comput Law Sec Rev* 2013;**29**:236–45.
8. State security breach notification laws. Available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (19 May 2016, date last accessed).

9. Dekker 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.
10. Gal-Or E, Ghose A. The economic incentives for sharing security information. *Inform Syst Res* 2005;**16**:186–208.
11. Acquisti A, Friedman A, Telang R. Is there a cost to privacy breaches? An event study. In: *Workshop on Economics of Information Security (WEIS), University of Cambridge, UK*, 2006.
12. Romanosky S, Telang R, Acquisti A. Do data breach disclosure laws reduce identity theft? In: *Workshop on Economics of Information Security (WEIS), Hanover, NH, USA*, 2008.
13. Romanosky S, Hoffman D, Acquisti A. Empirical analysis of data breach litigation. *J Empir Leg Stud* 2014;**11**:74–104.
14. 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.
15. 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 University, MA, USA*, 2010.
16. Gordon L, Loeb M, Lucyshyn W. Sharing information on computer systems security: An economic analysis. *J Account Publ Pol* 2003;**22**:461–85.
17. Hausken K. Information sharing among firms and cyber attacks. *J Account Publ Pol* 2007;**26**:639–88.
18. Öğüt H, Menon N, Raghunathan S. Cyber insurance and IT security investment: Impact of interdependent risk. In: *Workshop on the Economics of Information Security (WEIS), Harvard University, MA, USA*, 2005.
19. Laube S, Böhme R. Mandatory security information sharing with authorities: Implications on investments in internal controls. In: *ACM Conference on Computer and Communication Security (ACM CCS), Workshop on Information Sharing and Collaborative Security, Denver, CO, USA*, 2015, pp. 31–42.
20. ENISA. Cyber security information sharing: An overview of regulatory and non-regulatory approaches. Technical report. European Union Agency For Network And Information Security (ENISA), 2015.
21. 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.
22. Winn J. Are 'better' security breach notification laws possible? *Berk Tech Law J* 2009;**24**:1133–65.
23. Cavusoglu H, Mishra B, Raghunathan S. The value of intrusion detection systems in information technology security architecture. *Inform Syst. Res* 2005;**16**:28–46.
24. Liu D, Ji Y, Mookerjee V. Knowledge sharing and investment decisions in information security. *Decis Support Syst* 2011;**52**:95–107.
25. Ng D, Stoeckenius J. Auditing: Incentives and truthful reporting. *J Account Res* 1979;**17**:1–24.
26. Nalebuff B, Scharfstein D. Testing in models of asymmetric information. *Rev Econ Stud* 1987;**54**:265–77.
27. Zhou L. The value of security audits, asymmetric information and market impacts of security breaches. PhD Thesis, University of Maryland, MD, USA, 2004.
28. Laffont J, Martimort D. *The Theory of Incentives: The Principal–agent model*. Princeton, NJ: Princeton University Press, 2002.
29. Gordon L, Loeb M. The economics of information security investment. *ACM Trans Inform Syst Secur* 2002;**5**:438–57.
30. Khouzani M, Pham V, Cid C. Strategic discovery and sharing of vulnerabilities in competitive environments. In: Poovendran R, Saad W (ed). *Decision and Game Theory for Security, Vol. 8840. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, 2014, 59–78.
31. Naghizadeh P, Liu M. Inter-temporal incentives in security information sharing agreements. In: *AAAI-16 Workshop on Artificial Intelligence for Cyber Sercurity (AICS), Phoenix, AZ, USA*, 2016.
32. Gay S. Strategic news bundling and privacy breach disclosures. In: *Workshop on the Economics of Information Security* (*WEIS*)*, Berkeley, CA, USA*, 2016.
33. Böhme R. Security audits revisited. In: Keromytis A (ed), *Financial Cryptography and Data Security (FC), Volume 7397, Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, 2012, 129–47.
34. Lippmann R, Haines J, Fried D, *et al*. The 1999 DARPA off-line intrusion detection evaluation. *Comput Network* 2000;**34**:579–95.
35. 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 State University, PA, USA*, 2014.
36. Macho-Stadler I, Pérez-Castrillo D. Principal–agent models. In: Meyers R (ed). *Encyclopedia of Complexity and Systems Science*. New York: Springer, 2009, 6977–90.
37. Statistisches Bundesamt. *Statistisches Jahrbuch Deutschland und Internationales*. Wiesbaden: Statistisches Bundesamt, 2013.

Appendix 1: Symbols

Table A1. 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	$a \in [0, 1]$
q_2	Parameter	Security breach disclosure costs	$q_2 \geq 0$
γ	Parameter	Security interdependence	$\gamma \in [0, 1]$
b	Parameter	Effectiveness of an authority	$b \in [0, 1]$
n	Constant	Number of firms	$n = 2$
S	Constant	Sanction level	$S = 1$
ϵ	Constant	Error rate of detective controls	$\epsilon = .2$
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	Changes in 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	$\psi \in \{0, 1\}$

Appendix 2: Social planner controls both security investments and security breach reporting (cf. Section "Social optima")

The first derivations of Equation (9), w. r. t. x and t, are:

$$\frac{\partial c}{\partial x} = [\gamma \cdot \eta(t^*) \cdot (1 - P(x)) + (1 - \gamma \cdot \eta(t^*) \cdot P(x))] \cdot L(t^*, 0) \cdot \frac{\partial P(x)}{\partial x} + 1\,, \tag{A.1}$$

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

Appendix 2.1 Optimal security investment

The root of the first-order condition of Equation (9) $\partial c / \partial x = 0$ is:

$$x^*(t^*) = -\frac{\log\left(\frac{\gamma \cdot \eta(t^*)+1}{4 \cdot \gamma \cdot \eta(t^*)} - \sqrt{\frac{(\gamma \cdot \eta(t^*)+1)^2}{16 \cdot \gamma^2 \cdot \eta(t^*)^2} - \frac{1}{2 \cdot \gamma \cdot \log\,(\beta) \cdot \eta(t^*) \cdot L(t^*, 0)}}\right)}{\log(\beta)}\,. \tag{A.3}$$

This expression corresponds to Equation (10).

Appendix 2.2 Optimal security breach reporting and Proof of Lemma 1

Proof. The second derivation of Equation (9) $\partial^2 c / \partial t^2$ is:

$$\frac{\partial^2 c}{\partial t^2} = -2 \cdot b \cdot \gamma \cdot q_2 \cdot (1 - \epsilon)^2 \cdot (1 - P(x^*)) \cdot P(x^*)\,. \tag{A.4}$$

Based on Equation (A.4), we observe that, for $b > 0$, $\gamma > 0$, $q_2 > 0$, $\epsilon > 0$ and any x^*, $\partial^2 c / \partial t^2 < 0$. Thus, the cost function in Equation (9) is concave in t, and $t^*(x^*) \in \{0, 1\}$ are boundary values.

Appendix 3: Agents control both security investments and security breach reporting (cf. Section "Nash equilibria")

The first derivations of Equation (12), w. r. t. x_i and t_i, are:

$$\frac{\partial c_i}{\partial x_i} = (1 - \gamma \cdot \eta(t_{1-i}) \cdot P(x_{1-i})) \cdot L_i(t_i, a) \cdot \frac{\partial P(x_i)}{\partial x_i} + 1\,, \tag{A.5}$$

$$\frac{\partial c_i}{\partial t_i} = P_i(x_i, x_{1-i}, t_{1-i}) \cdot (1 - \epsilon) \cdot (q_2 - a \cdot (q_2 + S))\,. \tag{A.6}$$

Appendix 3.1 Security investments

The root of the first-order condition of Equation (12) $\partial c_i / \partial x_i = 0$, i.e., the best response of agent i, is:

$$x_i^+(x_{1-i}, t_i, t_{1-i}, a) = \sup\left\{-\frac{\log\left(\frac{1}{\log\,(\beta) \cdot L(t_i, a) \cdot (1 - \gamma \cdot \eta(t_{1-i}) \cdot \beta^{-x_{1-i}})}\right)}{\log(\beta)}, 0\right\}. \tag{A.7}$$

The mutual best response $\tilde{x}(\tilde{t}, a) = x_i^+(\tilde{x}, \tilde{t}, \tilde{t}, a)$ leads to security investments at Nash equilibria. Note that because of the constraint in Equation (12), there also exists a corner case if $0 = x_i^+(0, \tilde{t}, \tilde{t}, a)$. Thus, equilibria can imply the security investments:

$$\tilde{x}_{1,2}(\tilde{t}, a) = -\frac{\log\left(\frac{1}{2 \cdot \gamma \cdot \eta(\tilde{t})} \pm \sqrt{\frac{1}{4 \cdot \gamma^2 \cdot \eta(\tilde{t})^2} - \frac{1}{\gamma \cdot \log\,(\beta) \cdot \eta(\tilde{t}) \cdot L(\tilde{t}, a)}}\right)}{\log(\beta)}\,, \tag{A.8}$$

$$\tilde{x}_3(\tilde{t}, a) = 0\,. \tag{A.9}$$

This corresponds to Equations (13) and (14).

Appendix 3.2 Proof of Lemma 2

Proof. The amount of present equilibria depends on the discriminant in Equation (A.8). If the discriminant is negative, e.g., because

$$\gamma > \frac{\log(\beta) \cdot L(\tilde{t},a)}{4 \cdot \eta(t)} \,, \tag{A.10}$$

then only one equilibrium implying $\tilde{x}_3(\tilde{t},a) = 0$ exists. Otherwise, the two equilibria with investments $\tilde{x}_{1,2}(\tilde{t},a)$ may exist additionally, where $\tilde{x}_3(\tilde{t},a) \leq \tilde{x}_1(\tilde{t},a) \leq \tilde{x}_2(\tilde{t},a)$. Based on Equations (A.7) and (A.8), the three equilibria implying security investments $\tilde{x}_{1,2,3}(\tilde{t},a)$ can exist simultaneously under the conditions:

$$-\frac{\log\left(\frac{1}{2\cdot\gamma\cdot\eta(\tilde{t})} + \sqrt{\frac{1}{4\cdot\gamma^2\cdot\eta(\tilde{t})^2} - \frac{1}{\gamma\cdot\log\,(\beta)\cdot\eta(\tilde{t})\cdot L(\tilde{t},a)}}\right)}{\log\,(\beta)} \geq 0, \text{and} \tag{A.11}$$

$$-\frac{\log\left(\frac{1}{\log\,(\beta)\cdot L(t_i,a)\cdot\left(1-\gamma\cdot\eta(t_{1-i})\cdot\beta^{-0}\right)}\right)}{\log\,(\beta)} \leq 0\,. \tag{A.12}$$

Both conditions are fulfilled iff:

$$\gamma \geq \frac{\log\,(\beta) \cdot L(\tilde{t},a) - 1}{\log\,(\beta) \cdot \eta(\tilde{t}) \cdot L(\tilde{t},a)}\,. \tag{A.13}$$

Equations (A.10) and (A.13) can also be solved for all other parameter and the audit probability: all parameter and the audit probability influence the existence of all equilibria.

Based on the previous constraints, we can differentiate between three categories of model parameter settings that lead to different equilibria: (i) an equilibrium implying $\tilde{x}_3(\tilde{t},a)$ exist alone iff Equation (A.10) holds; (ii) the equilibria with security investments $\tilde{x}_{1,2,3}(\tilde{t},a)$ all exist simultaneously if Equation (A.13) holds, but not Equation (A.10); (iii) the equilibrium implying $\tilde{x}_2(\tilde{t},a)$ exists alone iff Equation (A.13) does not hold.

Appendix 3.3 Security breach reporting and Proof of Lemma 3

Proof. Based on the first derivation of Equation (12) $\partial c_i/\partial t_i$, we observe that:

$$\frac{\partial c_i}{\partial t_i} = \underbrace{P_i(x_i, x_{1-i}, t_{1-i})}_{>0} \cdot \underbrace{(1-\epsilon)\cdot(q_2 - a\cdot(q_2+S))}_{\text{sign depends on } a,\, S \text{ and } q_2}\,. \tag{A.14}$$

If $a = 0 \wedge q_2 > 0$, an agent does not have incentives to report security breaches, i.e., $\partial c_i/\partial t_i > 0$. Consequently, equilibria implying $\tilde{t}(\tilde{x},0) = 0$ evolve. Otherwise, if $a = 0 \wedge q_2 = 0$, agents are indifferent to reporting, i.e., $\partial c_i/\partial t_i = 0$. Based on our assumptions on agents' reporting behavior in Section "Disclosure costs and security audits", this leads to compliance. If $q_2 > 0$, a principal can incentivize agents to report breaches with the introduction of audits $a > 0$, which may lead to $\partial c_i/\partial t_i \leq 0$. In order to determine a principal's minimum audit probability $a = a_{\min}$ that incentivizes security breach reporting of agents, we use the second part of Equation (A.14), i.e.,

$$0 = (1-\epsilon)\cdot(q_2 - a_{\min}\cdot(q_2+S)) \Longleftrightarrow a_{\min} = \frac{q_2}{q_2+S}\,. \tag{A.15}$$

A principal can incentivize agents to report breaches with the introduction of an audit probability $a \geq a_{\min} = q_2/(q_2+S)$. Consequently, equilibria implying the reporting strategy $\tilde{t}(\tilde{x},a) = 1$ evolve if the audit probability is high enough.

Appendix 4: Principal controls audit probability (cf. Section "Nash equilibria")

The first derivation of Equation (16), w. r. t. a, is

$$\frac{\partial c}{\partial a} = 2\cdot P_i(x_i, x_{1-i}, t_{1-i})\cdot((1-t_i)\cdot(1-\epsilon)\cdot(q_2+S) + \epsilon\cdot(q_2+S))\,. \tag{A.16}$$

Appendix 4.1 Proof of Lemma 4

Proof. Based on Equation (A. 16), if the sanction level is positive $S > 0$, and except for the case where the audit probability incites $\tilde{t} = 1$, we find that:

$$\frac{\partial c}{\partial a} > 0\,. \tag{A.17}$$

Appendix 4.2 Proof of Lemma 5

Proof. In Appendix 3.3, we derived the audit probability to incentivize reporting of agents, i.e., $a_{\min} = q_2/(q_2+S)$. The first derivations of $a_{\min}$, w. r. t. S and q_2, are

$$\frac{\partial a_{\min}}{\partial S} = -\frac{q_2}{(q_2+S)^2}\,, \text{ and} \tag{A.18}$$

$$\frac{\partial a_{\min}}{\partial q_2} = \frac{S}{(q_2+S)^2}\,. \tag{A.19}$$

If $q_2 > 0$ and $S > 0$, we find that $\partial a_{\min}/\partial S < 0$ and $\partial a_{\min}/\partial q_2 > 0$.