Attack-Deterring and Damage-Control Investments in Cybersecurity*

Wing Man Wynne Lam†

May, 2015

Abstract

This paper studies investment in cybersecurity, where both the software vendor and the consumers can invest in security. In addition, the vendor can undertake attack-deterring and damage-control investments. I show that full liability, under which the vendor is liable for all damages, does not achieve efficiency and, in particular, the vendor underinvests in attack deterrence and overinvests in damage control. Instead, the joint use of an optimal standard, which establishes a minimum compliance framework, and partial liability can restore efficiency. This suggests that policies that encourage not only firms, but also consumers to invest in security might be desirable.

Keywords: cybersecurity, investment, standard, liability, bilateral care

JEL Classification: K13, L1, L8

1 Introduction

New security concerns are constantly arising as privacy breaches proliferate and cyber attacks escalate. For example, a recent data breach on an unprecedented scale saw more than 1.2 billion credentials stolen by a Russian criminal group.[1] Moreover, we continue to see the rise of "ransomware" (a malicious program that encrypts files on the victim's computer and demands a fee before unlocking those files), the discovery of security flaws on smartphones, and the emergence of new security risks from the "Internet of Things" (such as hackers stealing sensitive data from owners of Internet-connected objects—from locks, lights, thermostats, televisions,

*I thank Paul Belleflamme, Giacomo Calzolari, Jacques Crémer, Vincenzo Denicolò, Axel Gautier, Domenico Menicucci, Paul Seabright, anonymous reviewers from the WEIS 2015 conference, and participants at the LCII and CORE 2015 Digital Economy Workshop, as well as at the seminar at Saint-Louis University Brussels for their helpful comments. I also acknowledge the support of Toulouse School of Economics and University of Bologna in earlier versions of this work. Any opinions expressed are those of the author only.

†University of Liege (ULg), HEC Management School, Liege Competition and Innovation Institute (LCII). E-mail: wingmanwynne.lam@ulg.ac.be

[1]See "Russia gang hacks 1.2 billion usernames and passwords," *BBC News*, August 6 2014, available at `http://www.bbc.com/news/technology-28654613`.

refrigerators, washing machines, to cars). A critical gap has thus emerged between firms' investment in cybersecurity and today's rapidly evolving technological advances, which warrants further research. More particularly, good security depends on more than just the design of the technology. It requires a deeper understanding of the investment incentives of different parties. While software vendors are motivated to minimize their own private costs, the social planner's goal is to minimize society's costs.[2] We therefore expect that firms' incentives to invest are suboptimal, but it remains an interesting open question of how best to solve the problem.

In the software industry, technologies are never faultless. Firms often undertake investments in attack prevention and bug fixing sequentially. In the existing literature on bilateral care, both the firm and the consumers can only engage in one type of precaution to lower the expected damage. It is important to recognize, however, that multiple types of investments undertaken by one party will change the conventional result that strict liability with a defense of contributory negligence, under which the firm is *fully* liable only if the consumer is not negligent, yields optimal investment (Brown, 1973). Instead this paper shows that the joint use of a *partial* liability regime (or more precisely, the firm bears a fine/reimbursement that is smaller than consumers' damage level) and an optimal standard can restore the first-best outcome. This argument is also consistent with the view taken by some security experts, for example, Bruce Schneier argued informally that

> *"100% of the liability should not fall on the shoulders of the software vendor, just as 100% should not fall on the attacker or the network owner. But today, 100% of the cost falls directly on the network owner, and that just has to stop."*[3]

More specifically, a standard is a minimum level of security set by courts or other regulatory agencies. In practice, there are different types of security standards, such as encryption standards, security breach notification standards, IT continuity standards, set by the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) in the U.S., and more widely by the International Organization for Standards (ISO) and Internet Engineering Task Force (IETF). Liability rules state the amount of damage each party is liable for, and they are governed by the tort system. For example, consumers may file lawsuits against firms for security breaches, data leakage, and infringement of privacy, and firms, if proven they have caused harm or they are negligent in exercising due care (usually a standard set by courts), will be held accountable for consumer damages. However, it is not clear which kind of legislation (particularly, standards or liability rules) would better incentivize firms and consumers to invest in security optimally, whether these interventions should be used jointly or separately, and which liability regime could lead to socially efficient investments.

This paper presents a formal model for analyzing these questions. I consider a firm that sells software products, which are subject to potential security problems. The firm can invest in attack deterrence and damage control to increase security. Considering attack-deterring

[2]See Anderson, Clayton and Moore (2009), and Anderson and Moore (2009) for surveys of the economics of Internet security.

[3]See Schneier (2007). "Information Security and Externalities," available at `https://www.schneier.com/essays/archives/2007/01/information_security_1.html`.

investments, if, for example, good infiltration detection and authentication technologies are in place, online attacks (phishing, denial-of-service, virus attacks, among others) can be prevented in the first place. Damage-control investments are remediation strategies, for example, finding, testing, and fixing the bug prevents consumers' data from falling into the wrong hands again. If the firm discovers the bug, it can choose whether to disclose it or hide it. If the firm discloses the bug information, consumers can choose whether to take precaution or not. For example, once a security problem is disclosed, consumers can adopt various defenses (firewalls, cryptographic protocols, virus detection techniques, intrusion detection systems, data-loss prevention features, among others) against online attacks. Consumers differ in their costs of taking precaution: actions are more costly for the laymen than for the computer experts. For example, the costs of taking precautions vary for different sectors and for different size of companies. While financial services, telecommunication sectors, utilities and government departments have far more resources to hire security professionals to maintain and manage top-notch security tools, smaller companies in other sectors such as manufacturing and retail have relatively limited budgets to hire, and hence their engineers may not have a keen understanding about the state-of-the-art security, which results in higher learning costs than their better trained counterparts.

I find that since the firm does not suffer the full costs of the society in case of security failure, its incentives to invest are suboptimal and, in particular, it underinvests in attack deterrence and overinvests in damage control. I show that there are inefficiencies associated with the joint use of a full liability rule and an optimal standard to increase security. Interestingly, switching to a partial liability rule leads to socially efficient investments by both the firm and the consumers, and this result continues to hold when liability is imposed as a fine to the regulator and when it is imposed as a reimbursement to the consumers. The important implications of these results are that the regulator could implement similar standards of security and privacy as other, already regulated, industries such as automotive and aviation, and put in place policies that promote the sharing of security investment responsibility between firms and consumers. Since not all users apply patches immediately after their introduction (e.g. ordinary computer users may ignore security risk warnings, while enterprise engineers are time constrained to apply patches and malware-removal tools in a timely manner), there is usually a gap between the date when a patch is released and when it is adopted. This suggests that policies that help synchronize patch release and adoption cycles, raise cybersecurity awareness by sending information to users, and implement third-party vulnerability management could be useful. I will explore these policy implications in more detail in Section 3.1.

In addition to multiple investments, the presence of network externalities is another important feature of the software industry. Considering indirect network externalities, an interesting corollary of my result is that increasing the number of computer experts improves social welfare, but it exacerbates the under- and over-investment problems when the firm is liable for a substantial part of the damage. The reason for the latter is that the difference between the private and social incentives to invest arises from two sources of inefficiency. The first is that the firm does not pay fully for the damage, and the total amount of damage is decreasing in the number of experts. The second source of inefficiency is that the firm ignores the precautionary costs of the consumers when it makes its investment decision, and the total cost of precaution

is increasing in the number of experts. When the firm bears substantial liability for consumers' damage, the second source of inefficiency dominates. These results suggest that if the objective of the government is to improve social welfare, policymakers can provide support and training in the area of cybersecurity so that users become more competent in managing security threats. However, if the goal is to alleviate inefficiency, then the government needs to be careful about increasing the number of experts because the objectives of the social planner and the firm will become more divergent.

The main contribution of this paper is that it considers three types of investments. As in traditional bilateral care models in the literature on torts, my model allows both the firm and the consumer to invest in security in order to lower the expected damage, but in addition, I introduce two types of investment the firm can undertake, namely, attack deterrence and damage control. In the software industry, technology is always changing. Firms develop and release new functionalities quickly. Software products are therefore never free of bugs, and it is very common to observe multiple rounds of debugging (sequential investments). I show that such possibility of sequential investments on the part of the firm complemented by a third precautionary investment on the part of the consumers leads to a new argument supporting the joint use of a standard and partial liability, under which the firm is only partially liable for damage caused. The result of a partial liability rule being optimal in this paper parallels the results in the literature on asymmetric information, which studies how the presence of double moral hazard problem affects optimal warranty design. When the firm has private information about its product quality, but such quality is unobservable to consumers, it can use warranties to signal good quality. However, if firms offer full warranties or refunds to consumers, consumers might not exercise reasonable care, which leads to a double moral hazard problem. Cooper and Ross (1985) and Belleflamme and Peitz (2010), for instance, show that under double moral hazard, the optimal warranty calls for partial compensation for a defective product. However, I show that a partial liability rule supports optimal care even when all investments are publicly observable (to the firm, the consumers and the courts). That is, the result of a partial rule being optimal does not require moral hazard. This suggests that the seed of an explanation for shifting some of the burden of care to the consumers lies in the cost of precautionary actions of the consumers rather than the presence of moral hazard problem. It is then important for the regulator to recognize that solving the moral hazard problem is not sufficient to restore investment efficiency. Instead, the regulator should focus on the design of policies that share the burden of care between the software vendor and the consumers. Furthermore, I show that introducing three types of investments may lead to "vaporware" practice even in the absence of preemptive motives and reputation concerns: because attack-deterring and damage-control investments are substitutes, allowing firms to fix security problem later increases the likelihood of releasing a less secure software product in the first place—a new perspective in the vaporware literature.

1.1 Literature

This paper contributes to three strands of literature. First, it is related to recent works on the economics of security investment. Gordon and Loeb (2002) study the optimal protection of information, which varies with the information set's vulnerability.[4] Kunreuther and Heal (2003), August and Tunca (2011), Acemoglu et al. (2013), and Riordan (2014) study investment incentives in the presence of network externalities. My model differs from these papers in that they consider each firm taking one action, whereas the firm in this paper can undertake both attack-deterring and damage-control investments. Varian (2004) examines full liability in a model in which efforts of multiple parties are needed to increase security. He finds that liability should be assigned entirely to the party who can best manage the risk. Different from his analysis, I also consider partial liability, and the joint effect of partial liability and standards.

Second, this paper relates to the economics and legal literature on tort laws, but it departs from traditional bilateral care models (see, for instance, Brown, 1973; Shavell, 1980; Landes and Posner, 1985; and Daughety and Reinganum, 2013a), in which both the firm and the consumer can lower the expected damage by their choices of care, by introducing three types of investments.[5] More specifically, in their models each party can take one type of care, whereas in my model the firm can invest in attack deterrence and damage control, and additionally the consumer can take precautionary action. Modeling in this way, I find that a partial liability rule yields the socially efficient outcome, which differs from what is found in Brown (1973).[6] I will explain the sources of the difference in results in Section 3. There is also some literature that focuses on either attack-deterring investment, as in Daughety and Reinganum (1995, 2006), or damage-control investment, as in Polinsky and Shavell (2010);[7] rather than dealing with both. Other papers such as Shavell (1984) and Kolstad et al. (1990) compare standards with liability rules. However, Shavell's analysis is based on the inefficiencies associated with the potential bankruptcy of the firm and the uncertainty of lawsuit by the consumers, while the inefficiencies studied by Kolstad et al. are due to the uncertainty over the legal standard to which the firm will be held liable. Differently, inefficiencies here are caused by the firm having the possibility to undertake two types of investments.

Finally, this paper shares with the literature on disclosure laws (see, for example, Granick

[4]There are other security investment models in computer science (for a survey, see Böhme, 2010), which, for instance, investigate questions about the appropriate amount of security budgets (i.e. how much to invest) and firms' security investment strategies (i.e. when and where to invest). However, they do not tackle the investment problem from the legal and economic perspectives, meaning that the effects of security standards and liability policies on investment incentives (i.e. what measures should the regulator implement) have been largely ignored in this literature.

[5]See Shavell (2008) and Daughety and Reinganum (2013b) for excellent surveys of the literature on torts.

[6]Since I do not consider usage in this model, Shavell (1980) and Landes and Posner (1985), who study proportional-harm model (meaning the effect of harm is linear on usage), and Daughety and Reinganum (2013a), who focus on cumulative-harm model (meaning the effect of harm is non-linear on usage), are not the primary point of comparison with this model.

[7]Polinsky and Shavell analyze information acquisition about product risks when product quality is uncertain. Therefore, their problem concerns damage-control, rather than attack-deterring, investment.

(2005) and Choi et al. (2010a)) the focus on the tradeoff that arises from disclosing software vulnerabilities: while secrecy prevents attackers from taking advantage of publicized security flaws, it interferes with scientific advancement in security, which is largely based on information sharing and cooperation. Choi et al. also examine the effect of a mandatory disclosure policy and a "bug bounty" program on welfare. However, they take security investments as given, and do not discuss optimal investment. Daughety and Reinganum (2005) study the effect of confidential settlement on product safety, but their focus is not on investment. This paper extends this literature by analyzing the optimal investment in security, and such investment is of two types: attack deterrence and damage control.

2 The Model

Monopoly software vendor. Consider a firm that produces a software product which contains potential bugs. For simplicity, I assume away prices, so that the problem is simplified to choosing a level of security that minimizes the sum of the costs. The assumption is reasonable for consumers who have already bought the software and are therefore not concerned about the prices. Moreover, if the firm generates profit from channels other than selling the software product such as advertisement, then the objective is simply to minimize the costs.

Heterogeneous consumers. There is a unit mass of consumers. Consumers have different precaution costs: a proportion α of them are "computer experts" and have precaution cost γ drawn from a distribution $F(\gamma) \sim [0, +\infty)$, while the others are "laymen" with $\gamma = \infty$. The firm knows $F(\gamma)$, but cannot observe each consumer's type. Experts are security professionals who can take security precautions such as monitoring the system for attacks and patching the system if the firm discloses the presence of a security problem, while laymen without such professional knowledge will never take precautions.[8] Assume that consumers always have positive utility in using the software.

In the main text, there are two types of consumers: all experts have the same γ and all laymen have an infinite cost. However, in the alternative model presented in Appendix A, I consider a continuum of consumers whose precautionary cost γ is distributed according to $F(\gamma)$ (with a slight abuse of notations). However, this would not change my main results.

Timing of the game. (i) The firm invests s in security at a cost $c(s)$ in order to prevent attacks. Such investment could take the form of improvement in infiltration detection or authentication technologies. (ii) By investing $m(b)$ in damage control, the firm will find a bug before the hacker does with probability b.[9] Let $p(s)$ be the probability that the hacker will attack. I assume away strategic attacks.[10] (iii) If the firm discovers a bug, it can choose whether

[8] I assume that consumers take precaution after the firm has disclosed the information about the bug. One could alternatively think of consumers taking precaution ex ante. However, the qualitative result will not change as long as the costs associated with these precautions are not borne by the firm.

[9] Whether the firm chooses s and b sequentially or simultaneously does not affect the results, but in practice attack deterrence and damage control usually happen sequentially. The novelty is to have two types of investments on the part of the firm.

[10] Strategic attacks are modeled in, for instance, Acemoglu et al. (2013). They show that strategic targeting provides additional incentives for overinvestment in security because larger investment shifts attacks from one

or not to disclose the security problem. There is no cost in disclosing the bug. For example, the firm can simply post the information on its website. However, disclosure increases the probability of attack by a small ϵ.[11] (iv) γ is realized. If the firm discloses a bug, the experts can choose whether or not to take precaution.

Assumption 1. $c'(0) = 0, c'(s) > 0, c''(s) > 0, c'''(s) > 0, m'(0) = 0, m'(b) > 0, m''(b) > 0, m'''(b) > 0, p'(s) < 0,$ *and* $p''(s) > 0$.

Under Assumption 1, investment costs $c(s)$ and $m(b)$ are thrice differentiable, convex, and increasing in s and b respectively; and that probability of attack $p(s)$ is convex and decreasing in s.[12] [13] This model assumes that all investments are publicly observable. In reality, regulators and courts can monitor safety investments more easily in some cases (especially when it leads to lawsuits) compared to others. However, I chose not to model moral hazard in the firm's incentives to invest because this set-up allows me to highlight the source of investment inefficiency comes from the presence of consumers' precautionary costs rather than the moral hazard problem itself, which suggests that policies that merely get rid of the moral hazard problem is not enough to restore efficiency.

Damage. For the firm, the damage incurred from an attack is $\overline{\eta}$ in case the hacker discovers the bug before the firm does, and $\underline{\eta}$ in case the firm identifies the bug first. Assume that $\overline{\eta} > \underline{\eta}$. This could be the financial losses and reputational harm caused by stolen information of the firm becoming available to the hacker. Such loss is smaller if the firm finds the bug first as it can then try to fix the problem. However, the firm may face substantial loss if the hacker exploits a bug that has not been previously identified—a phenomenon known as "zero-day attacks". For the consumers, the damage from an attack is $\overline{\mu}$ if they do not take precaution and $\underline{\mu}$ if they do. This could be monetary loss due to fraudulent use of their personal information. Assume that $\overline{\mu} > \underline{\mu}$, meaning once informed, consumers can take actions to mitigate the risk of being attacked. Let $\lambda \in [0, 1]$ denote the part of consumers' damages for which the firm is liable.

In reality, liability can be imposed as a fine paid by the firm to the regulator, in which case the fine does not affect consumers' precautionary behavior, or liability can be imposed as a reimbursement to the consumers, in which case the refund does affect consumers' precautionary behavior. For example, fines are common in the IT industry. Regulatory bodies such as the British Information Commissioner's Office can issue fines to firms that breach the UK Data Protection Act. Companies such as Sony and eBay have historically been fined for a breach of the Act. Another example is AT&T's recent data breaches that took place in 2013 and 2014 at three of its international call centers. This has led to a $25 million fine, which is the

agent to another.

[11] Arora, Nandkumar and Telang (2006) show empirically that in some cases vulnerability disclosure increases the frequency of attacks.

[12] The third derivatives ensure that the profit function is well-behaved.

[13] If there are externalities between the two cost functions, meaning investing more in attack deterrence will make finding bugs easier, then there will be more investment in attack deterrence under both optimal and equilibrium regimes because of the cost reduction in damage control. However, it will not change the qualitative result that partial liability rule supports optimal investment, provided the firm does not take into account consumer's precautionary cost when choosing its investments.

largest penalty the Federal Communications Commission has ever imposed on a company for data security and privacy violations.[14] Reimbursements, however, are more common in finance. Many banks, for instance, guarantee zero liability for unauthorized online transactions, meaning consumers are reimbursed for all financial losses originating from identity theft. As another example, Target will reimburse victims of its data breach that occurred in 2013, which has resulted in the theft of at least 40 million credit card numbers.[15] In other industries and in general, fines are more applicable to cases where it is difficult for consumers to file lawsuits (for instance, because of the triviality of the security breach or the lack of financial resources to go against big firms), so that the firm cannot identify the victims of the attack to offer a refund. The basic model considers the case with fine, while Section 4.3 considers the case with reimbursement. Nevertheless, I show that the main result of Proposition 2 (below) that the partial liability rule yields the socially efficient outcome would not change under reimbursement. I focus on three liability regimes:[16]

- Full liability, under which the firm is liable for all damages faced by the consumers, i.e. $\lambda = 1$;
- Partial liability, under which the firm is partially liable for consumers' damages, i.e. $\lambda \in (0, 1)$;
- No liability, under which the firm is not liable for consumers' damages, i.e. $\lambda = 0$.

Thus, the total loss for the firm is $\eta + \lambda\mu$, where $\eta \in [\overline{\eta}, \underline{\eta}]$ and $\mu \in [\overline{\mu}, \underline{\mu}]$.

Regulatory policies. The regulator can set the minimal security standard, s, but cannot regulate directly the probability of finding a bug, b, which is difficult to predict in practice as b depends on the constantly evolving technologies of both the hackers and the defenders. Because of these unpredictable changes, the regulator chooses the optimal liability rule instead of b. A striking result is that partial liability is optimal as opposed to full liability emphasized in tort models, yielding interesting policy implications, which I will discuss in Section 3.1.

[14] See "AT&T pays record $25m fine over customer data thefts," *BBC News*, April 9 2015, available at `http://www.bbc.com/news/technology-32232604`.

[15] See "Target to pay $10m to settle lawsuit over data breach," *BBC News*, March 19 2015, available at `http://www.bbc.com/news/technology-31963612`.

[16] The legal literature uses other terminologies, for instance, they call the situation wherein a firm must fully compensate a consumer for harm caused "strict liability" instead of "full liability"; the situation wherein a firm is liable only if the consumer is not negligent "strict liability with a defense of contributory negligence"; and the situation wherein a negligent firm is only partially liable if the consumer is also negligent "comparative negligence".[17] However, much of the legal literature focuses on the first two rules, but rarely discusses the role of partial liability.

I adopt slightly different terminologies to disentangle the effect of two instruments—standards and liability rules—because in practice they are usually implemented by separate regulatory agencies. For example, rather than one court or agency making a centralized decision altogether, we have the tort system governing the circumstances under which a party is liable for damages caused, and other regulatory agencies setting standards.

3 Optimal Investment

I now work backward from the last stage. When the firm discloses a bug, the expected damage for a consumer who does not take precaution is $p(s)\overline{\mu}$, and that for a consumer who takes precaution is $p(s)\underline{\mu} + \gamma$. Therefore, the consumer will take precaution if

$$\gamma < p(s)(\overline{\mu} - \underline{\mu}). \tag{1}$$

In the disclosure stage, the firm can choose its disclosure policy in case it discovers a bug. If it does not disclose the security problem, its expected cost is $p(s)(\underline{\eta} + \lambda\overline{\mu})$. If it chooses to disclose, there are two cases. If consumers take precaution, the firm incurs a cost of $p(s)[\underline{\eta} + \lambda(\alpha\underline{\mu} + (1-\alpha)\overline{\mu})]$. However, if consumers do not take precaution, the cost becomes $p(s)(\underline{\eta} + \lambda\overline{\mu})$.[18] Therefore, the firm will only disclose if this leads consumers to take precaution, that is, if Equation (1) holds.

In the investment stage, the firm chooses s and b to minimize its expected loss, which is denoted by $\mathcal{L}^f$.

$$\begin{aligned}\min_{b,s} \mathcal{L}^f = {} & (1-b)p(s)(\overline{\eta} + \lambda\overline{\mu}) \\ & + b\left\{\int_0^{p(s)(\overline{\mu}-\underline{\mu})} p(s)[\underline{\eta} + \lambda(\alpha\underline{\mu} + (1-\alpha)\overline{\mu})]dF(\gamma) + \int_{p(s)(\overline{\mu}-\underline{\mu})}^{\infty} p(s)(\underline{\eta} + \lambda\overline{\mu})dF(\gamma)\right\} \\ & + m(b) + c(s). \end{aligned} \tag{2}$$

Let $b^m(s)$ denote the firm's optimal damage-control investment strategy given attack-deterring investment s, and let s^* and $b^* \equiv b^m(s^*)$ denote the solutions of Equation (2).

The first term in Equation (2) is the expected cost of the firm when the hacker discovers the bug first, in which case both the firm and the consumers suffer a large damage. When the firm finds the bug before the hacker, either it discloses the bug if consumers' cost is small, which is captured by the second term, or it does not disclose if consumers' cost is large, which is captured by the third term. In this case, the firm suffers a small damage from attack because it identifies the bug sooner than the hacker, while the extent of damages suffered by the consumers depends on whether precautionary measures are taken. The last two terms represent the costs of attack-deterring and damage-control investments.

The social planner's incentive to disclose is aligned with that of the firm, that is, the social planner will disclose as long as γ is small enough.[19] However, different from the firm, if the social planner chooses to disclose, its expected cost is $p(s)(\underline{\eta} + \alpha\underline{\mu} + (1-\alpha)\overline{\mu}) + \alpha\gamma$, which is higher than that of the firm. This is because the social planner also takes into account consumers' cost of taking precautions ($\alpha\gamma$) when choosing the socially efficient investments.

[18] When consumers do not take precaution, the firm would strictly prefer not to disclose because disclosure would increase the probability of attack by ϵ.

[19] The disclosure stage is not critical to my analysis because the firm's private incentive to disclose is aligned with social incentive to disclose, but including the disclosure stage is meant to highlight the robustness and general nature of my results. An open question for future research is how, under moral hazard, firm's disclosure decision could signal its effort about security investments.

Moreover, the social planner internalizes all the society's costs, so there is no liability issue. In case of non-disclosure, the expected cost is $p(s)(\underline{\eta}+\overline{\mu})$.

The social planner chooses s and b to minimize the expected loss of the society, which is denoted by $\mathcal{L}^{SP}$.

$$\begin{aligned}\min_{b,s}\mathcal{L}^{SP} =&(1-b)p(s)(\overline{\eta}+\overline{\mu})+b\left\{\int_0^{p(s)(\overline{\mu}-\underline{\mu})}[p(s)(\underline{\eta}+\alpha\underline{\mu}+(1-\alpha)\overline{\mu})+\alpha\gamma]dF(\gamma)\right.\\ &\left.+\int_{p(s)(\overline{\mu}-\underline{\mu})}^{\infty}p(s)(\underline{\eta}+\overline{\mu})dF(\gamma)\right\}+m(b)+c(s)\\ =&\mathcal{L}^{f}|_{\lambda=1}+b\alpha\int_0^{p(s)(\overline{\mu}-\underline{\mu})}\gamma dF(\gamma). \qquad (3)\end{aligned}$$

Let $b^{SP}(s)$ denote the social planner's optimal damage-control investment strategy given attack-deterring investment s, and let s^o and $b^o \equiv b^{SP}(s^o)$ denote the solutions of Equation (3).

The difference between $\mathcal{L}^f$ and $\mathcal{L}^{SP}$ is that the firm minimizes its own private costs, while the social planner minimizes the sum of firm's and consumers' costs.

Lemma 1. *Under full liability ($\lambda = 1$), $b^m(s)$ and $b^{SP}(s)$ decrease with s.*

Proof. See Appendix B. □

Lemma 1 shows that the firm has less incentive to find bugs given a high security level for attack deterrence, meaning that attack-deterring and damage-control investments are substitutes.

Lemma 2. *Under full liability ($\lambda = 1$), $b^m(s) > b^{SP}(s)$ for all s. In particular, if the standard is set at the socially optimal level, $s^* = s^o$, the firm will overinvest in damage control, $b^m(s^o) > b^{SP}(s^o)$.*

Proof. See Appendix C. □

One might expect that under full liability and an optimal standard the firm will invest optimally, but it turns out differently when consumers also bear some costs in protecting their computers. The intuition runs as follows. If a bug is not found, both the firm and the society suffer the same magnitude of heavy losses because hackers can exploit a bug fully before it is patched by developers and since the bug is not identified, consumers cannot take any precautionary actions to reduce damage. If a bug is discovered, the firm suffers less damage than the social planner because once a problem is disclosed consumers can employ various defenses against online attacks. However, since the firm decides on the amount of investment to minimize its own private costs, it will ignore the precautionary costs on the part of consumers, whereas the social planner minimizes the sum of these costs. Because the firm has more to gain in finding bugs, it will overinvest with respect to the socially efficient level.

I assume that full liability is defined for "net" damages to the consumers. One can alternatively define it for "total" damages, which includes also consumers' precaution cost. In this case, full liability alone is enough to restore the first-best. I model the liability regime the

way I did because in practice, firms are typically liable for financial damages to the consumers caused by, for example, a data breach. Liability sometimes also covers for litigation costs,[20] but very rarely for investment costs in precaution. One difficulty lies in estimating the amount of time and effort consumers spent on managing, maintaining and patching a system.

Proposition 1. *(Full Liability with Fines). Under full liability* ($\lambda = 1$)*, under which the firm must pay a fine to the regulator for all the damages caused, the firm underinvests in attack deterrence,* $s^* < s^o$*, and overinvests in damage control,* $b^* > b^o$*.*

Proof. See Appendix D. □

Proposition 1 shows that full liability alone does not achieve the first-best solution. The reason is that, as shown in Lemma 2, the firm has more to gain in finding the bug than the social planner, and hence it invests too much in damage control. The firm invests too little in attack deterrence because it expects to overinvest in damage control, as was shown in Lemma 1. Furthermore, in Appendix F, I show that if liability regime is the only instrument of public policies, neither liability regime (full, partial or zero) is not enough to provide the right incentives for two investments.

Proposition 2. *(Partial Liability). The socially optimal level of investment,* s^o *and* b^o*, can be achieved with the joint use of an optimal standard* s^o *and a partial liability rule* $\lambda \in (0, 1)$*.*

Proof. See Appendix E. □

When security standards are set at the socially optimal level, it is inefficient to implement full liability because the firm will overinvest in damage control; it is also inefficient to set firm's liability to zero because it will then underinvest in damage control. As a consequence, the optimal liability rule is a partial one.

This result is related to Brown's (1973) work on bilateral care model, wherein he finds that "strict liability with a defense of contributory negligence" (i.e. the firm is strictly liable unless the consumer is negligent) supports the socially efficient outcome. Although a direct comparison with his model is difficult because I did not model negligence explicitly,[21] it would be useful to understand why different rules lead to optimality. More particularly, I find that strict liability, with and without a standard, do not achieve efficiency, but instead partial liability and an optimal standard do, both for the cases with fine (this section) and with reimbursement (Section 4.3). The main difference between this model and Brown's model is that in Brown's model both parties (the firm and the consumer) choose one type of care,

[20] Incorporating litigations in the model would not change my qualitative results since in the alternative model the expected damage faced by consumers will change from μ to the probability of losing the litigation times μ, whereas the firm's expected liability will become its probability of losing the litigation times λ times μ; all that matters is the magnitude.

[21] Negligence is not the main focus of my model because it is generally less costly for the courts to define a negligence system when the firm can undertake one type of investment compared to the case with two types of investments. Since in the latter case, the firm may be negligent in deterring attacks, in reducing damage or in both. It would then be difficult to define whether the firm should be judged negligent if it violates one due care standard but meets the other one.

whereas in this model one party (the firm) chooses two types of care. In his model, under strict liability with a defense of contributory negligence, both parties will exert the right level of care. Because the firm is liable for all losses sustained by consumers, it is led to choose the correct level of care. Moreover, consumers, knowing that they have to bear their losses if they are negligent (meaning that they fail to meet the due care standard), will also exercise due care. However, with one more type of investment on firm's side, I find that the joint use of full liability and an optimal standard would generate inefficient investments for reasons discussed before (see Lemma 2).

3.1 Policy Implications: standards and partial liability

Proposition 2 shows that security can be improved with the joint use of an optimal standard and a partial liability rule. For standards, they can either be implemented by the legal system as negligence rules, under which the party who does not comply with the due care standard chosen by courts will be penalized, or by a separate regulatory agency. Such agency can establish minimum standards for IT security (such as a mandatory compliance framework in encryption and security breach notification) as other already regulated industries like automotive and aviation, where new models of car and aircraft must pass some safety tests conducted by international or national regulatory bodies before they are allowed on the road or in the air.

As for liability rules, the system of tort law can implement them. I find that, given an optimal standard, shifting some liability to the consumers is welfare improving. This means that the regulator should not impose a one hundred percent liability on the software vendor because this will distort its investment incentives. Instead, an effective policy is to ask both the software vendor and its customers to share the costs of security.[22]

On individual level, despite the fact that users dislike or feel concerned about security problems, many of them do not take appropriate care to prevent insecurity: they ignore breach notification letters, they do not patch their machines, and use simple passwords. In the case of ChoicePoint's data breach, for instance, more than 90% of the customers whose personal information had been stolen did not take up the mitigating solutions (such as free credit monitoring service and insurance) proposed by ChoicePoint.[23] One reason for this may be that consumers have other competing demands on their time, and paying attention to security advice appears to be low on their priority list. Thus, it seems reasonable to promote cybersecurity awareness among home users so they will begin to take more precautions to protect themselves. As another example, because of the hassle of remembering strong and multiple passwords, many users use easy-to-remember passwords and reuse the same credentials across websites. Thus, another way to incentivize users to change their behavior is to promote the development and

[22]Although this discussion interprets costs of security as a form of liability, they are different from the costs explained by γ in that consumers ignoring or not noticing security alerts is not an investment, but rather it shows a systematic lack of security consciousness. This raises the question of who should be responsible for the damages that arise from such negligence.

[23]See Jon Brodkin, "Victims of ChoicePoint Data Breach Didn't Take Advantage of Free Offers," *Network World*, April 10, 2007, `http://www.networkworld.com/news/2007/041007-choicepoint-victim-offers.html?page=1`.

the adoption of password managers, which can generate and store unique passwords, thereby saving on users' hassle costs.

On enterprise level, installing patches could be time- and resource-consuming, especially for large companies, because the plethora of security updates can often overwhelm software engineers, who have to keep track of all relevant bugs and patches, and match the version of all those updates to versions of software their company is using. Once a problem is identified, they need to figure out which updates get priority, and look for solutions to deal with it.[24] As a consequence, few companies can apply updates in a timely manner, which easily leads to the missing of some major security problems. This suggests that a desirable policy should try to eliminate the delay in applying the solutions to security problems. First, the government could persuade or mandate the users to react more quickly (for example, within a predetermined window of time) as soon as the vendor makes the solutions available and notifies them in a reasonable way. Second, third parties can be introduced to help enterprises to find, select and deploy the solutions that are relevant to their systems. For example, using the cloud computing technology, firms could outsource security activities to external providers by moving part of the business processes to the cloud. Qualys, Inc., a vulnerability management company that helps businesses to adhere to compliance and security standards in the IT and financial sectors, provides another example.

3.2 Network Externality

In this subsection, I consider direct and indirect network effects in turn. Direct network effects are common in cybersecurity because one compromised system may affect many other users, for example, attackers can steal millions of credit card details from a compromised e-commerce website or they can use the infected system to host phishing sites, distribute spam e-mails or other unlawful content. Kunreuther and Heal (2003), August and Tunca (2006), Acemoglu et al. (2013), and Riordan (2014), for instance, examine agents' incentive to invest in security in the presence of network externalities. While they focus on one type of security investment, this paper deals with two types.[25]

In the previous analysis, I have assumed that there are no direct network effects, but my qualitative results would not change even if we add this. Re-interpreting damage-control investment as a patch release and consumers' action as the choice of patch installation, direct

[24]Practitioners have commonly considered patch management as a time- and resource-consuming activity. See "Automating Patch Management," *Symantec*, February 8, 2005, available at `http://www.symantec.com/articles/article.jsp?aid=automating_patch_management`. On average, firms spend 600 hours per week on the malware containment process. See "Four in five malware alerts are a 'waste of time'," *ZDNet*, January 19, 2015, available at `http://www.zdnet.com/article/businesses-waste-1-3m-a-year-on-false-malware-alarms/?tag=nl.e552&s_cid=e552&ttag=e552&ftag=TRE3e6936e`.

[25]More particularly, August and Tunca (2006) focus on the problem of patch management, and therefore consider damage-control investment only. Security investments are strategic complements in Kunreuther and Heal (2003), strategic substitutes in Acemoglu et al. (2013), and can be strategic complements or strategic substitutes in Riordan (2014) depending on whether the attacks are direct or indirect, but agents can only invest once in these models.

network effects between consumers could arise when consumers who do not patch increase the security risks on other consumers, and consumers who patch reduce the probability of others being attacked. In this case, increasing the proportion of experts α will lower the damage to all experts, $\underline{\mu}$, and that to all laymen, $\overline{\mu}$, meaning only magnitude changes. However, the main qualitative result of liability-sharing between the firm and the consumers remains valid, provided consumers have to take precautionary actions.

Indirect network effects exist as well because the software vendor's investment strategy is affected by the proportion of consumers taking precaution. In this model, α can be interpreted as a measure of indirect network effect.

Corollary 1. *(Indirect network effects). When λ is large, increasing the proportion of computer experts, α, exacerbates underinvestment in attack deterrence and overinvestment in damage control.*

Proof. See Appendix G. □

The intuition behind Corollary 1 runs as follows. Comparing Equations (2) with (3), for a given s the difference between the private and social incentives to invest that is related to α arises from the following.

$$p(s) \underbrace{(1-\lambda)(\alpha\underline{\mu}+(1-\alpha)\overline{\mu})}_{\text{distortion from liability assignment}} + \underbrace{\alpha\gamma}_{\text{distortion from consumers' costs}}.$$

Investment incentives are distorted by two forces: first, the firm does not pay fully for the damage; second, the firm ignores the precautionary costs of the consumers when it makes its investment decision. If the firm is held liable for a large proportion of damage (i.e. λ is large), then reducing the proportion of experts (α) mitigates suboptimal investment incentives. The reason is that an increase in firm's liability reduces the first type of distortion, whereas a decrease in the proportion of experts reduces the second type of distortion. Taking the effects together, the objectives of the social planner and the firm become more aligned, and thus a decrease in α reduces the extent that the firm is investing suboptimally.[26]

As for social welfare, it is easy to see from Equation (3) that an increase in the proportion of experts leads to a decrease in society's loss. This suggests that if the primary objective of the government is to improve social welfare, policymakers can provide support and training in the area of cybersecurity so that users become more competent in managing security threats. For example, many security breaches involve attackers trying to compromise users' accounts, and users are sometimes unaware of such attack. Even if they are aware of the attack, they sometimes lack the skills needed to resolve the security problem. Cisco forecasted that there will be a global shortage of IT security professionals that are needed to cope with cyber threats in both public and private sectors.[27] Therefore, increasing training that aims at enhancing

[26] If λ is small, the firm, knowing that they are only liable for a small part of the damage, may underinvest in both attack deterrence and damage control. The effect of α is then difficult to generalize because it depends on not only λ, but also s^*, s^o, b^* and b^o.

[27] See "Cybersecurity's hiring crisis: A troubling trajectory," *ZDNet*, August 25 2014, available at `http://www.zdnet.com/cybersecuritys-hiring-crisis-a-troubling-trajectory-7000032923/?s_cid=e552&ttag=e552&ftag=TRE3e6936e`.

specific engineering skills of these users appears to be appropriate, provided that the training costs are not too large. Further, earlier intervention before young people enter the labor market might be appropriate. The government in the UK, for instance, is trying to improve the IT curriculum at all levels of education to address IT skills shortages.[28] At primary and secondary levels, the Raspberry Pi, which is a bare-bones computer developed in the UK by the Raspberry Pi Foundation, improves the coding incentives of young students by giving them the opportunity to learn how to write the code that makes the software work rather than learning how to use the software created by other engineers. At university level, schools offer more master classes and on-the-job practical trainings in computer science.[29] This kind of policy makes sense if the government's aim is to enhance welfare. However, if the goal is to alleviate investment inefficiency, the government needs to be careful about increasing the number of experts because the objectives of the social planner and the firm would further diverge. That being said, this does not mean that offering cybersecurity training is undesirable (e.g. it could potentially generate cost savings for firms through detecting, defending against and recovering from cyber-attacks), but that the potential adverse effects on incentives should not be ignored.

4 Discussion

This section discusses alternative interpretations of this model and, in particular, how the underinvestment and overinvestment results can be used to explain real-world security issues in IT and in other industries where firms undertake two investments, and how to address these issues by implementing alternative policies, such as reimbursing consumers instead of imposing fines.

4.1 Vaporware

"Vaporware" refers to the software industry practice of announcing new products well in advance of their actual release on the market.[30] The previous literature, for instance, Bayus et al. (2001) and Haan (2003), studies how such product pre-announcements can be used as a means of entry deterrence in a signaling model. Choi et al. (2010b) examine how reputation concerns may induce firms to make honest announcements in a repeated cheap-talk game. Although vaporware practice typically means the release dates of the products are much later than the original announced dates, we could alternatively view the announced product as a product characteristics (a security feature, for instance) instead of the physical product. Vaporware could then be interpreted as delivering a lower-quality product compared to the standard set by some regulatory agencies or bodies of law, which is consistent with the current development in the industry: software firms often "experiment" the alpha versions of their products (e.g.

[28] See "UK recovery 'constrained' by lack of engineers," *BBC News*, November 4 2014, available at `http://www.bbc.com/news/education-24779016`.

[29] See "Degree apprenticeships launched to boost hi-tech skills," *BBC News*, November 26 2014, available at `http://www.bbc.com/news/education-30193095`.

[30] Vaporware may also mean the announced products never reach the market, but this is not the focus of this paper because the firm always introduces the product in this model.

software, mobile applications, and smart-home appliances) in public and release improved beta versions at a later date. Thus, alpha versions of many software products are susceptible to security risks. The result of underinvestment in attack deterrence in this model captures the essence of this situation. Moreover, I show that vaporware practice (underinvestment in attack deterrence/the release of lower quality software) is in fact a profit-maximizing strategy for the firm, and it may occur even in the absence of preemptive motives and reputation concerns. This is therefore different from the vaporware literature, where firms engage in vaporware only to prevent entry or when reputational concern is not so important. The new insight here is that the possibility of sequential investments, which allows the firm also to fix security problems later, provides an alternative explanation at least in part for vaporware practice in the software market.

4.2 More General Applications

The analysis also provides insight into other industries in which sequential investments are important, such as automobiles. We can then re-interpret the seller as a firm that produces a product with some safety features. There are again two types of investments the firm can undertake: first investment in pre-sale product design and second investment in post-sale remedial measures. For example, the pre-sale investment could lead to the development of a new technology in cars that is subject to potential safety defect. After sale, the firm can invest in remedying these safety problems. It is, for instance, common to observe product recalls because of problems in engines or braking in the car industry. Note that, however, in the car industry, there is generally a stricter compliance framework for producers compared to the software industry, and thus vaporware, the practice of announcing a product well in advance of its actual release, is less of an issue.

Other examples include employers making the first investment in safety technology that reduces risks at workplace and prevents injuries of their employees, and the second investment in fixing any problems arising from actual injuries and replacing equipment that is worn out with usage; firms building a factory that may generate harm (e.g. pollution and radiation) to residents who live nearby, and they have to first decide on the amount of precautions to take in factory design and then decide on the level of care it takes in regular inspection of the facility. With these re-interpretations, this model would be useful for studying investment incentives of different parties, in particular whether there are incorrect incentives to deter the occurrence of harm and to reduce damage on the part of the injurer, and to take precautionary action on the part of potential victims, as well as how to correct them.

4.3 Reimbursement

Up to now, we have interpreted liability as a fine, which does not affect consumer's precautionary behavior. Now suppose that the firm, instead of paying a fine to courts for a proportion λ of the damage, is required to reimburse consumers an amount specified by one of the liability regimes. Let ρ denote the refund that returns to the pockets of consumers, which can be equal to or smaller than consumers' damage level. I show that

Proposition 3. *(Full Liability with Reimbursements). Under full refund ($\rho = 1$), under which the firm must reimburse fully to a consumer for damage caused, the firm overinvests in attack deterrence, $s^* > s^o$, and underinvests in damage control, $b^* < b^o$.*

Proof. See Appendix H. □

Under full reimbursement, if a bug is not found, both the firm and the society suffer the same loss. However, if a bug is found, consumers, knowing that they will be fully reimbursed anyway, have no incentive to take precaution in equilibrium, whereas under social optimum some consumers (the experts in particular) will take precaution when the benefit of an increase in precautionary action outweighs the cost. The benefit of investing in b for the firm is therefore lower compared to that of the social planner. Consequently, the firm underinvests in damage control. And since attack-deterring and damage-control investments are substitutes, the firm overinvests in attack deterrence.

The banking sector is a case in point. Financial institutions invest a large amount of money in developing new technologies that defend their consumers against password theft, but much less in damage reduction because tracing suspicious money transfers from one bank account to another is relatively easier than preventing password-stealing attacks in the first place.

It is also straightforward to show Proposition 2 remains valid in the case with reimbursement. Although different instruments (a fine or a reimbursement) yields different investment incentives, in both cases a partial liability rule results in the socially efficient outcome. This suggests that when both the firm and the consumers can invest in security and the firm can undertake two types of investments, it would be useful for policymakers to think about passing some liability to consumers instead of adopting either full or zero liability rules, and about whether a fine or a reimbursement is the more appropriate regulatory instrument.

5 Conclusion

More and more devices, such as mobile phones, home appliances, health devices, cars, and even some infrastructures (e.g. traffic lights), become Internet connected, but we continue to discover security failures, including malware (e.g. ransomware, chargeware and adware), poor encryption and backdoors that allow unauthorized access. This paper suggests that to increase security, the key is not so much about holding the seller of these devices solely liable for the loss, but balancing the investment incentives between the firm and the consumers.

In practice, there are few policies regulating the software industry compared to financial services and transportation. Establishing national or international regulatory body to implement security standards for Internet-connected devices and updating existing regulations to ensure that only products with adequate defenses against attacks can be released on the market could represent a useful start. For example, Finland has passed a new legislation, the "Information Society Code", at the beginning of 2015, which enforces security standards on a wide range of platforms such as Apple, Facebook and Twitter.

In future work, it would be interesting to relax the single-firm assumption and study competition between software vendors. The possibility of interdependencies between software prod-

ucts may lead to interesting dynamics between firms, and investment incentives may be different depending on whether firms' investments are substitutes. Alternatively, one could study contagion issues in a network of multiple firms.[31]

Appendices

A Continuum of Consumers

With a slight abuse of the notation, suppose that there is a continuum of consumers whose precaution cost γ is drawn from a distribution $F(\gamma) \sim [0, +\infty)$. As before, consumers will take precaution if $\gamma < p(s)(\overline{\mu} - \underline{\mu})$, and the marginal consumer, who is indifferent between taking and not taking precaution, is given by $\gamma(s) \equiv p(s)(\overline{\mu} - \underline{\mu})$.

If the firm does not disclose the bug, its expected cost is $p(s)(\underline{\eta} + \lambda\overline{\mu})$; if it discloses the bug, it expected cost is $p(s)[\underline{\eta} + \lambda(F(\gamma(s))\underline{\mu} + (1 - F(\gamma(s)))\overline{\mu})]$. Since the latter is smaller than the former, the firm will always disclose. Therefore, the firm chooses s and b to minimize

$$\min_{b,s} \mathcal{L}^f = (1-b)p(s)(\overline{\eta} + \lambda\overline{\mu}) + bp(s)[\underline{\eta} + \lambda(F(\gamma(s))\underline{\mu} + (1 - F(\gamma(s)))\overline{\mu})] + m(b) + c(s). \quad \text{(A.1)}$$

As for the social planner, the cost for non-disclosure is $p(s)(\underline{\eta} + \overline{\mu})$, whereas the cost for disclosure is $p(s)[\underline{\eta} + F(\gamma(s))\underline{\mu} + (1 - F(\gamma(s)))\overline{\mu}] + \int_0^{\gamma(s)} \gamma dF(\gamma)$. Since the latter is smaller than the former, the social planner will always disclose. The social planner therefore solves

$$\begin{aligned}\min_{b,s} \mathcal{L}^{SP} = {} & (1-b)p(s)(\overline{\eta} + \overline{\mu}) \\ & + b\left\{p(s)[\underline{\eta} + F(\gamma(s))\underline{\mu} + (1 - F(\gamma(s)))\overline{\mu}] + \int_0^{\gamma(s)} \gamma dF(\gamma)\right\} + m(b) + c(s). \quad \text{(A.2)}\end{aligned}$$

It is easy to see that since $\int_0^{\gamma(s)} \gamma dF(\gamma) > 0$, $\mathcal{L}^{SP} > \mathcal{L}^f$ for any λ. Thus, the main results of underinvestment in attack deterrence and overinvestment in damage control carry through.

B Proof of Lemma 1

Since $\lambda = 1$, the first-order conditions with respect to b are given by

$$\begin{aligned}\frac{\partial \mathcal{L}^{SP}}{\partial b} &= 0, \\ \Leftrightarrow m'(b) &= p(s)(\overline{\eta} + \overline{\mu}) - \underbrace{\int_0^{p(s)(\overline{\mu}-\underline{\mu})} [p(s)(\underline{\eta} + \alpha\underline{\mu} + (1-\alpha)\overline{\mu}) + \alpha\gamma] dF(\gamma)}_{G^{SP}(s)} \\ &\quad - \int_{p(s)(\overline{\mu}-\underline{\mu})}^{\infty} p(s)(\underline{\eta} + \overline{\mu}) dF(\gamma), \quad \text{(B.1)}\end{aligned}$$

[31] See, for instance, Morris (2000), Acemoglu et al. (2013), and Goyal et al. (2014) for treatment of contagion in networks.

and

$$\begin{aligned}
\frac{\partial \mathcal{L}^f}{\partial b} &= 0, \\
\Leftrightarrow m'(b) &= p(s)(\overline{\eta}+\overline{\mu}) - \underbrace{\int_0^{p(s)(\overline{\mu}-\underline{\mu})} p(s)(\underline{\eta}+\alpha\underline{\mu}+(1-\alpha)\overline{\mu})dF(\gamma)}_{G^f(s)} \\
&\quad - \int_{p(s)(\overline{\mu}-\underline{\mu})}^{\infty} p(s)(\underline{\eta}+\overline{\mu})dF(\gamma). \qquad \text{(B.2)}
\end{aligned}$$

The right hand sides of Equations (B.1) and (B.2) are decreasing in s.

C Proof of Lemma 2

We can see from Equations (B.1) and (B.2) that if $s^* = s^o$, then $G^f(s^o) < G^{SP}(s^o)$. Thus, $b^m(s^o) > b^{SP}(s^o)$.

D Proof of Proposition 1

Since $\lambda = 1$, the first-order conditions with respect to s are given by

$$\begin{aligned}
\frac{\partial \mathcal{L}^{SP}}{\partial s} &= 0, \\
\Leftrightarrow -\frac{c'(s)}{p'(s)} &= (1-b)(\overline{\eta}+\overline{\mu}) + b\left[\int_0^{p(s)(\overline{\mu}-\underline{\mu})} (\underline{\eta}+\alpha\underline{\mu}+(1-\alpha)\overline{\mu})dF(\gamma)\right. \\
&\quad \left. + \int_{p(s)(\overline{\mu}-\underline{\mu})}^{\infty} (\underline{\eta}+\overline{\mu})dF(\gamma)\right], \qquad \text{(D.1)}
\end{aligned}$$

and

$$\begin{aligned}
\frac{\partial \mathcal{L}^f}{\partial s} &= 0, \\
\Leftrightarrow -\frac{c'(s)}{p'(s)} &= (1-b)(\overline{\eta}+\overline{\mu}) + b\left[\int_0^{p(s)(\overline{\mu}-\underline{\mu})} (\underline{\eta}+\alpha\underline{\mu}+(1-\alpha)\overline{\mu})dF(\gamma)\right. \\
&\quad \left. + \int_{p(s)(\overline{\mu}-\underline{\mu})}^{\infty} (\underline{\eta}+\overline{\mu})dF(\gamma) - \alpha p(s)(\overline{\mu}-\underline{\mu})^2 f(p(s)(\overline{\mu}-\underline{\mu}))\right]. \qquad \text{(D.2)}
\end{aligned}$$

Define the right hand side of Equation (D.1) as $H^{SP}(b)$, and that of Equation (D.2) as $H^f(b)$. Clearly, the left hand sides of Equations (D.1) and (D.2) are equal. However, $H^{SP}(b^{SP}(s)) > H^f(b^{SP}(s)) > H^f(b^m(s))$. The first inequality follows from $H^{SP}(b) > H^f(b)$ for any b, whereas the second inequality is due to the fact that $H^f(b)$ is decreasing in b.

Since $c'''(s) > 0$ and $p'''(s) > 0$, it is easy to see that $-c'(s)/p'(s)$ is convex and increasing in s, and it has the limits $\lim_{s\to 0} -c'(s)/p'(s) = 0$ and $\lim_{s\to\infty} -c'(s)/p'(s) = \infty$. As for the right hand sides, the limits of both $H^{SP}(b)$ and $H^f(b)$ are bounded away from ∞ as s tends to ∞. Moreover, $H^{SP}(0) > 0$, and if $H^f(0) > 0$, the solution to both equations exists, and

we denote them by s^* and s^o respectively. In addition, if the solution is unique, we must have $s^* < s^o$ due to the fact that $H^{SP}(b^{SP}(s)) > H^f(b^m(s))$.[32]

Using Lemma 1, if $s^* < s^o$, then $b^* > b^o$.

E Proof of Proposition 2

Suppose $s^* = s^o$. If $\lambda = 1$, Lemma 2 implies $b^m(s^o) > b^{SP}(s^o)$. If $\lambda = 0$, Equation (B.2) becomes

$$m'(b) = p(s)(\overline{\eta} - \underline{\eta}).$$

Comparing with Equation (B.1), $b^m(s^o) < b^{SP}(s^o)$. Therefore, there exists $\lambda \in (0,1)$ such that $b^m(s^o) = b^{SP}(s^o)$.

F Liability regime as the only instrument

Suppose that there exists $\lambda \in [0,1]$ such that $b^* = b^o$ and $s^* = s^o$. This implies that $\partial \mathcal{L}^f / \partial b = \partial \mathcal{L}^{SP} / \partial b$ and $\partial \mathcal{L}^f / \partial s = \partial \mathcal{L}^{SP} / \partial s$. However, we can easily verify that these two conditions cannot be satisfied at the same time.

G Proof of Corollary 1

The difference between Equations (B.1) and (B.2) is

$$m'(b^*) - m'(b^o) = \alpha \int_0^{p(s)(\overline{\mu}-\underline{\mu})} \gamma dF(\gamma),$$

which is positive and increasing in α, meaning that a larger α worsens overinvestment in damage control.

Similarly, the difference between Equations (D.1) and (D.2) is

$$(b^* - b^o)\left[\int_0^{p(s)(\overline{\mu}-\underline{\mu})} (\underline{\eta} + \alpha\underline{\mu} + (1-\alpha)\overline{\mu}) dF(\gamma) + \int_{p(s)(\overline{\mu}-\underline{\mu})}^{\infty} (\underline{\eta} + \overline{\mu}) dF(\gamma) - (\overline{\eta} + \overline{\mu})\right] - \alpha b^* p(s)(\overline{\mu} - \underline{\mu})^2 f(p(s)(\overline{\mu} - \underline{\mu})).$$

The first term $(b^* - b^o)$ is positive and increasing in α, and the term in the square bracket is negative and decreasing in α. The product of these two terms is thus negative and decreasing α. Since the final term $-\alpha b^* p(s)(\overline{\mu} - \underline{\mu})^2 f(p(s)(\overline{\mu} - \underline{\mu}))$ is also negative and decreasing in α, taken together the difference between Equations (D.1) and (D.2) is negative and decreasing in α, meaning that underinvestment in attack deterrence is more severe as α increases.

This proof remains valid as long as λ is large enough.

[32] For example, there exists a unique equilibrium investment when both $F(p(s))$ and $p(s)f(p(s))$ are convex, and $m(b)$ is quadratic.

H Proof of Proposition 3

First, with reimbursement, the problem for the social planner is the same as in the case with fine. The social planner will ask the experts to take precaution if the cost of an increase in precautionary action is less than the marginal benefit of reducing damage, i.e. when Equation (1) is satisfied.

In the market equilibrium, when consumers are reimbursed fully for all damages, their incentives to take precaution are weakened. More specifically, a consumer now takes precautionary action if

$$\gamma < (1-\rho)p(s)(\bar{\mu}-\underline{\mu}).$$

Thus, the firm chooses s and b to minimize

$$\begin{aligned}\min_{b,s} \mathcal{L}_r^f &= (1-b)p(s)(\overline{\eta}+\rho\overline{\mu}) \\ &+ b\left\{\int_0^{(1-\rho)p(s)(\overline{\mu}-\underline{\mu})} p(s)[\underline{\eta}+\rho(\alpha\underline{\mu}+(1-\alpha)\overline{\mu})]dF(\gamma) + \int_{(1-\rho)p(s)(\overline{\mu}-\underline{\mu})}^{\infty} p(s)(\underline{\eta}+\rho\overline{\mu})dF(\gamma)\right\} \\ &+ m(b) + c(s), \quad \text{(H.1)}\end{aligned}$$

where subscript r denotes the case of reimbursement. The difference between Equation (2) in the main text (the case with fine) and the equation above (the case with reimbursement) lies in the boundaries of the integrals.

The first-order condition with respect to b (when $\rho = 1$) for the firm is

$$m'(b) = p(s)(\overline{\eta}+\overline{\mu}) - \int_0^{\infty} p(s)(\underline{\eta}+\overline{\mu})dF(\gamma). \quad \text{(H.2)}$$

In comparison with the first-order condition with respect to b for the social planner (see Equation (B.1)), it is clear that for a given s, the marginal benefit of investing in b for the firm is always lower than that of the social planner. Therefore, the firm underinvests in damage control.

As for the incentive to invest in attack deterrence, the first order condition with respect to s for the firm is

$$\frac{c'(s)}{p'(s)} = (1-b)(\overline{\eta}+\overline{\mu}) + b(\underline{\eta}+\overline{\mu}). \quad \text{(H.3)}$$

Comparing it with the first-order condition with respect to s for the social planner (see Equation (D.1)), it is easy to see that for a given b, the right hand side of the Equation (H.3) for the firm is always higher than that of the social planner. Using the same assumptions as in Proposition 1, the firm will overinvest in attack deterrence.

References

[1] Daron Acemoglu, Azarakhsh Malekian, and Asu Ozdaglar. Network Security and Contagion. MIT Working Paper, 2013.

[2] Ross Anderson, Richard Clayton, and Tyler Moore. The Economics of Online Crime. *Journal of Economic Perspectives*, 23(3):3–20, 2009.

[3] Ross Anderson and Tyler Moore. Information Security: Where Computer Science, Economics and Psychology Meet. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, 367(1898):2717–2727, 2009.

[4] Ashish Arora, Anand Nandkumar, and Rahul Telang. Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers*, 8(5):350–362, 2006.

[5] Terrence August and Tunay Tunca. Network Software Security and User Incentives. *Management Science*, 52(11):1703–1720, 2006.

[6] Terrence August and Tunay Tunca. Who Should Be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments. *Management Science*, 57(5):934–959, 2011.

[7] Barry Bayus, Sanjay Jain, and Ambar Rao. Truth or Consequences: An Analysis of Vaporware and New Product Announcements. *Journal of Marketing Research*, 38(1):3–13, 2001.

[8] Paul Belleflamme and Martin Peitz. Marketing tools for experience goods. In *Industrial Organization: Markets and Strategies*, chapter 13, pages 309–330. Cambridge University Press, 2010.

[9] Rainer Böhme. Security Metrics and Security Investment Models. In Isao Echizen, Noboru Kunihiro, and Ryoichi Sasaki, editors, *Advances in Information and Computer Security, Lecture Notes in Computer Science*, volume 6434, pages 10–24. Springer Berlin Heidelberg, 2010.

[10] John Brown. Toward an Economic Theory of Liability. *Journal of Legal Studies*, 2(2):323–349, 1973.

[11] Jay Pil Choi, Chaim Fershtman, and Neil Gandal. Network Security: Vulnerabilities and Disclosure Policy. *Journal of Industrial Economics*, 58(4):868–894, 2010a.

[12] Jay Pil Choi, Eirik Kristiansen, and Jae Nahm. Vaporware. *International Economic Review*, 51(3):653–669, 2010b.

[13] Russell Cooper and Thomas Ross. Product Warranties and Double Moral Hazard. *RAND Journal of Economics*, 16(1):103–113, 1985.

[14] Andrew Daughety and Jennifer Reinganum. Product Safety: Liability, R&D and Signaling. *American Economic Review*, 85(5):1187–1206, 1995.

[15] Andrew Daughety and Jennifer Reinganum. Secrecy and Safety. *American Economic Review*, 95(4):1074–1091, 2005.

[16] Andrew Daughety and Jennifer Reinganum. Markets, Torts and Social Inefficiency. *RAND Journal of Economics*, 37(2):300–323, 2006.

[17] Andrew Daughety and Jennifer Reinganum. Cumulative Harm, Products Liability, and Bilateral Care. *American Law and Economics Review*, 15(2):409–442, 2013a.

[18] Andrew Daughety and Jennifer Reinganum. Economic Analysis of Products Liability: Theory. In Jennifer Arlen, editor, *Research Handbook on the Economics of Torts*, chapter 3, pages 69–96. Edward Elgar Publishing Ltd., 2013b.

[19] Lawrence Gordon and Martin Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4):438–457, 2002.

[20] Sanjeev Goyal, Hoda Hiedari, and Michael Kearns. Competitive Contagion in Networks. *Games and Economic Behavior*, 2014, forthcoming.

[21] Jennifer Granick. The Price of Restricting Vulnerability Publications. *International Journal of Communications Law & Policy*, 9:1–35, 2005.

[22] Marco Haan. Vaporware as a Means of Entry Deterrence. *Journal of Industrial Economics*, 51(3):345–358, 2003.

[23] Charles Kolstad, Thomas Ulen, and Gary Johnson. Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements? *American Economic Review*, 80(4):888–901, 1990.

[24] Howard Kunreuther and Geoffrey Heal. Interdependent Security. *Journal of Risk and Uncertainty*, 26(2-3):231–249, 2003.

[25] William Landes and Richard Posner. A Positive Economic Analysis of Products Liability. *Journal of Legal Studies*, 14(3):535–567, 1985.

[26] Stephen Morris. Contagion. *Review of Economic Studies*, 67(1):57–78, 2000.

[27] A. Mitchell Polinsky and Steven Shavell. Mandatory Versus Voluntary Disclosure of Product Risks. *Journal of Law, Economics, & Organization*, 28(2):360–379, 2010.

[28] Michael Riordan. Economic Incentives for Security. Powerpoint Slides presented at Cybercriminality Seminar at Toulouse School of Economics on 4 June, 2014.

[29] Steven Shavell. Strict Liability versus Negligence. *Journal of Legal Studies*, 9(1):1–25, 1980.

[30] Steven Shavell. A Model of the Optimal Use of Liability and Safety Regulation. *RAND Journal of Economics*, 15(2):271–280, 1984.

[31] Steven Shavell. Liability for Accidents. The New Palgrave Dictionary of Economics, 2008. Available at `http://www.law.harvard.edu/faculty/shavell/pdf/124_liability.pdf` (accessed 26 October, 2014).

[32] Hal Varian. System Reliability and Free Riding, 2004. Available at http://people.ischool.berkeley.edu/~hal/Papers/2004/reliability (accessed 1 December, 2013).