The Philippine Review of Economics
Vol. LI No. 1, June 2014 pp. 84–116

Optimal solution to cybercrimes: lessons from law and economics

Ruperto P. Majuca

A model is presented wherein cybercrimes are addressed through a combination of private and public measures. This captures the substitutability of private and public responses and determines the optimal combination of these approaches. The socially optimal level of security is achieved by equalizing the marginal-benefit-to-marginal-cost ratios of each of the three alternatives: private security investment, nonrivalrous security investment, and law enforcement measures. The interrelatedness of Internet risks causes individual firms to underinvest in private and public security goods. The government thus lowers the level of police enforcement expenditures to induce firms to invest more in individual precautions. In certain conditions, cooperation results in socially optimal levels of expenditures in private and public security goods. The Shapley [1953] value can be used as a criterion for allocating the costs and benefits among the members of a security cooperative.

JEL classification: K0
Keywords: law and economics, cybersecurity, interrelated risks, public goods, law enforcement

1. Introduction

Cybersecurity has become a significant concern, with cybercrime and cyberattacks on the Internet increasing in recent years. Available hacking programs have made it easier to mount attacks through such activities as hacking passwords and authentication codes, computer intrusions, denial-of-service (DOS) attacks, Web defacements, proliferation of worms and viruses, phishing, identity theft, etc. Many government agencies and businesses have experienced Internet attacks, and hacking has evolved from what used to be merely the pastime of mischievous individuals to what is now big

business.[1] Thus, it is clear that cyber-threats merit considerable attention. Even the Philippine government recognized this by recently passing Republic Act 10175, otherwise known as the Cybercrime Prevention Act of 2012.

On the one hand, a big branch of the literature in law and economics deals with public law enforcement (e.g., police enforcement). On the other hand, some studies have examined private expenditures on security as a way to protect against crimes. These studies model private precautions but leave out public law enforcement in their models. In reality, crimes are solved by a combination of private precautions and public enforcement of the law. In this paper, we study a model in which crimes are addressed through a combination of private and public measures. By so doing, we capture the substitutability of private and public responses, and determine the optimal combination of these approaches.

In addition, in this paper, we capture two important aspects that are relevant in cybersecurity—to wit, the public-goods nature of privately provided cybersecurity goods, as well as the externalities in the form of interrelatedness of cyberrisks.

That is, Internet security entails both public and private goods.[2] Insofar as everyone shares common available risks (has a common pool of hackers and

[1] As Kesan and Majuca [2006] observed:

> The CERT/CC reports that the number of cyber-incidents increased from 252 in 1990 to 137,529 in 2003 … Government agencies, as well as businesses, have experienced Internet attacks. The Navy, for one, had its satellite guidance computer control compromised by a hacker who penetrated the Research Laboratory's network and downloaded software used in guiding satellites. Hackers have also breached the on-line security of government agencies including: the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), the Environmental Protection Agency (EPA), the National Aeronautics and Space Administration (NASA), and the U.S. Senate. (citations omitted)

In fact, in the Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) 2007 survey of computer crimes and security, 46 percent of the respondent US companies reported that they suffered a security incident. They reported an average annual loss of USD 350,424, which is more than double of previous year's average of USD 168,000.

It should be noted that, in general, there is a wide dispersion in the amount of losses arising from Internet security incidents, and even in the methodology for measuring the losses. For example, some scholars argue that a cyber attack's impact on the stock prices should be included in the loss calculation. This can be captured, for example, using an event study analysis, wherein the market value of the firm prior to the security breach is compared to its market value immediately after the attack (see, for example, Cavusoglu, Mishra, and Raghunathan [2004]). The Yankee Group has estimated that the year 2000 distributed DOS (DDOS) attacks on Yahoo!, Ebay, and Amazon resulted in more than USD 1.2 billion in combined loses due to lost customers, plunging stock prices, cost of network security upgrades (Cisco Systems, Inc. [2004]; see also Garg, Curtis, and Halper [2003]).

[2] A textbook definition is that a "public good is a commodity for which use of a unit of the good by one agent does not preclude its use by other agents" [Mas-Colell, Whinston, and Green 1995:359]. Put differently, public goods are goods which are nonrival or nondepletable: consumption by one person does not diminish or reduce the supply available to others. Classic examples are national defense, police protection, lighthouses, public parks, information and knowledge, clean air, etc. A distinction is also sometimes made in the literature according to the excludability of an individual from the enjoyment of a public good. "Every private good is automatically excludable, but public goods may or may not be" [MasColell, Whinston, and Green 1995:360]. In contrast, private goods are goods "whose consumption only affects a single economic agent" [Varian 1992:414].

vulnerabilities that can be exploited), and will thus all benefit from the reduction in such common pool of risks ("public bads"), then Internet security has public goods aspects, in the same manner that police and fire protection are traditionally regarded as public goods. On the other hand, insofar as there are residual risks not entirely eliminated by police enforcement, individuals can protect themselves against the residual risks by investing in individual-level precautions. These individual precautions in turn can take one of two forms: (a) investments in private security goods (such as the purchase of firewalls, intrusion detection systems [IDS], antivirus, security authentication codes, etc.); or (b) investments in nonrivalrous security goods (such as compiling information on software vulnerabilities, security holes, security incidents, hacking patterns, state of the art, etc.), which have the aspects of public goods. In sum, Internet security has both public and private goods dimensions; the public goods aspects of Internet security in turn can be provided either privately or publicly by the government (see Table 1).

TABLE 1. Private and public goods aspects of Internet security

Nature of the good/service	How provided	
	Privately (by individuals/firms)	Publicly (by the government)
Private goods	IDS, firewalls, etc.	
Public	Information on attacks, vulnerabilities, solutions	Police enforcement/protection

Also, the significant interrelatedness of risks in the Internet gives rise to externalities among individual Web sites. If an individual does not use an antivirus to clean his/her system, the computer virus can affect not only his/her computer systems but others' as well. Hence, a computer system can be breached not only directly but also indirectly through the negligence of other individuals in interconnected networks. In other words, privately provided private security goods do not have private benefits alone. Due to externalities, these private investments have spillover effects on other Internet users (the public).

The foregoing discussions raise an interrelated set of interesting questions. What optimal combination of each of these security measures—police enforcement, and individual investments in both private and nonrivalrous security goods—should be used to effectively combat cybercrimes? How should society handle the spillover effects arising from the interrelatedness of Internet risks? What role, if any, does police enforcement play?

In this paper, we study a model that combines all of these elements—namely, private investments in security, investments in security that have the nature of public goods, externalities, and public enforcement of law (see Figure 1).

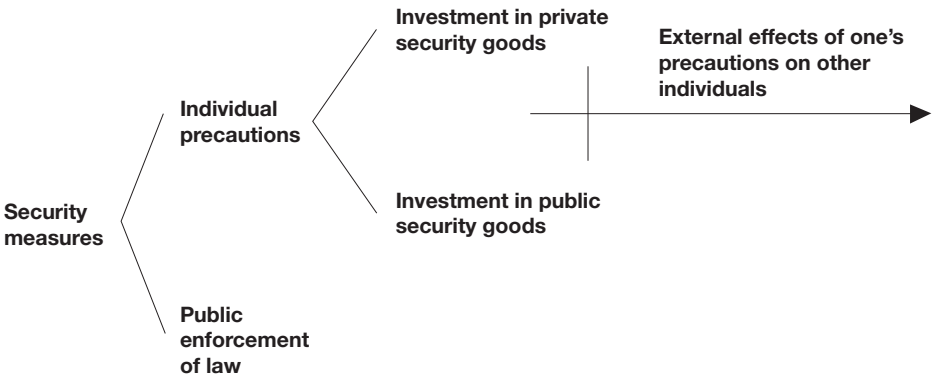

FIGURE 1. Elements of the model

That is, we model a situation wherein firms invest in both private and public security goods, risks are interrelated, and there is public enforcement of law against hackers. In reality, crimes can be solved by a combination of private precautions and public enforcement of the law. Expenditures on police enforcement reduce the number of crimes, while investments in individual precautions reduce the effectiveness of criminals in causing harm to their victims. In this paper, we study a model in which crimes are addressed through a combination of private and public measures. By so doing, we hope to capture the substitutability of private and public responses, and determine the optimal combination of these approaches.[3]

Looking at these elements together presents a more holistic view of the various ways society can protect itself against cyberattacks, and enables one to see the interplay, substitutability, and optimal combination of these means to effectively combat cyberattacks. By modeling the collective solution, we also aim to examine the role, if any, that cooperation plays in Internet security.

We find that just because Internet security has a public goods aspects does not necessary mean that the government, rather than the individual, should provide it. Rather, the solution is a combination of public and private alternatives. The problem with ceding to the government the entire function of providing Internet security is that such a solution is susceptible to the well-known problem

[3] Although past studies have looked at some of the aspects mentioned in Figure 1 individually and in isolation, none of these studies have looked at all the elements mentioned above together. For example, Heal and Kunreather [2003] have looked at interrelatedness of risks (e.g., in the context of terrorism and computer security) but has not looked into the other elements mentioned in Figure 1 above. Shavell [1991] and Kobayashi [2005] have also analyzed private security expenditures as a way to protect against crimes and have modeled private precautions but left out public enforcement of law in their models. Shavell [1991] has looked at investments in rival private precautions in general, and Kobayashi [2005] has considered investments in both private and public cybersecurity goods individually (i.e., he considered separate investments in either of these goods but not both of them together).

of "government failure".[4] On the other hand, the problem with adopting an entirely private solution is its susceptibility to the problem of "market failure". Externalities and the public goods aspect of Internet security result in a divergence between the private solution and what is socially optimal. The solution therefore, we think, is a careful combination of private and public measures, which brings us to the next point.

How should society achieve an optimal allocation of security investments across various public and private alternatives? We find that the socially optimal level of security is achieved by combining private security investment, nonrivalrous security investment, and law enforcement measures in such a way that their marginal-social-benefit-to-marginal-social-cost ratios are equalized. These marginal *social* benefits of private and public security good investments are greater than the marginal *private* benefits because individuals do not take into account the spillover effects of their own security investments on other computer systems, resulting in an underinvestment of both nonrivalrous and rivalrous security goods. Additionally, we find that in certain situations it would be optimal for the government to deliberately lower the level of police enforcement to induce firms to invest more in individual precautions.

Lastly, we find that under certain conditions, a cooperative undertaking results in the close approximation of the socially optimal level of private and public security good investments and police enforcement expenditures. This lends support to the recent government initiative to encourage the formation of information sharing and assessment centers (ISACs). The Shapley [1953] value can be used as a criterion for allocating the costs and benefits among the members of an ISAC. Alternatively, tradeable externality permits may be considered another mechanism for apportionment among group members. Some sort of political equilibrium mechanism wherein members vote so that their preferences may be incorporated into the group's decision-making process may be considered as well.

This result buttresses our conclusion that even if there is a market failure arising from public goods and externalities aspects of Internet security, it does

[4] In Internet security, government failure can manifest itself in the inability to know what the optimal social level of cybersecurity should be, considering that it does not possess the error correction mechanism of the market's profit and loss system (Coyne and Lesson [2005]; Powell [2005]). And because the public goods aspects of Internet security imply that these goods are not traded openly in the market, it is difficult for the government to estimate the socially optimal level of cybersecurity and then measure it against what was provided by the market [Powell 2005]. Furthermore, since the government does not have the same market pressures, it does not have the same incentive as the market participants to employ the hardware and software configuration that will reduce the damage from specific attacks, at the least cost [Coyne and Lesson, 2005]. In fact, there may be public relations pressures on the bureaucrats to make them pressure firms to overspend instead [Powell 2005]. Another problem is that once the regulation is passed and the cybersecurity situation changes, it is often difficult for bureaucracy-tied policymakers to assess, evaluate, and change the original policy. This is a particularly important consideration in the case of information security because of the ever dynamic nature of the technology environment [Coyne and Lesson, 2005].

not necessarily mean that government role is automatically prescribed to the exclusion of the private sector. Since under certain conditions the collective approximates the socially optimal solution, then some form of decentralized group solution can be utilized in certain cases to help address the problem of Internet security. The situation we envision is some kind of a group formation of the Buchanan [1965, 1999] type wherein group members choose the size of the group membership, the amount of public goods, and the incentives (i.e., Pigouvian penalties and subsidies). A cooperative game-theoretic formulation of this club theory is available (see, for example, Pauly [1967, 1970]) and its specific application to Internet security along the lines contemplated here may be explored further.

The rest of this paper consists of the following: section 2 introduces the model. Section 3 discusses the model's results under three different cases—namely, (a) the socially optimal solution, (b) the individual firm's private solution, and (c) the model's cooperative solution. Section 4 presents examples using specific functional forms, as well as some simulations. Section 5 concludes and summarizes the paper.

2. The model

We model a society populated with n symmetric risk-neutral firms and h identical risk-neutral hackers. Hacking requires an effort level e to each hacker, while n firms spend, respectively, $x_1, x_2, \ldots, x_n$, also denoted by the vector $\mathbf{x}$, on private security goods, and $y_1, y_2, \ldots, y_n$, also denoted by the vector $\mathbf{y}$ on public security goods. The government decides on the level of law enforcement expenditures, z. Since firms are identical, and to save on notation, we shall at times use x to denote the common value of $x_1 = x_2 = \ldots = x_n$, where this is permissible. Likewise, we use y to refer to the common value of $y_1 = y_2 = \ldots = y_n$, while $y_T = \sum y_i = y_T(\mathbf{y})$ denotes the sum of nonrivalrous private investments in security goods available to all firms. The hacking effort costs hackers $c(e)$, while the cost of individual investments in private security goods, and the cost (per firm) of maintaining the police force, are respectively $f(x_i)$ and $g(z)$, where $f'(x_i) > 0$, $f''(x_i) \geq 0$, $g'(z) > 0$, and $g''(z) \geq 0$ by assumption. The cost per unit of nonrivalrous security goods is normalized to 1 for simplicity.

The hacker's optimization problem is then to choose the effort level e that solves:

$$\max_{e} G(e, \mathbf{x}, y_T(\mathbf{y}), z) = e \cdot g(\mathbf{x}, y_T(\mathbf{y}), z) - c(e) \tag{1}$$

where $g(\cdot)$ is the hacker's gain from hacking, $c(e)$ is the cost of the effort to the hacker. It is reasonable to suppose that the gain of the hacker decreases (at a decreasing rate) with an increase in any of the security measures x, y_T, and z—that

is, $(\partial g/\partial x_i) < 0$, $\forall i$, $(\partial g/\partial y_T) < 0$, $(\partial g/\partial z) < 0$, with $(\partial^2 g/\partial x_i^2) > 0$, $\forall i$, $(\partial^2 g/\partial y_T^2) > 0$, and $(\partial^2 g/\partial z^2) > 0$. We further assume that $c'(e) > 0$ and $c''(e) > 0$.

The hacker's first-order condition for a maximum is $g(\mathbf{x}, y_T(\mathbf{y}), z) = c'(e)$, which implicitly defines $e = e(\mathbf{x}, y_T(\mathbf{y}), z)$. Hence, $g(\mathbf{x}, y_T(\mathbf{y}), z) = c'(e(\mathbf{x}, y_T(\mathbf{y}), z))$, and $(\partial g/\partial x_i) = c'' \cdot (\partial e/\partial x_i) \Rightarrow (\partial e/\partial x_i) = (\partial g/\partial x_i)(1/c') < 0$, $\forall i$, and $(\partial g/\partial z) = c'' \cdot (\partial e/\partial z) \Rightarrow (\partial e/\partial z) = (\partial g/\partial z)(1/c'') < 0$. That is, the effort level of the hacker decreases, *ceteris paribus*, with an increase in any of the security measures.

Define $p^i(\mathbf{x}, y_T(\mathbf{y}), z)$ to be the probability of the loss and $L^i(\mathbf{x}, y_T(\mathbf{y}), z)$ to be the magnitude of loss to an individual firm i, and $s(\mathbf{x}, y_T(\mathbf{y}), z) = L - g$ to be the associated deadweight social welfare loss from hacking. Owing to symmetry, $p^i(\cdot) = p^k(\cdot) = p(\cdot)$ and $L^i(\cdot) = L^k(\cdot) = L(\cdot)$, $\forall i, k$.

Both police enforcement z and own precautions x_i lower the probability of one's sites being attacked, thus:

$$p^i_z(\mathbf{x}, y_T(\mathbf{y}), z) < 0 \tag{2}$$

$$p^i_{x_i}(\mathbf{x}, y_T(\mathbf{y}), z) < 0, \forall i \tag{3}$$

Private security expenditures not only lower the probability of breach but also reduce the amount of loss. For example, file recovery efforts like regular backups and disaster-planning strategies are designed to mitigate the amount of a loss arising from a computer incident. Public enforcement likewise lowers the magnitude of the loss, thus

$$L^i_{x_i}(\mathbf{x}, y_T(\mathbf{y}), z) < 0, \forall i \tag{4}$$

$$L^i_z(\mathbf{x}, y_T(\mathbf{y}), z) < 0 \ \forall i \tag{5}$$

Internet security is interdependent. The lack of security in a network can cause damage not only to that network but also to other networks. If a computer virus or worm, for instance, penetrates an unprotected machine, there is a chance that it can breach other computers as well, as in fact a lot of viruses reproduce themselves [Heal and Kunreuther 2003]. Individual neglect therefore contributes to the probability of computer breach to other's systems. The probability of computer intrusion in one firm depends not only on its own precautions but also on the precautions of others. Likewise, one's private precautions lower the probability of breach not only of one's own computer systems but of other systems as well. For example, if a computer administrator regularly uses antivirus software, then it not only reduces its own probability of intrusion but also lowers the probability that a virus or a worm can infect other computers through its machine. A very common example is the proliferation of e-mail with virus attachments. A person who does not use antivirus software affects not only his/her machine but also others', since

many viruses are programmed to be sent to others in the e-mail group. Had the person used antivirus software and been protected, others would not have been infected. Thus,

$$p^{i}_{x_k}(\mathbf{x}, y_T(\mathbf{y}), z) < 0, k \neq i \tag{6}$$

We also assume that one's private security expenditures similarly reduce the losses of others. Since compromised computers can be used to launch attacks against other computers, if one's computers are not secure, hackers can possibly stage the attack against other Web sites through one's systems. In the case of denial-of-service attacks (DoS) and distribute denial-of-service attacks (DDoS) against other sites, the amount of damage on the attacked site depends, among others, on the length of time of the attack and the number of computers from where the attacks are staged. In essence, this implies that

$$L^{i}_{x_k}(\mathbf{x}, y_T(\mathbf{y}), z) < 0, k \neq i \tag{7}$$

Finally, we assume that the following signs of second and cross-partial derivatives of the functions p and L (dispensing with the superscripts):

$$p_{x_i x_k}(\mathbf{x}, y_T(\mathbf{y}), z) > 0, \forall i \neq k \tag{8a}$$

$$p_{x_i z}(\mathbf{x}, y_T(\mathbf{y}), z) > 0, \forall i \tag{8b}$$

$$L_{x_i x_k}(\mathbf{x}, y_T(\mathbf{y}), z) > 0, \forall i \neq k \tag{8c}$$

$$L_{zz}(\mathbf{x}, y_T(\mathbf{y}), z) > 0 \tag{8d}$$

$$L_{x_i z}(\mathbf{x}, y_T(\mathbf{y}), z) > 0, \forall i \tag{8e}$$

$$p_{zz}(\mathbf{x}, y_T(\mathbf{y}), z) > 0 \tag{8f}$$

$$p_{x_i x_k}(\mathbf{x}, y_T(\mathbf{y}), z) > 0, \forall i \tag{8g}$$

3. Results

3.1. The socially optimal solution

In this subsection, we discuss the socially optimal level of investments in private security goods, nonrivalrous security goods, and police and law enforcement expenditures. We view the solution from the perspective of the social

planner, which minimizes the total cost to all members in this society. Our finding is summarized in the following proposition.

Proposition 1. The socially optimal level of security is achieved by equalizing the marginal benefit-to-marginal cost ratios of each of the three alternatives: private security investment, nonrivalrous security investment, and law enforcement measures.[5]

The social planner's problem is

$$\min_{\{x,\, y_T,\, z\}} n\left[f(x)+g(z)\right]+y_T(\mathbf{y})+h\cdot\left\{c\left[e(\mathbf{x},\, y_T(\mathbf{y}),\, z)\right]+e(\mathbf{x},\, y_T(\mathbf{y}),\, z)\cdot s(\mathbf{x},\, y_T(\mathbf{y}),\, z)\right\} \quad (9)$$

That is, the social planner minimizes the total cost to all members of society, which in this model comprises the firms and the hackers. The total costs to society are thus equivalent to the sum of four components. First are the costs of providing the private security goods and police enforcement expenditures. For each firm i, this cost is $f(x) + g(z)$. Second is the cost of providing the nonrivalrous security good, y_T. This is produced at a cost of y for each firm. Third is the deadweight social loss from hacking, which represents losses of firms not transferred as gains to the hackers. Note that, as is standard in law and economics literature, losses to the firm that are gains to the hacker are not a social loss; they merely represent a "transfer from one pocket to the other". In Internet security breaches, however, losses to the firms may often not be transferred to the hackers. These types of losses are counted as a deadweight loss to society. Per hacker, this cost is $e(\cdot)\cdot s(\cdot)$. Lastly, the effort costs of the hackers, $h\cdot c(e)$, are a deadweight loss to society, since they represent costs to the hackers but are not gains to firms.[6]

As shown in the Appendix, in order to achieve the optimum amount of security investment per type, the social planner should set the common level of the private security good, $x_i = x_k = x$, the nonrivalrous security good, y_T, and police enforcement expenditures, z, so that

$$-\left(\sum_{i=1}^{n} p_{x_i}\right)\cdot L - p\cdot\left(\sum_{i=1}^{n} s_{x_i}\right) = f'(x) \quad (10)$$

$$-n(p_{y_T} L + p s_{y_T}) = 1 \quad (11)$$

$$-p_z\cdot L - p\cdot s_z = g'(z) \quad (12)$$

[5] Proofs of all propositions are provided in the Appendix.

[6] The gain to the hacker from hacking is already accounted for in the third component, since as mentioned in the previous section, $s(\cdot) = L - g$.

The left-hand side of equations (10), (11), and (12), represent respectively the marginal benefit of private security investment, nonrivalrous security investment, and police enforcement expenditures. On the right-hand side, meanwhile, are the marginal costs of those types of security investments.

As equation (10) shows, the marginal benefit of investing in private security good has two parts. The first part, captured by $-(\sum_{i=1}^{n} p_{x_i}) \cdot L$, represents the total marginal deterrence effect. In contrast to the standard result in the literature (see Shavell [1991:130]), here, because of the interrelatedness of security, the overall deterrence effect has to account for the reduction in the probability of intrusion of a Web site as a result of the investments on the security of other Web sites. For example, in many cases, compromised computers can be used to intrude into the target Web site. Thus, a firm benefits from the security investments of other firms because the security investments of the latter reduce the amount lost by the former. In like manner, a stronger security infrastructure of a firm would have positive spillover effects on the security of the others.

The second term in equation (10), $-p \cdot (\sum_{i=1}^{n} s_{x_i})$, represents the marginal *social waste reduction effect*. It captures the expected reduction in the amount of deadweight social welfare loss as a result of security investments. By definition, this term can be decomposed into the expected reduction of the amount stolen from the firm, $-p \cdot (\sum_{i=1}^{n} L_{x_i})$; that is, the marginal *theft reduction effect* in Shavell's [1991] terminology, *minus* the expected reduction of the gain to the hacker, $p \cdot (\sum_{i=1}^{n} g_{x_i})$.

Overall, in contrast to previous results in the literature, equation (10) shows that with externalities, the *social* marginal benefit of investing in security now includes not only the reduction of the probability or amount stolen from one's digital assets but also the reduction of the probability of intrusion and amount stolen from the other Web sites.

Dividing equations (10) and (12) by $f'(x)$ and $g'(z)$, respectively, proves Proposition 1, thus

$$\frac{-\left(\sum_{i=1}^{n} p_{x_i}\right) \cdot L - p \cdot \left(\sum_{i=1}^{n} L_{x_i}\right) + p \cdot \left(\sum_{i=1}^{n} g_{x_i}\right)}{f'(x)} = \frac{-n(p_{y_T} L + p s_{y_T})}{1} = \frac{-p_z \cdot L - p \cdot s_z}{g'(z)} \quad (13)$$

That is, the optimal solution to the cybersecurity problem is for society to equalize the marginal benefit-to-marginal cost ratios of the private security good, the public security good, and law enforcement measures.

We next discuss that the optimal amount of investment in each of these types of security goods changes depending on the reaction of the probability and magnitude of the loss to additional investments in each type.

Corollary 1. The more responsive the probability or the magnitude of the loss is to a particular security measure, the more of that security measure should be used, holding constant the cost of providing such measure.

Note that equation (13) can be rewritten in elasticity form. Thus, defining $\varepsilon_{p} = (\partial p/\partial x) \cdot (x/p)$, and defining ε_{s}, $\varepsilon_{p_{y_T}}$, etc., analogously, equation (13) becomes:

$$\frac{\left\{-(pL/x)\sum_{i=1}^{n}\varepsilon_{p_i}-(ps/x)\sum_{i=1}^{n}\varepsilon_{s_i}\right\}}{(f/x)\varepsilon_{f_x}}=\frac{\left\{-n\left[(pL/x)\,\varepsilon_{p_{y_T}}+(ps/y_T)\,\varepsilon_{s_{y_T}}\right]\right\}}{1}=\frac{\left\{-(pL/z)\,\varepsilon_{p_z}-(ps/z)\,\varepsilon_{s_z}\right\}}{(g/z)\varepsilon_{g_z}} \quad (14)$$

Hence, it will be optimal for society to adjust the level of private rivalrous and nonrivalrous security investments, and law enforcement expenditures, in accordance with the elasticity or responsiveness to them of the probability of loss, the amount of social loss, and the cost of providing the security measures. In general, the more elastic or responsive the probability of loss and the social loss to private rivalrous investment, the higher the optimal level of private rivalrous investment. The same applies to private nonrivalrous security investments, and the public expenditures on law enforcement.[7]

3. 2. The individual solution

In this subsection, we analyze how individual firms behave and how much investment in private and nonrivalrous security goods they undertake. We then compare the individual firm's solution with that of the socially optimal solution as previously discussed. We also analyze how the government sets the level of police enforcement expenditures given the individual firms' decisions.

Proposition 2. Individual firms have a tendency to underinvest in private security goods.

This result is best illustrated when we simplify L to equal s (the "social loss case"). The optimization problem of an individual firm (suppressing index i) is:[8]

$$\min_{\{x,\,y\}} p(x, y_T(\mathbf{y}), z) \cdot L\,(x, y_T(\mathbf{y}), z) + f(x) + y + g(z) \quad (15)$$

[7] This is similar to the result on price discrimination by a monopolist who sells in different markets. In the latter context, the monopolist sets its price in accordance with the price elasticity of demand in those markets. Of course, in the present cybersecurity context, the social planner also needs to take into account the reaction of the costs to these changes in the level of the different security measures.

[8] Technically, the optimization problem of an individual firm i is:

$$\min_{\{x,\,y\}} p(x_i \mid \mathrm{x}_{-i}, y_T(\mathbf{y}), z) \cdot L\,(\mathrm{x}, y_T(\mathbf{y}), z) + f(x_i) + y + g(z),$$

where x_{-i} represents the amount of security investments of all the other firms. Strictly speaking, $p(x_i \mid \mathrm{x}_{-i}, y_T(\mathbf{y}), z)$ is different from $p(\mathrm{x}, y_T(\mathbf{y}), z) = (h/n)\mathrm{e}$ since firms can divert hackers to the other sites (see Shavell [1991] and Kobayashi [2005]). In order to focus our discussion, however, we abstract from this issue and simplify the model to the case where $p(x_i \mid \mathrm{x}_{-i}, y_T(\mathbf{y}), z) = p(\mathrm{x}, y_T(\mathbf{y}), z)$.

The first-order condition of the individual firm with respect to private security investments, x, is

$$-p_x \cdot L - pL_x = f'(x) \tag{16}$$

This is in contrast to the socially optimal amount of private security investment, which is

$$-\left(\sum_{i=1}^{n} p_{x_i}\right) \cdot L - p \cdot \left(\sum_{i=1}^{n} L_{x_i}\right) = f'(x) \tag{10'}$$

in the social loss case.

Equation (15) says that, while it is socially optimal to set the level of private security investment to account for the positive spillover effects of one's security investments to other Web sites (Proposition 1), the individual firm does not care about the positive spillover effects it can generate for the other Web sites. Instead, it will care only about its own marginal benefit and set its level of private security investments so that its marginal cost is equal to its marginal *private* diversion effect and *private* loss reduction effects.

Equation (16) implies that

$$f'(x) = -(pL/x)(\varepsilon_p + \varepsilon_L) \tag{17}$$

where $\varepsilon_p = (\partial p/\partial x)(x/p)$, etc.

Equation (17) says that an individual firm will equate marginal cost to the reduction in the expected cost per unit of precaution, multiplied by the sum of the responsiveness of both the probability and the magnitude of the loss to the change in its own private security investment. The higher the expected loss and the more responsive the probability of the loss and the magnitude of the loss are with respect to the amount of precaution, the higher the marginal benefit of the precaution, and thus, the higher the optimal level of private precaution.

We next discuss the amount of nonrivalrous security good that an individual firm would undertake, and compare that amount to the socially optimal level.

Proposition 3. The level of public security goods will also be underprovided; the public good nature of the security investment causes the divergence of the level of public security expenditures from the socially optimal amount.

From the first-order condition of equation (15) with respect to the nonrivalrous security good, y, we see the individual firm will set its level of nonrivalrous security investments so that

$$-p_{y_T} \cdot L - pL_{y_T} = 1 \tag{18}$$

This is in contrast to equation (11) where in the social loss case ($L=s$), it is optimal for society to set the level of nonrivalrous security goods so that

$$-n(p_{y_T} L + pL_{y_T}) = 1 \tag{11'}$$

Equation (19) states that from an individual firm's viewpoint, for an investment in private security good to be at the optimal level, the cost to the firm of a little more precaution, normalized to 1 unit, should equal the decrease in the expected cost of the loss from hacking, both in terms of reduction in the intrusion rate and the reduction in the loss from intrusions. From the perspective of the individual firm, the motivation for investing in precaution (marginal benefit) is the reduction in the expected cost of the harm. From the social planner's perspective, however, since the security good is nonrivalrous, the *social* marginal benefit is magnified by the number of firms.

We next address an interesting question.

Proposition 2 says that firms have a tendency to underinvest in private security goods ("externality effect"), while Proposition 3 says that the level of nonrivalrous security goods will also be underprovided ("free-riding effect"). Does it then follow that in the case of public security goods, there will both be the free riding from the public good and the externality effect to worsen the underinvestment to a large extent? At first, it may seem that the answer is yes. But upon perusal, we see that the "externality effect" drops out of the picture. That is, in the case of public security goods, the positive effect of one's public security investment on others is "internalized" by the firm in calculating its optimal level of public security goods.

The reason for this is that the original spender strategically takes into account the positive effect on itself of the other firms' use of the former's privately provided public security good. In economic parlance, the original spender knows that other firms will "free-ride" on its nonrivalrous security investment. However, such free riding will benefit the original spender because security is interdependent. Therefore, the original spender strategically allows this free riding by other firms on its nonrivalrous security investment in order to increase its (the original spender's) own security. In legal parlance, it is as if the original spender uses other firms as its agent in that it knows that if it invests in the public security good, that same good will be available to the other firms, whose use of such good will reduce the other firms' security intrusions, and because security is interdependent, such will ultimately redound to its (the original spender's) benefit. We illustrate this important point more concretely in section 4 below, where we stress that the more interdependent Internet security is, the more the original spender will want other firms to free-ride on its nonrivalrous security investments.[9]

[9] Thus, this is one less problem associated with the market solution and one more argument in favor of it compared to the alternative of government-provided security.

The next proposition discusses what happens to the level of underinvestment by individual firms as the number of firms increases.

Proposition 4. As the number of firms, n, increases, the amount of the underinvestment in private and public security goods investment correspondingly increases. Also, the "public-good effect" worsens.

This case be readily seen again by comparing equation (10') with equation (16), and equation (11') with (18).

The next proposition discusses how an individual firm's choices of the level of private security-good investment, x^* (= x_1^* = x_2^* =…= x_n^*) and the level of nonrivalrous security-good investment, y^* (= y_1^* = y_2^* …= y_n^*), change with the level of police or law enforcement expenditures, z.

Proposition 5. Under regular conditions, an increase in the government law enforcement expenditures lowers both private rivalrous and nonrivalrous expenditures, except if the cross-elasticities of substitution between rivalrous and nonrivalrous security expenditures are so high that they dominate the effect of the reduction in one type of private security expenditure caused by the increase in government expenditures.

The proof of this is clear from equations (A-13) and (A-14) in Appendix A, where it can be seen that $(dx_i/dz) < 0$ [$(dy_i/dz) < 0$], so long as it is not the case that both (a) the cross effects between x_i and y_i are so great and (b) the elasticity of substitution between z and y (resp. z and x_i) is much greater than that between z and x_i (resp., z and y_i), as to overwhelm the effect of reduction of x_i (resp., y_i) as a result of increase in z. Thus, in general, public expenditure on police and law enforcement has a moral hazard effect: it reduces the propensity of firms to invest in private- and public-security goods for their own protection.

The next proposition discusses how the government responds to this moral-hazard effect of police enforcement on the level of the individual firms' security investments.

Proposition 6. The government decidedly lowers the level of police enforcement in order to induce private firms to invest more in individual precautions.[10] Also, because the underinvestment in both private-security goods and public-security goods worsens with the increase in the number of firms, the government correspondingly tailor-fits the size of its adjustment to the size of the underinvestment.

[10] The first part of this proposition is similar to the result obtained by Orszag and Stiglitz [2002], who studied the optimal size of fire departments.

Imposing symmetry, we have $x_i = x^*$, $y_i = y^*$ $\forall i$, with both x^* and y^* being implicit functions of z. The government then chooses z in order to solve

$$\min n\Big[f(x^*(z) + y^*(z) + g(z)\Big] + h\Big[c\Big(e(\mathbf{x}^*(z), y_T^*(\mathbf{y}(z), z)\Big) + e\Big(\mathbf{x}^*(z), y_T^*(\mathbf{y}(z), z)\Big) \cdot s\Big(\mathbf{x}^*(z), y_T^*(\mathbf{y}(z), z)\Big)\Big] \tag{19}$$

where $y_T^*(\mathbf{y}(z)) = \sum_{i=1}^{n} y_i^*(z)$.

As shown in Appendix equation A-19, the first-order condition of the government is

$$-p_z L - ps_z - \partial x^*/\partial z \left[\left(\sum_{i=2}^{n} p_{x_i}\right) \cdot L + p \cdot \left(\sum_{i=2}^{n} L_{x_i}\right) - p \cdot \left(\sum_{i=1}^{n} g_{x_i}\right)\right] - \partial y^*/\partial z \left[(n-1) \cdot p_{y_T} L + (n-1) \cdot pL_{y_T} - n \cdot pg_{y_T}\right] = g'(z) \tag{20}$$

Comparing equation (20) with equation (12), we see that in the individual solution case, the government will deliberately underprovide public law enforcement expenditures by the amount

$$-\partial x^*/\partial z \left[\left(\sum_{i=2}^{n} p_{x_i}\right) \cdot L + p \cdot \left(\sum_{i=2}^{n} L_{x_i}\right) - p \cdot \left(\sum_{i=1}^{n} g_{x_i}\right)\right] - \partial y^*/\partial z \left[(n-1) \cdot p_{y_T} L + (n-1) \cdot pL_{y_T} - n \cdot pg_{y_T}\right].$$

This amount is simply the sum of the amount of the individual's underinvestment in private and public security goods (i.e., the difference between the social planner's and the private firm's first-order conditions: equations [10] minus [16], and [11] minus [18], respectively), weighted by the responsiveness of these security investments to law enforcement expenditures.

In other words, since under the individual solution both levels of the private security goods and the nonrivalrous security goods are underprovided, and since lowering the government police expenditures increases investment in both types of security goods (Proposition 5), the government lowers the amount of police protection in order to induce the individuals to invest more in precautions. The government tailor-fits this strategy according to the size of the individual's underinvestment.

3.1. The cooperative solution

This subsection analyses the situation wherein the individual firms cooperate with each other to address cybersecurity problems. As the next proposition shows, this cooperative arrangement approximates the socially optimal solution to the cybersecurity problem.

Proposition 7. Under the social loss case (i.e., if $L = s$), a cooperative results in socially optimal levels of expenditures in police enforcement and private and public security goods investments.

The cooperative's problem is

$$\min_{\{x,\, y_T\}} n \cdot p\left(\mathbf{x}, y_T, (\mathbf{y}), z)\right) \cdot L\left(\mathbf{x}, y_T, (\mathbf{y}), z)\right) + n \cdot f(x) + y_T + n \cdot g(z) \tag{21}$$

which results in the following first-order conditions:

$$\{x\} \qquad -\left[\left(\sum_{i=1}^{n} p_{x_i}\right) \cdot L + p \cdot \left(\sum_{i=2}^{n} L_{x_i}\right)\right] = f'(x) \tag{22}$$

$$\{y_T\} \qquad -n \cdot \left[p_{y_T} L + p L_{y_T}\right] = 1 \tag{23}$$

The government then decides on the level of police enforcement expenditures by choosing z so as to

$$\begin{aligned}\min n\Big[f(x^{**}(z)) + g(z)\Big] + y^{**}(z) + h\Big[c\Big(e(\mathbf{x}^{**}(z), y_T^{**}(\mathbf{y}^{**}(z), z)\Big) \\ + e\Big((\mathbf{x}^{**}(z), y_T^{**}(\mathbf{y}^{**}(z), z)\Big) \cdot s\Big((\mathbf{x}^{**}(z), y_T^{**}(\mathbf{y}^{**}(z), z))\Big)\Big]\end{aligned} \tag{24}$$

This results in the following first-order condition

$$\begin{aligned}-p_z L - p s_z - \partial x^{**}/\partial z \left[f'(x) + L \cdot \left(\sum_{i=1}^{n} p_{x_i}\right) + p \cdot \left(\sum_{i=1}^{n} s_{x_i}\right)\right] \\ - \partial y^{**}/\partial z \left[1 + n \cdot p_{y_T} L + p s_{y_T}\right] = g'(z)\end{aligned} \tag{25}$$

Substituting in the collective's first-order condition (and if $L = s$), this reduces to

$$-p_z L - p s_z = g'(z) \tag{26}$$

By comparing the socially optimal solution (equations (10), (11) and (12)) with the cooperative solution (equations (22), (23), and (26)), we can see that the cooperative solution approximates the socially optimal solution.

This finding is consistent with the present move of the US government to encourage the formation of ISACs. The question that arises, however, is how ISAC group members among themselves can allocate the costs associated with generating the (public) security goods. Other than the ISAC members bargaining among themselves, one mechanism that can be explored is the creation of tradeable externality permits among the members of ISACs themselves, with the overall group "quota" on the externality determined by the coalition on the basis of optimization by the collective. Under this scenario, the overall level of

externalities that will be allowed will be determined on the basis of optimization by the collective, and then the distribution of allowable externalities will be priced out among the members—that is, those desiring to "use" the externality will purchase the externality permit by bidding for it.

If such a "market-based" allocation of the externality proves unwieldy in practice, another solution that can be considered is allocating on the basis of the member's Shapley value:

$$\psi_i = \sum_C \frac{(n-k)!(k-1)}{n!} [v(C) - v(C - \{i\})] \tag{27}$$

where k is the size of the coalition C, n is the total players, $v(C)$ is the value of the coalition, $v(C–\{i\})$ is the value of the coalition without player i, and where the sum is taken over all the coalition C that includes i as a member. Since $[v(C) – v(C – \{i\})]$ is the marginal contribution of i to the coalition C, the Shapley value of i simply reflects the expected marginal contribution of i. Hence, the Shapley value would be an appropriate measure in this case, since it approximates what an actual market mechanism would reward to the member for his/her contribution, and the Shapley value is a way of tying the payoffs to the member's marginal productivity, when an actual market cannot be arranged. This approach of applying the principles of cooperative game theory has been adopted in various cost-allocation games such as municipal cost sharing (see, for example, Suzuki and Nakayama [1976]; Young, Okada, and Hashimoto [1982]), building airport runways (see, for example, Littlechild [1974]; Littlechild and Owen [1973]), and minimum cost spanning tree games (see, for example, Granot and Huberman [1981]; Granot and Huberman [1984]; Megiddo [1978]).

Another form of decentralized group solution that can be utilized is the Buchanan [1965, 1999] type wherein the members of the group choose the size of the group membership, the amount of the public good, and the incentives (i.e., Pigouvian penalties and subsidies) (see, for example, Fabella [2005]). A cooperative game-theoretic formulation of this club theory is available (see, for example, Pauly [1967, 1970]) and its specific application to Internet security along the lines contemplated here may be explored further.

In sum, the same procedure of decentralized group formation can be used to help address the problem of Internet security. That is, a market failure arising from the public goods and externalities aspects of Internet security does not necessarily mean that government role is automatically prescribed to the exclusion of the private sector. Instead, both public and private sector initiatives can be utilized.

In Table 2, we summarize the amounts of privately provided private and public security goods, and the level of government-provided law enforcement expenditures, under the three different scenarios. A simple two-firm case is presented to aid intuition.

TABLE 2. Summary of first-order conditions and level of security investments (by type of agent and security investment)

	First-order condition (x)	Level of private security good
Individual	$-p_{x_1} \cdot L - p \cdot L_{x_1} = f'(x)$	x^*
Collective	$-(p_{x_1} + p_{x_2})L - p\,(L_{x_1} + L_{x_2}) = f'(x)$	x^{**}
Socially optimal	$-(p_{x_1} + p_{x_2})L - p\,(s_{x_1} + s_{x_2}) = f'(x)$	x^o
	First-order condition (y)	**Level of public security good**
Individual	$-p_{y_T}L - pL_{y_T} = 1$	y^*
Collective	$-2[p_{y_T}L - pL_{y_T}] = 1$	y^{**}
Socially optimal	$-2[p_{y_T}L - ps_{y_T}] = 1$	y^o
	First-order condition (z)	**Public enforcement of law**
Individual	$-p_zL - ps_z - (\partial x^*/\partial z)\,[p_{x_2}L + pL_{x_2} - p \cdot (g_{x_1} + g_{x_2})]$ $-(\partial y^*/\partial z)\,[p_{y_T}L + ps_{y_T} - pg_{y_T}] = g'(z)$	z^*
Collective	$-p_zL - ps_z = g'(z)$	z^{**}
Socially optimal	$-p_zL - ps_z = g'(z)$	z^o

From Table 2, we can see that

$$\begin{cases} x^{**} = x^o > x^* \text{ for } s = L \\ x^{**} > x^o > x^* \quad\quad s < L; \end{cases}$$

$$\begin{cases} y^{**} = x^o > y^* \text{ for } s = L \\ y^{**} > x^o > y^* \quad\quad s < L; \end{cases} \quad \text{and}$$

$$z^{**} = z^o > z^*.$$

Thus, in the social loss case, wherein the hacking simply results in loss to firms but not transferred as gain to the hacker,[11] the cooperative solution achieves the socially optimal level of security investments for all three types (private security investment, nonrivalrous security investment, and government expenditures on law enforcement) (see also Proposition 7). Where the hacking results in a gain to the hacker ($s < L$),[12] since the social planner does not view the loss to the firms transferred as gain to the hackers as a social loss, the social planner will have a lower level of private and public security good investments than the security cooperative.

[11] This applies to cases like DOS, distributed DOS (DDOS), Web defacements, and the like, which result in damages to firms but without monetary gain for the hackers.

[12] Such as in credit card, identity, intellectual property theft, and the like.

The individual firms, however, underinvest in both private and nonrivalrous security goods, for both the social-loss case and the case in which hacking results in a gain to the hacker. As can be seen from Table 2, the underinvestment in private-security good arises because Internet security is interdependent, yet the individual firms do not take into account the positive spillover effects of their precautions on others. On the other hand, the underinvestment in (privately provided) public-security good results from the fact that the nonrivalrous nature of such good allows others to use it. Finally, the level of government-provided security goods (e.g., police enforcement) is also lower in the individual solution than in the socially optimal case, since as mentioned in Proposition 6, the government strategically lowers its level of expenditures in order to incentivize firms to invest more in private- and public-security goods.

4. Examples and simulations

We can illustrate the abovementioned results and make the discussions more concrete by specifying functional forms and applying it to the two-firm case. We adopt the following functional specifications for the probability and loss functions:

$$p(x_1, x_2, y_T, z) = (1 - q)e^{-(\alpha x_1 y_T + \theta z)} + qe^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)} \tag{28}$$

$$L(x_1, x_2, y_T, z) = A\left[(1 - q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c\right] \tag{29}$$

$$g(x_1, x_2, y_T, z) = \lambda(x_1, x_2, y_T, z) \cdot A\left[(1-q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c\right] \tag{30}$$

where $\lambda \in [0,1]$. Thus,

$$s(x_1, x_2, y_T, z) = [1-\lambda] \cdot A\left[(1 - q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c\right] \tag{31}$$

We assume $0 < \alpha, \beta, \theta \leq 1$.

We thus decompose the attack into direct attacks and attacks staged indirectly through other compromised computers. Thus, equation (28) tells us that total probability of attack to firm 1 is the combination of the direct attack probability, $e^{-(\alpha x_1 y_T + \theta z)}$, and the probability that firm 1 will be attacked indirectly through firm 2, $e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}$. $(1 - q)$ provides a relative measure of the number of the *direct* computer attacks, while q provides a relative measure of attacks staged *indirectly* through other compromised computers. Thus, q measures the strength of the interdependence of the security of the two firms. That is, if $q = 0$, the indirect effect, $q \cdot e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}$, drops out and the probability of attack is simply the probability of direct attack to firm 1. On the other hand, a relatively large q signifies that firm 1 must guard not only against direct attacks to its systems but also against attacks and viruses coming from other computers. Normally, we expect q to be greater than 0, reflecting the interdependent nature of computer security, and at the same

time q is expected to be less than ½, signifying that direct attacks always account for the greater portion of attacks than indirect attacks.

We note that the probability of attack ranges from 0 to 1—as it ought to be—under these functional forms. Also, the probability of attack decreases with an increase in the level of private-security investment, public-security investment, or the law enforcement expenditures (see Figure 2 below). The same thing holds true for the magnitude of the loss. Thus, the probability multiplied by the magnitude of the loss goes down with x, y_T, and z (see, for example, Figure 3 below).

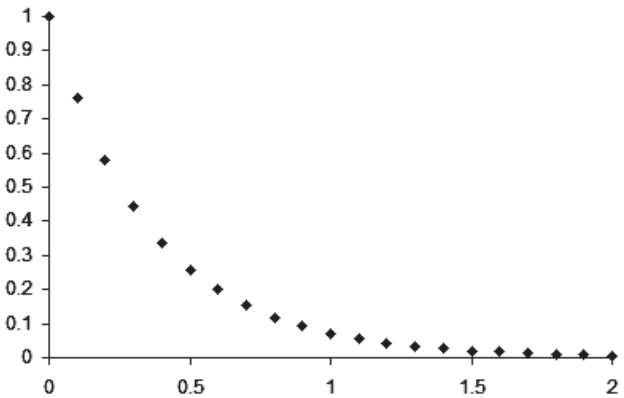

FIGURE 2. $p(x_1, x_2, y_T, z)$ **when** $x_1 = x_2 = z, y_T = 1$

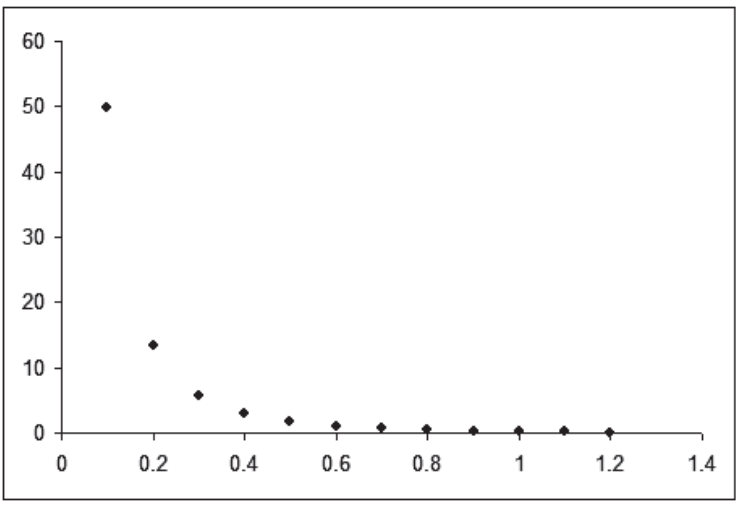

FIGURE 3. $p(x_1, x_2, y_T, z) \cdot L(x_1, x_2, y_T, z)$ **when** $x_1 = x_2 = z, y_T = 1$

We also note that an increase in the security investment of firm 2 decreases the indirect attack probability (i.e., $(\partial e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}/\partial x_2) < 0$), but does not affect the direct attack probability, as $(\partial e^{-(\alpha x_1 y_T + \theta z)}/\partial x_2) = 0$. In contrast, firm 1 can decrease the probability that its systems will be breached either directly or indirectly by increasing its own precaution, x_1, since both $\partial e^{-(\alpha x_1 y_T + \theta z)}/\partial x_1$ and $\partial e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}/\partial x_1$ are negative.

The parameters α, β, and θ measure the relative effectiveness of one's own precautions, other's precautions, and police protection, respectively, in reducing computer intrusions in one's systems, while a, b, and c measure the same with respect to the reduction in the magnitude of the loss.

We now illustrate the important points of our simulations with the use of graphs.[13]

Figure 4 shows that the optimal level of Internet security should be determined by balancing the trade-off between the reduction in the probability multiplied by the magnitude of the loss and the cost associated with providing the security. Figure 5, on the other hand, depicts the marginal benefit of the precaution to the individual firm vis-à-vis the marginal benefit to the cooperative. The optimal level of precaution is determined by equalizing the marginal benefit to the marginal cost.

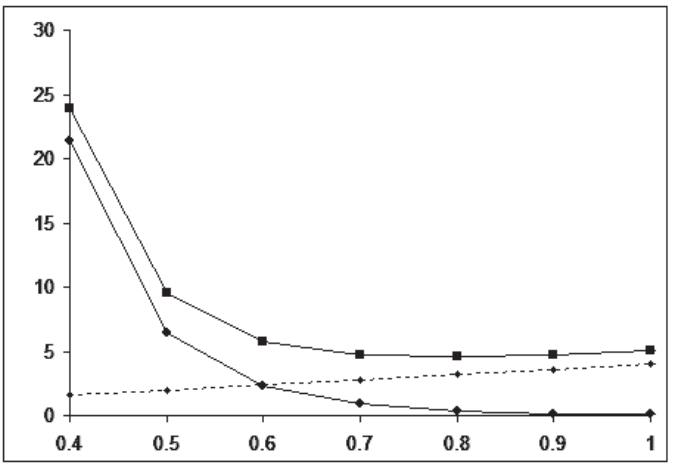

FIGURE 4. $p \cdot L + f(x_1) + y_T + g(z)$ **when** $x_1 = x_2 = z$, $y_T = 1$, $f(x_1) = 4x_1$

[13] In Appendix B, we show the calculations of the first, second, and cross-partial derivatives used in Figures 4–7.

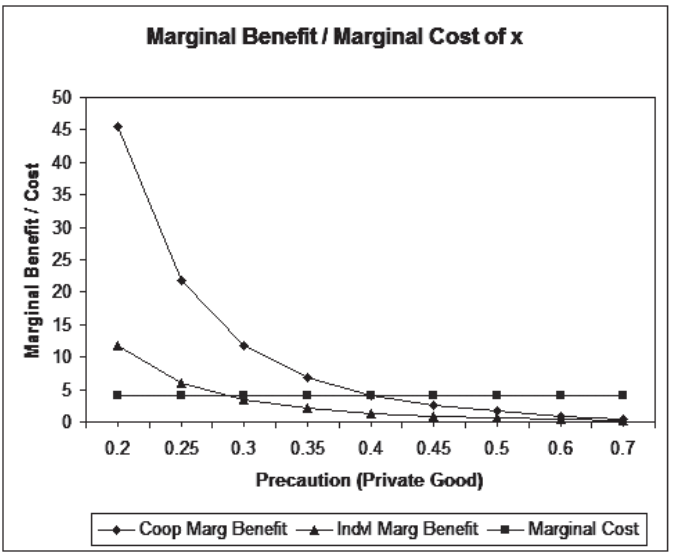

FIGURE 5. Optimal private precaution: cooperative vs. individual solution

Also, as Proposition 1 implies, the marginal cost of a particular type of security measure is an important consideration in determining the optimal level of investment in that security measure relative to others. Our simulations confirm this point. Thus, under the abovementioned functional specifications, we find that as the marginal cost of the private-security good increases, *ceteris paribus*, the investment in private-security measures decreases relative to the level of investment in public-security goods. More specifically, for the collective and social planner, $y_T/x = 2f'(x)$ for any parameter specification. (Mathematically, the reason for this is that, looking at the marginal benefit of x and y_T for the collective and the social planner, we see that p_{y_T} is basically equal to $p_{x_1} + p_{x_2}$ and $L_{y_T}(s_{y_T})$ is basically equal to $L_{x_1} + L_{x_2}(s_{x_1} + s_{x_2})$, with x and y_T interchanged. Thus, from the first-order conditions, we know that the marginal conditions for x and y_T are different because of the number 2 (i.e., the number of firms) and $f'(x)$, the marginal cost of x (since the marginal cost of y_T is normalized to 1).

As for the individual solution, although the relationship between y_T and x is not as neatly summarized by a formula,[14] our simulations show that y_T/x nonetheless monotonically increases with the marginal cost of x, *ceteris paribus.* We find this to be true for different values of α, β, θ, λ, q, a, b, and c. Thus, for example, if $q = 0.5$, $\alpha = 1.5$, $\beta = 1$, $\theta = 0.5$, $a = -1.5$, $b = -1$, $c = -0.5$, $\lambda = 0.5$, and $g'(z)=4$, we have Figures 6–9, thus:

[14] The reason for the difference between the individual and the collective/socially optimal cases will be discussed in the next result.

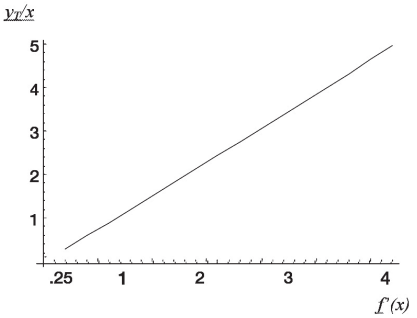

FIGURE 6. Individual firm's y_T/x as a function of $f'(x)$

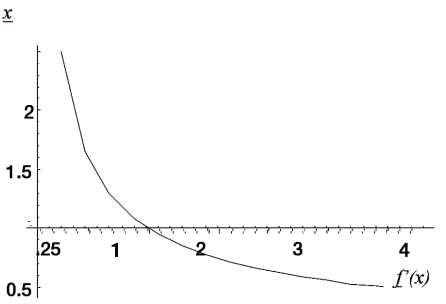

FIGURE 7. Individual firm's x as a function of $f'(x)$

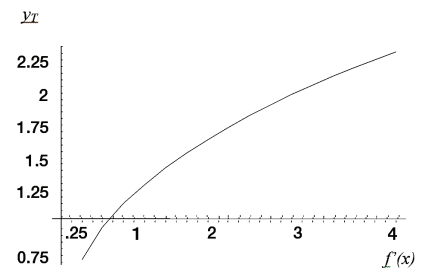

FIGURE 8. Individual firm's y_T as a function of $f'(x)$

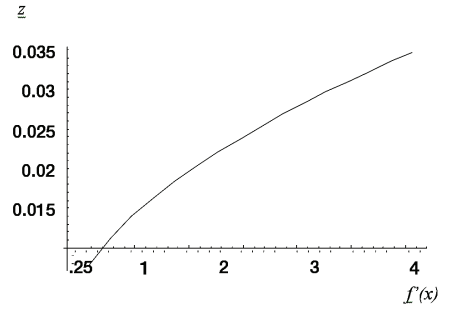

FIGURE 9. Individual firm's z as a function of $f'(x)$

Thus, as Figures 6–9 illustrate, if the (marginal) costs of a security measure are high, the firms will tend to provide less of that security measure and substitute it with the others.

Another important finding we gather from the simulations is that, as q, the measure of interdependence, increases, the individual firm will increase investment in public-security goods, y_T, relative to its investment in private-security goods, x.[15] The reason for this is that, looking at the first-order conditions for y_T and x, we see that the marginal benefit of the public- and private-security goods are differentiated by the terms $\beta x_2 \cdot qe^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}$ and $b \cdot q x_1^{\,a} x_2^{\,b} y_T^{\,a+b-1} z$, representing the *additional* reduction in both the probability and magnitude of the loss that the individual firm achieves because its public-security goods investment is being used by other firm, which in turn benefits firm 1. Hence, although firm

[15] Thus, for α= 1.5, β= 1, θ = 0.5, λ = 0.5, a = -1.5, b = -1, c = -0.5, $f'(x)$ = 4, and $g'(z)$ = 0.5, we have x = 0.1923, 0.2141, and 0.2355 for q = 0.2, 0.5, and 0.8 respectively, while y_T = 1.0232, 1.2626, and 1.49, for the same values of q. Again, we have rigorously tried the simulations for different values of the parameters (e.g., high $f'(x)$ case, low $f'(x)$ case, high $g'(z)$, low $g'(z)$, high/low a, high/low θ, high λ/low λ, high/low |a|, etc.) and the result remains the same.

2 is technically free-riding on firm 1's investment in public-security good, such free-riding is actually benefiting firm 1 because the more secure firm 2 is, the less firm 1 is affected by intrusions coming its way through firm 2. Hence, the more interrelated cybersecurity is, the higher an individual firm's public-security investment relative to private-security investment tends to be.

In contrast, the ratio of public-to-private security-goods investment of both the social planner and the collective is constant at $y_T/x = 2f'(x)$ and does not vary with the level of security interdependence, q. This formula states that the collective and the social planner will choose more public-security investment relative to private-security investment as its weapon of attack against cybercrimes, the higher the marginal cost of private-security goods is, and the higher the number of firms (2 in this case). However, both the collective and the social planner will not vary their public-to-private security-goods ratio according to the level of interdependence. On the other hand, although the individual firm also takes into account the marginal cost and the number of firms in its determination of its public-to-private security-goods ratio, it also, on top of the above considerations, includes the level of interdependence in its calculation. The higher the level of interdependence, the bigger the bang per buck of its public-security investment, since the more interdependent the firms' security, the more beneficial the "free-riding" by the other firms in its public-goods investment.[16] This phenomenon, however, does not apply in the case of the socially optimal and the collective solution because the social planner and the cooperative already take into account the external effects of both the public-goods *and* the private-goods investment on other firms' security, and so, the ratio y_T/x is constant for different levels of q in those cases. In contrast, in the case of the individual firm, while the public-goods investments are available for use by the other firms (and which use by other firms benefits the security of the provider of the public security good), the private goods investments (by definition) are not. Hence, for the individual firm, the ratio y_T/x is higher the greater q is; for the collective and the social planner, such ratio is constant with q and follows the $y_T/\ x = 2f'(x)$ formula.

5. Conclusions

Previous studies have examined private expenditures on security as protection against crimes. These studies have modeled private precautions but leave out public enforcement of law in their models. In reality, crimes are solved by a combination of private precautions and public enforcement of the law. In this paper, we study a model wherein crimes are addressed through a combination of private and public measures. By so doing, we capture the substitutability between

[16] In other words, the greater the interdependence, the more a firm will want other firms to "free-ride" on its nonrivalrous security investment.

private and public responses, and determine the optimal combination of these approaches.[17]

In addition, our model captures two other important aspects of cybercrime protection. First, in the Internet, individual precautions can take one of two forms: (a) investments in private-security goods (such as the purchase of firewalls); or (b) investments in nonrivalrous security goods (such as compiling information on software vulnerabilities, security holes, security incidents, and hacking patterns), which therefore have aspects of public goods. Second, in the Internet, there is significant interrelatedness of risks, which give rise to externalities among individual Web sites. Thus, in this paper, we study a model that combines all of these elements: private investments in security, investments in security that has the nature of public goods, externalities, and public enforcement of law.

We find that the socially optimal level of security is achieved by equalizing the marginal benefit-to-marginal cost ratios of each of the three alternatives—private security investment, nonrivalrous security investment, and law enforcement measures. Thus, as the marginal benefit (marginal cost) of a particular security measure decreases (increases) relative to the others, *ceteris paribus*, the investment in such type of security measure decreases relative to the others. In particular, if the marginal cost of a security measure is high, society should provide less of that security measure and substitute it with the others.

Also, the optimal amount of investment in each of these types of security measure changes depending on the reaction of the probability and magnitude of the loss to additional investments in each type. The more responsive the probability or the magnitude of the loss is to a particular security measure, the more of that security measure should be used.

We also find that the interrelatedness of Internet risks causes individual firms to underinvest in private-security goods. The individual firm's level of nonrivalrous security goods is also underprovided, as the public-good nature of the security investment causes the divergence of the firm's level of public security expenditures and the socially optimal amount. Although at first it may seem that in the case of nonrivalrous security goods both the free-riding and the externality effect combine to compound the underinvestment, upon perusal, the "externality effect" drops out of the picture. That is, if a firm spends on nonrivalrous security investments, it is likely that other firms will "free-ride"; however, such free-riding will benefit the original spender (since security is interdependent), and therefore the original spender strategically allows this free-riding by other firms

[17] In this paper, we studied a model involving symmetric firms. Future studies can perhaps explore the case where firms are not symmetric. In many real-world situations, firms may have asymmetric incentives, such as, for example, a bank and a depositor where a depositor would merely be content to have a simple antivirus, but a bank, because it has more to lose, may invest in a dedicated IT unit. Future studies can also perhaps tackle the complementariness of the different types of security investments. The author would like to thank an anonymous referee for these insights.

in order to increase its (the original spender's) own security. In effect, the positive effect of one's public security investment on others is "internalized" by the firm in calculating its optimal level of public security goods. The more interrelated cybersecurity is, the higher an individual firm's public security investment relative to its private security investment. This is because, from the original spender's perspective, the higher the level of interdependence, the bigger the bang per buck of its nonrivalrous security investment, since the greater the interdependent firms' security, the more "free-riding" by the other firms in its public-goods investment will benefit it. From the societal perspective, too, the higher the number of firms, the more public-security investment relative to private-security investment should be utilized as the weapon of attack against cybercrimes.

In addition, we find that the level of private and public security goods investments by firms decreases as the government increases expenditures for police enforcement. This is akin to a moral hazard effect of law enforcement. In order to counter this moral hazard effect, the government decidedly lowers its expenditures for law enforcement, to incentivize firms to increase their investments in private and nonrivalrous security goods.

In conclusion, a market failure arising from the public goods and the externalities of Internet security does not necessarily mean that the government role is automatically prescribed to the exclusion of the private sector. Instead, both public and private sector initiatives can be utilized. More specifically, we find that under certain conditions cooperation results in socially optimal levels of expenditures in private- and public-security goods. We can thus envision a situation wherein members of a security cooperative either (a) bargain among themselves; (b) use the Shapley [1953] value as a guide in allocating the costs and benefits among members of the security cooperative; or (c) adopt a Buchanan [1965; 1999]-type decentralized group solution in which group members choose its size, the amount of the public goods, and the incentives (i.e., Pigouvian penalties and subsidies).

The simulations illustrate our ideas and make the results of the model more concrete.

De La Salle University

References

Buchanan, James [1965] "An economic theory of clubs", *Economica* **32**: 1–14.

Buchanan, James [1999] "Three research programs in constitutional political economy: discussion of political science and economics" in: J. Alt, M. Levi, and E. Ostrom, eds., *Competition and cooperation: conversations with nobelists about economics and political science*. New York: Russel Sage Foundation.

Cavusoglu, H., B. Mishra, and S. Raghunathan [2004] "The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers", *International Journal of Electronic Commerce* **9**: 69–104, http://info.freeman.tulane.edu/huseyin/paper/market.pdf.

Cisco Systems, Inc. 2004. "White paper: defeating DDOS attacks", http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.pdf. Accessed 17 April 2014.

Coyne, C. J. and P. T. Leeson [2005] "Who's to protect cyberspace?" *Journal of Law, Economics and Policy* 1(2): 473-496.

Fabella, R. V. [2005] "A Nozick-Buchanan contractarian governance as solution to some invisible hand failures", *Quarterly Review of Economics and Finance* **45**: 284–295.

Garg, A., J. Curtis, and H. Halper [2003] "The financial impact of IT security breaches: what do investors think", *Info Systems Security*, http://www.auerbach-publications.com/dynamic_data/2466_1358_cost.pdf.

Granot, D. and G. Huberman [1981] "Minimum cost spanning tree games", *Mathematical Programming* **21**: 1–18.

Granot, D. and G. Huberman [1984] "On the core and nucleolus of minimum cost spanning tree games", *Mathematical Programming* **29**: 323–347.

Heal, G. and H. Kunreuther [2003] "You only die once: managing discrete interdependent risks", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=419240.

Kesan, J. and R. Majuca [2006] "Cybercrimes and cyber-attack: technological, economic, and law-based solutions" in: *Cybercrime & Security*. Oceana Law.

Kobayashi, B. H. [2005] "An economic analysis of the private and social costs of the provision of cybersecurity and other public security goods", *Supreme Court Economic Review* **14**.

Littlechild, S. [1974] "A simple expression for the nucleolus in a special case", *International Journal of Game Theory* **3**: 21–29.

Littlechild, S. and G. Owen [1973] "A simple expression for the Shapley value in a special case", *Management Science* **20**: 370–372.

Mas-Colell, A., M. D. Whinston, and J. R. Green [1995] *Microeconomic theory*. New York, NY: Oxford University Press.

Megiddo, N. [1978] "Cost allocation for Steiner trees", *Networks* **8**: 1–6.

Orszag, P. and J. Stiglitz [2002] "Optimal fire departments: evaluating public policy in the face of externalities", *Brooking Working Paper*, February.

Pauly, M. V. [1967] "Clubs, commonality, and the core: an integration of game theory and the theory of public goods", *Economica* **34**: 314–324.

Pauly, M. V. [1970] "Cores and clubs", *Public Choice* **9**: 53–65.

Powell, B. [2005] "Is cybersecurity is a public good? Evidence from the financial services industry", Working Paper 57, Independent Institute, Oakland, CA.

Shapley, L. [1953] "A value of *n*-person games", *Annals of Mathematics Studies* **28**: 307–318.

Shavell, S. [1987] *Economic analysis of accident law*.

Shavell, S. [1991] "Individual precautions to prevent theft: private versus socially optimal behavior", *International Review of Law and Economics* **11**: 123–132.

Suzuki, M. and M. Nakayama [1976] "The cost assignment of the cooperative water resource development: a game theoretical approach", *Management Science* **22**: 1081–1086.

Varian, H. R. [1992] *Microeconomic analysis.* Third edition. W. W. Norton & Company.

Young, H., N. Okada, and T. Hashimoto [1982] "Cost allocation in water resources development", *Water Resources Research* **18**: 463–475.

APPENDIX A. Proofs of propositions

1. The social planner's solution

The social planner's problem

$$\min_{\{x,\, y_T,\, z\}} n\Big[f(x)+g(z)\Big]+y_T+h\cdot\Big[c\Big(e(\mathbf{x},\, y_T(\mathbf{y}),\, z)+e(\mathbf{x},\, y_T(\mathbf{y}),\, z)\cdot s(\mathbf{x},\, y_T(\mathbf{y}),\, z)\Big)\Big] \tag{A-1}$$

First-order conditions

$$\{x\}\; nf'(x)+h\cdot\{c'\cdot(e_{x_1}+e_{x_2}+\ldots+e_{x_n})+e\cdot(s_{x_1}+s_{x_2}+\ldots+s_{x_n})+s\cdot(e_{x_1}+e_{x_2}+\ldots+e_{x_n})\}=0 \tag{A-2}$$

$$\{y_T\}\qquad 1+h\cdot\{c'\cdot e_{y_T}+e\cdot s_{y_T}+s\cdot e_{y_T}\}=0 \tag{A-3}$$

$$\{z\}\qquad ng'(z)+h\cdot\{c'\cdot e_z+e\cdot s_z+s\cdot e_z\}=0 \tag{A-4}$$

Applying $c'=g$; $s=L-g$; $p=(h/n)e \Rightarrow e=(np/h)$, $e_{x_1}=(n/h)p_{x_1}$, etc. , we have

$$-\left(\sum_{i=1}^{n}p_{x_i}\right)\cdot L+p\cdot\left(\sum_{i=1}^{n}s_{x_i}\right)=f'(x) \tag{A-5}$$

$$-n(p_{y_T}L+ps_{y_T})=1 \tag{A-6}$$

$$-p_z\cdot L-p\cdot s_z=g'(z) \tag{A-7}$$

Dividing equations (A-5) and (A-6) by $f'(x)$ and $g'(z)$, respectively, proves Proposition 1.

2. The individual solution

The individual firm's optimization problem

Arbitrarily assign index 1 to the individual firm. Given $([x_i],\,[y_i]\,,\,z\}$, $i\neq 1$, find $(x_1,\,y_1)$ that solves:

$$\min p\Big(x_1,[x_i],\,y_T\,(y_1,[y_i]),\,z\Big)\cdot L\Big(x_1,[x_i],\,y_T\,(y_1,[y_i]),\,z\Big)+f(x_1)+y_1+g(z) \tag{A-8}$$

First-order conditions

$$\{x_1\}\qquad -p_{x_1}\cdot L-p\cdot L_{x_1}=f'(x) \tag{A-9}$$

$$\{y_1\}\qquad -p_{y_T}\cdot L-p\cdot L_{y_T}=1 \tag{A-10}$$

Totally differentiating the first-order conditions and imposing symmetry, we have:

$$\left[\left(\sum_{i=1}^{n} p_{x_1 x_i}\right)\cdot L + p_{x_1}\cdot\left(\sum_{i=1}^{n} L_{x_i}\right) + \left(\sum_{i=1}^{n} p_{x_i}\right)\cdot L_{x_1} + p\cdot\left(\sum_{i=1}^{n} L_{x_1 x_i}\right) + f''(x)\right]\cdot dx$$
$$+ n\cdot\left[p_{x_1 y_T}\cdot L + p_{x_1}\cdot L_{y_T} + p_{y_T}\cdot L_{x_1} + p\cdot L_{x_1 y_T}\right]\cdot dy$$
$$+ \left[p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p\cdot L_{x_1 z}\right]\cdot dz = 0 \qquad \text{(A-11)}$$

$$\left[\left(\sum_{i=1}^{n} p_{y_T x_i}\right)\cdot L + p_{y_T}\cdot\left(\sum_{i=1}^{n} L_{x_i}\right) + \left(\sum_{i=1}^{n} p_{x_i}\right)\cdot L_{y_T} + p\cdot\left(\sum_{i=1}^{n} L_{y_T x_i}\right)\right]\cdot dx$$
$$+ n\cdot\left[p_{y_T y_T}\cdot L + p_{y_T}\cdot L_{y_T} + p_{y_T}\cdot L_{y_T} + p\cdot L_{y_T y_T}\right]\cdot dy$$
$$+ \left[p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p\cdot L_{y_T z}\right]\cdot dz = 0 \qquad \text{(A-12)}$$

Comparing (A-11) and (A-12) with (A-5) and (A-6) and setting $L=s$ prove Propositions 2 and 3.

Assuming that the determinant of the coefficient matrix at $\{x^*,...,x^*,y^*,...,y^*,z\}$ is non-zero, by the implicit function theorem, we have:

$$dx = -dx\cdot\frac{\left\{\begin{array}{l}\left[p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p\cdot L_{x_1 z}\right]\cdot\left[n\cdot\left(\begin{array}{l} p_{y_T y_T}\cdot L + p_{y_T}\cdot L_{y_T} \\ + p_{y_T}\cdot L_{y_T} + p\cdot L_{y_T y_T}\end{array}\right)\right] \\ -\left[p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p\cdot L_{y_T z}\right]\cdot\left[n\cdot\left(\begin{array}{l} p_{x_1 y_T}\cdot L + p_{x_1}\cdot L_{y_T} \\ + p_{y_T}\cdot L_{x_1} + p\cdot L_{x_1 y_T}\end{array}\right)\right]\end{array}\right\}}{D} \qquad \text{(A-13)}$$

and

$$dy = -dz\cdot\frac{\left\{\begin{array}{l}\left[p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p\cdot L_{y_T z}\right]\cdot\left(\begin{array}{l}\left(\sum_{i=1}^{n} p_{x_1 x_i}\right)\cdot L + p_{x_1}\cdot\left(\sum_{i=1}^{n} L_{x_i}\right) \\ +\left(\sum_{i=1}^{n} p_{x_i}\right)\cdot L_{x_1} + p\cdot\left(\sum_{i=1}^{n} L_{x_1 x_i}\right) + f''(x)\end{array}\right) \\ -\left[p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p\cdot L_{x_1 z}\right]\cdot\left(\begin{array}{l}\left(\sum_{i=1}^{n} p_{y_T x_i}\right)\cdot L + p_{y_T}\cdot\left(\sum_{i=1}^{n} L_{x_i}\right) \\ +\left(\sum_{i=1}^{n} p_{x_i}\right)\cdot L_{y_T} + p\cdot\left(\sum_{i=1}^{n} L_{y_T x_i}\right)\end{array}\right)\end{array}\right\}}{D} \qquad \text{(A-14)}$$

where

$$D = \left\{\begin{array}{l}\left(\begin{array}{l}\left(\sum_{i=1}^{n} p_{x_1 x_i}\right)\cdot L + p_{x_1}\cdot\left(\sum_{i=1}^{n} L_{x_i}\right) + \left(\sum_{i=1}^{n} p_{x_i}\right)\cdot L_{x_1} + p\cdot\left(\sum_{i=1}^{n} L_{x_1 x_i}\right) + f''(x)\cdot \\ n\cdot\left[p_{y_T y_T}\cdot L + p_{y_T}\cdot L_{y_T} + p_{y_T}\cdot L_{y_T} + p\cdot L_{y_T y_T}\right]\end{array}\right) \\ -\left(\begin{array}{l} n\cdot\left[p_{x_1 y_T}\cdot L + p_{x_1}\cdot L_{y_T} + p_{y_T}\cdot L_{x_1} + p\cdot L_{x_1 y_T}\right]\cdot \\ \left(\sum_{i=1}^{n} p_{y_T x_i}\right)\cdot L + p_{y_T}\cdot\left(\sum_{i=1}^{n} L_{x_i}\right) + \left(\sum_{i=1}^{n} p_{x_i}\right)\cdot L_{y_T} + p\cdot\left(\sum_{i=1}^{n} L_{y_T x_i}\right)\end{array}\right)\end{array}\right\} \qquad \text{(A-15)}$$

$(dx/dz) < 0$ and $(dy/dz) < 0$ under conditions discussed in Proposition 5.

The government's optimization problem

The government chooses z in order to

$$\min n\Big[f(x^*(z)) + y^*(z) + g(z)\Big] + h\Big[c\Big(e(\mathbf{x}^*(z), y_T(\mathbf{y}^*(z)),\ z\Big) + e\Big(\mathbf{x}^*(z), y_T(\mathbf{y}^*(z),\ z\Big) \cdot s\Big(\mathbf{x}^*(z), y_T(\mathbf{y}^*(z),\ z\Big)\Big] \tag{A-16}$$

First-order condition

$$n \cdot [f' \cdot (\partial x^*/\partial z) + (\partial y^*/\partial z) + g'(z)] + h \cdot \Big[c'(e) \cdot \Big(\Big(\sum_{i=1}^{n} e_{x_i}\Big) \cdot (\partial^* x/\partial z) + n \cdot e_{y_T}(\partial^* y/\partial z) + e\Big)\Big] + h \cdot e\Big(\Big(\sum_{i=1}^{n} s_{x_i}\Big) \cdot (\partial x^*/\partial z) + n \cdot s_{y_T}(\partial y^*/\partial z) + s_z\Big) + h \cdot s\Big(\Big(\sum_{i=1}^{n} e_{x_i}\Big) \cdot (\partial^* x/\partial z) + n \cdot e_{y_T}(\partial^* y/\partial z) + e_z\Big) = 0. \tag{A-17}$$

Solving for $g'(z)$, we have:

$$-p_z L - ps_z - (\partial x^*/\partial z)\Big[f'(x) + \Big(\sum_{i=1}^{n} p_{x_i}\Big) \cdot L + p \cdot \Big(\sum_{i=1}^{n} s_{x_i}\Big)\Big] - (\partial y^*/\partial z)[1 + n \cdot p_{y_T} L + n \cdot ps_{y_T}] = g'(z) \tag{A-18}$$

Substituting in for the firm's first-order conditions, we have:

$$-p_z L - ps_z - (\partial x^*/\partial z)\Big[\Big(\sum_{i=2}^{n} p_{x_i}\Big) \cdot L + p \cdot \Big(\sum_{i=2}^{n} L_{x_i}\Big) - p\Big(\sum_{i=1}^{n} g_{x_i}\Big)\Big] - (\partial y^*/\partial z)[(n-1) \cdot p_{y_T} L + (n-1) \cdot pL_{y_T} - n \cdot pg_{y_T}] = g'(z) \tag{A-19}$$

Comparing (A-19) with the socially optimal case proves Proposition 6.

3. The cooperative solution

The cooperative's optimization problem

$$\min_{\{x,\, y_T\}} n \cdot p(\mathbf{x}, y_T(\mathbf{y}),\ z) \cdot L(\mathbf{x}, y_T(\mathbf{y}),\ z) + n \cdot f(x) + y_T(\mathbf{y}) + n \cdot g(z) \tag{A-20}$$

First-order conditions

$$\{x\} \qquad -\Big[\Big(\sum_{i=1}^{n} p_{x_i}\Big) \cdot L + p \cdot \Big(\sum_{i=1}^{n} L_{x_i}\Big)\Big] = f'(x) \tag{A-21}$$

$$\{y_T\} \qquad -n \cdot \Big[p_{y_T} L + pL_{y_T}\Big] = 1 \tag{A-22}$$

The government's optimization problem

$$\min n\Big[f(x^{**}(z)) + g(z)\Big] + y_T^{**}(y^{**}(z)) + h\Big[c\Big(e(\mathbf{x}^{**}(z), y_T^{**}(\mathbf{y}^{**}(z)),\ z\Big) + e\Big(\mathbf{x}^{**}(z), y_T^{**}(\mathbf{y}^{**}(z),\ z\Big) \cdot s\Big(\mathbf{x}^{**}(z), y_T^{**}(\mathbf{y}^{**}(z),\ z\Big)\Big] \tag{A-23}$$

First-order conditions

$$-p_z L - ps_z - (\partial x^{**}/\partial z)\left[f'(x) + L\Big(\sum_{i=1}^{n} p_{x_i}\Big) + p \cdot \Big(\sum_{i=1}^{n} s_{x_i}\Big)\right] - (\partial y^{**}/\partial z)[1 + n \cdot p_{y_T} L + n \cdot ps_{y_T}] = g'(z) \tag{A-24}$$

Substituting in the collective's first-order condition (and if $L = s$), this reduces to

$$-p_z L - ps_z = g'(z), \tag{A-25}$$

which proves Proposition 7.

APPENDIX B. Derivations of the first, second, and cross-partial derivatives used in section 4 figures

$$L_{x_1} = A\left[(1-q)ax_1^{a-1}y_T^{a}z^{c} + qax_1^{a-1}y_T^{a}(x_2y_T)^{b}z^{c}\right] \tag{B-1}$$

$$L_{x_2} = Aq(x_1y_T)^{a}bx_2^{b-1}y_T^{b}z^{c} \tag{B-2}$$

$$L_{y_T} = A\left[(1-q)x_1^{a}ay_T^{a-1}z^{c} + qx_1^{a}x_2^{b}(a+b)y_T^{a+b-1}z^{c}\right] \tag{B-3}$$

$$L_{z} = A\left[(1-q)(x_1y_T)^{a}cz^{c-1} + q(x_1y_T)^{a}(x_2y_T)^{b}cz^{c-1}\right] \tag{B-4}$$

$$p_{x_1} = -\alpha y_T \cdot [(1-q)\cdot e^{-(\alpha x_1y_T+\theta z)} + q\cdot e^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}] \tag{B-5}$$

$$p_{x_2} = -\beta y_T \cdot [q\cdot e^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}] \tag{B-6}$$

$$p_{y_T} = -\alpha x_1(1-q)e^{-(\alpha x_1y_T+\theta z)} - (\alpha x_1+\beta x_2)qe^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)} \tag{B-7}$$

$$p_{z} = -\theta[(1-q)\cdot e^{-(\alpha x_1y_T+\theta z)} + q\cdot e^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}] \tag{B-8}$$

$$L_{x_1x_1} = A\left[(a-1)(1-q)ax_1^{a-2}y_T^{a}z^{c} + qa(a-1)x_1^{a-2}y_T^{a}(x_2y_T)^{b}z^{c}\right] \tag{B-9}$$

$$L_{x_1x_2} = Aqax_1^{a-1}y_T^{a}bx_2^{b-1}y_T^{b}z^{c} \tag{B-10}$$

$$L_{x_1y_T} = A\left[(1-q)ax_1^{a-1}ay_T^{a-1}z^{c} + qax_1^{a-1}x_2^{b}(a+b)y_T^{a+b-1}z^{c}\right] \tag{B-11}$$

$$L_{x_1z} = A\left[(1-q)ax_1^{a-1}y_T^{a}cz^{c-1} + qax_1^{a-1}y_T^{a}(x_2y_T)^{b}cz^{c-1}\right] \tag{B-12}$$

$$p_{x_1x_1} = (\alpha y_T)^2\left[(1-q)e^{-(\alpha x_1y_T+\theta z)} + qe^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}\right] = (\alpha y_T)^2\cdot p \tag{B-13}$$

$$p_{x_1x_2} = (\alpha y_T)(\beta y_T)\left[qe^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}\right] \tag{B-14}$$

$$p_{x_1y_T} = -\alpha[(1-q)e^{-(\alpha x_1y_T+\theta z)} + qe^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}]$$

$$-(\alpha y_T)[(1-q)e^{-(\alpha x_1y_T+\theta z)}(-\alpha x_1)+qe^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}(-\alpha x_1-\beta x_2)]$$

$$= -\alpha\cdot p - (\alpha y_T)\cdot p_{y_T} \tag{B-15}$$

$$p_{x_1z} = -(\alpha y_T)\left[(1-q)e^{-(\alpha x_1y_T+\theta z)}(-\theta)+qe^{-(\alpha x_1y_T+\beta x_2y_T+\theta z)}(-\theta)\right] = -(\alpha y_T)\cdot p_z \tag{B-16}$$