

Public Goods and Externalities Aspects of Internet Security: Modeling the Spill-over Effects of Interrelated Risks and Solutions

Ruperto Majuca

<RupertoMajuca@weber.edu>
Weber State University
Department of Economics

ABSTRACT

Is Internet security a public good? How should society handle the spill-over effects arising from the interrelatedness of Internet risks? What role, if any, does police enforcement play? What optimal combination of each of these security measures – police enforcement, and individual investments in both private and non-rivalrous security goods – should be used to effectively combat cybercrimes?

In this paper, I argue that some, but not all, investments in security have the nature of public goods. Thus, I attempt to model the situation where firms invest in both private and public security goods. Furthermore, I include public enforcement of law in my model. Thus, I study a model where crimes are addressed through a combination of private and public measures. By so doing, I hope to capture the substitutability between the private and public responses, and determine the optimal combination of these approaches. Lastly, my model seeks to capture the interrelatedness of risks in the Internet. In sum, in this paper, I study a model that combines all of these elements: private investments in security; investments in security that have the nature of public goods; externalities; and public enforcement of law.

I 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, non-rivalrous security investment, and law enforcement measures. Furthermore, the interrelatedness of Internet risks causes individual firms to underinvest in private and public security goods. The government thus decidedly lowers the level of police enforcement expenditures in order to induce firms to invest more in individual precautions. I also find that, under certain conditions, cooperation results in socially-optimal levels of expenditures in private and public security goods expenditures. The Shapley (1953) value can be used as a criterion for allocating the costs and benefits among the members of a security cooperative. Several simulations illustrate the results of the model under several scenarios.

Keywords: Internet security, interrelated risks, public security goods, public enforcement of law

Draft version: August 31, 2006

1. INTRODUCTION

Is Internet security a public good? How should society handle the spill-over effects arising from the interrelatedness of Internet risks? What role, if any, does police enforcement play? What optimal combination of each of these security measures – police enforcement, and individual investments in both private and non-rivalrous security goods – should be used to effectively combat cybercrimes?

In this paper, I argue that some, but not all, investments in security have the nature of public goods. 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.” (MasColell, Whinston, and Green 1995, p. 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.¹ Classic examples are national defense, police protection, lighthouses, public parks, information and knowledge, clean air, etc. In contrast, private goods are goods “whose consumption only affects a single economic agent” (Varian 1992, p. 414). Classic examples of private goods are bread, shoes, etc.

On the basis of the above definition, I argue that Internet security has both public and private goods aspects. Insofar as everyone shares common available risks (has a common pool of hackers and 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], anti-virus, security authentication codes, etc.); or (b) investments in non-rivalrous 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 below).

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

¹ 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, p. 360) For simplicity, I will abstract from the issue of excludability.

Another important consideration is that, in the Internet, there is significant interrelatedness of risks giving rise to externalities among individual websites. For example, if an individual does not use an anti-virus 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 spill-over effects to other Internet users (the public).

Thus, in this paper, I study a model that combines all of these elements (see Figure 1):

- private investments in security;
- investments in security that have the nature of public goods;
- externalities; and
- public enforcement of law.

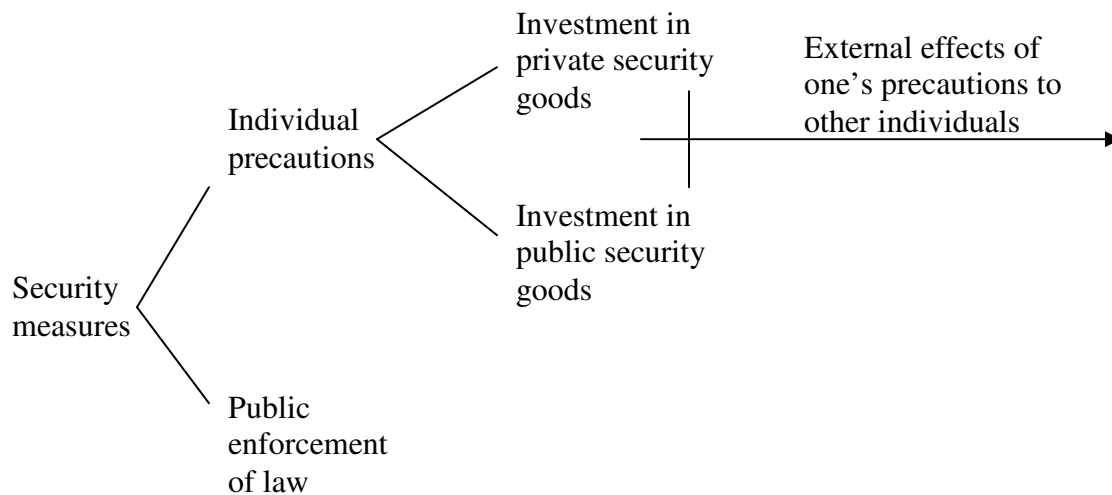


Figure 1. Elements of the model

That is, I model the situation where firms invest in both private and public security goods, when there is public enforcement of law against hackers. The previous studies that have analyzed private security expenditures as a way to protect against crimes have modeled private precautions but leave out public enforcement of law in their models (Shavell 1991, Kobayashi 2005). 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 incidents, while investments in individual precautions reduce the effectiveness of criminals in causing harm to the victims. In this paper, I study a model where crimes are addressed through a combination of private and public measures. By so doing, I hope to capture the substitutability between the private and public responses, and determine what is the optimal combination of these approaches.

Although past studies have looked at some of the aspects mentioned in Figure 1 individually and in isolation – for example, Heal and Kunreather (2003) has looked at interrelatedness of risks, e.g., in the context of terrorism and computer security; Shavell (1991) has looked at investments in rivalrous 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) – none of these studies have looked at all the elements mentioned above together. Looking at these elements together, I think, 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 cyber-attacks. Also, by modeling the collective solution, I aim to examine what role, if any, cooperation plays in Internet security.

I find that just because Internet security has public goods aspect 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 entirely to the government the function of providing Internet security is that such a solution is susceptible to the well-known problem of “government failure”. On the other hand, the problem with adopting an entirely private solution is that such is susceptible to the problem of “market failure”: the externalities and public goods aspect of Internet security results in the divergence between the private solution and the socially-optimal solution. The solution therefore, I think, is a careful balance between private and public measures. Which brings us to the next result.

How then should society achieve and optimal allocation of security investments across the various public and private alternatives? I find that the socially-optimal level of security is achieved by combining private security investment, non-rivalrous 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 the private and public security good investments are greater than the marginal *private* benefits because individuals don’t take into account the spill-over effects their own security investments have on other computer systems, resulting in an underinvestment of both non-rivalrous and rivalrous security goods. Additionally, I find that in certain situations it would be optimal for the government to deliberately lower the level of police enforcement in order to induce firms to invest more in individual precautions.

Lastly, I 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 thus 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 as 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 further buttresses the conclusion that even if there is a market failure arising from public goods and externalities aspects of Internet security, it does not necessarily mean that government role is automatically prescribed to the exclusion of the

private sector. Since under certain conditions the collective solution will approximate the socially-optimal solution, then some form decentralized group solution can be utilized in certain cases to help address the problem of Internet security. The situation I envision is some form of a group formation of the Buchanan (1965, 1999) type where 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, which shows how contractarian governance can, under certain conditions, restore Pareto optimality in situations that would otherwise have resulted in an invisible hand failure). 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.

I illustrate my results with specific functional forms and simulations.

Section 2 presents the model. Section 3 discusses the socially-optimal solution to the problem. Section 4 considers the individual's private solution, while Section 5 delves into the cooperative solution of the model. Section 6 presents specific examples, illustrations of specific functional forms, as well as some simulations. Section 7 presents the conclusions and summary of the paper.

2. THE MODEL

In this section, I study a model of 2 symmetric risk-neutral firms and h identical risk-neutral hackers, and in the Appendix generalize the model to n firms. Hacking requires an effort level e to each hacker, while firm 1 and firm 2 spend, respectively, x_1 and x_2 on private security goods, and y_1 and y_2 on public security goods. The government decides on the level of police enforcement expenditures, z . The hacking effort costs $c(e)$, while the cost of individual investments in private security goods, and the cost (per firm) of maintaining the police force, are respectively $f(x)$ and $g(z)$, where $f'(x) > 0$, $f''(x) \geq 0$, $g'(z) > 0$, and $g''(z) \geq 0$ by assumption. The cost per unit of non-rivalrous security goods are normalized to 1 for simplicity.

The hacker's optimization problem is

$$\underset{e}{\text{Max}} G(e, x_1, x_2, y_T(y_1, y_2), z) = e \cdot g(x_1, x_2, y_T(y_1, y_2), z) - c(e), \quad (1)$$

where $g(\cdot)$ is the hacker's gain from hacking, $c(e)$ is the cost of the effort to the hacker, and y_T , the total amount of non-rivalrous security goods available to both firms, equals $y_1 + y_2$. 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_1 , x_2 , y_T , and z , i.e., $\frac{\partial g}{\partial x_1} < 0$,

$\frac{\partial g}{\partial x_2} < 0$, $\frac{\partial g}{\partial y_T} < 0$, $\frac{\partial g}{\partial z} < 0$, $\frac{\partial^2 g}{\partial x_1^2} > 0$, $\frac{\partial^2 g}{\partial x_2^2} > 0$, $\frac{\partial^2 g}{\partial y_T^2} > 0$, and $\frac{\partial^2 g}{\partial z^2} > 0$. I further assume that $c'(e) > 0$ and $c''(e) > 0$.

The hacker's first-order condition is $g(x_1, x_2, y_T(y_1, y_2), z) = c'(e)$, which defines $e = e(x_1, x_2, y_T(y_1, y_2), z)$ implicitly. Hence,

$$g(x_1, x_2, y_T(y_1, y_2), z) = c'(e(x_1, x_2, y_T(y_1, y_2), z)), \text{ and } \frac{\partial g}{\partial x_1} = c'' \cdot \frac{\partial e}{\partial x_1} \Rightarrow \frac{\partial e}{\partial x_1} = \frac{\frac{\partial g}{\partial x_1}}{c''} < 0;$$

$$\frac{\partial g}{\partial x_2} = c'' \cdot \frac{\partial e}{\partial x_2} \Rightarrow \frac{\partial e}{\partial x_2} = \frac{\frac{\partial g}{\partial x_2}}{c''} < 0; \text{ and } \frac{\partial g}{\partial z} = c'' \cdot \frac{\partial e}{\partial z} \Rightarrow \frac{\partial e}{\partial z} = \frac{\frac{\partial g}{\partial z}}{c''} < 0. \text{ That is, the effort}$$

level of the hacker decreases, *ceteris paribus*, with an increase in any of the security measures.

Define $p(x_1, x_2, y_T(y_1, y_2), z)$ to be the probability of the loss, $L(x_1, x_2, y_T(y_1, y_2), z)$ to be the magnitude of loss, and $s(x_1, x_2, y_T(y_1, y_2), z) = L - g$ to be the deadweight social welfare loss from hacking.

Police enforcement and private precautions lower the probability of one's sites being attacked, thus:

$$p_z(x_1, x_2, y_T(y_1, y_2), z) < 0 \quad (2)$$

$$p_{x_1}(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (3)$$

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

$$L_{x_1}(x_1, x_2, y_T(y_1, y_2), z) < 0 \quad (4)$$

$$L_z(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (5)$$

Also, as mentioned, in the Internet, security is interdependent. The lack of security in a network can cause damage not only to that network, but also to other networks linked to it. 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). Neglect by an individual 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 other systems as well. For example, if a computer administrator regularly uses anti-virus 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

emails with virus attachments. A person who does not anti-virus does not affect his/her machine only, since many viruses are programmed to be sent to others in the email group. Had the person used an anti-virus software and not been infected, the others would not have been infected also. Thus,

$$p_{x_2}(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (6)$$

I also assume that one's private security expenditures also reduce the amount of others' loss. 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 websites 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 to the attacked site depends, among others, on the length of time of the attack and number of computers from where the attacks are staged. In essence, this implies that

$$L_{x_2}(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (7)$$

Finally, I assume that the following hold with respect the second and cross-partial derivatives:

$$p_{x_1x_2}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (8)$$

$$p_{x_1z}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (9)$$

$$L_{x_1x_2}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (10)$$

$$L_{zz}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (11)$$

$$L_{x_1z}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (12)$$

$$p_{zz}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (13)$$

$$p_{x_1x_1}(x_1, x_2, y_T(y_1, y_2), z) > 0. \quad (14)$$

3. THE SOCIALLY-OPTIMAL SOLUTION

Proposition 1. The socially-optimum level of security is achieved by equalizing the marginal benefit to marginal cost ratios of each of the three alternatives -- private security investment, non-rivalrous security investment, and law enforcement measures.

Proof. The social planner's problem is

$$\begin{aligned} \text{Min} \quad & 2[f(x) + g(z)] + y_T + h \cdot \{c[e(x_1, x_2, y_T(y_1, y_2), z)] + e(x_1, x_2, y_T(y_1, y_2), z) \cdot s(x_1, x_2, y_T(y_1, y_2), z)\} \\ & \{x, y_T, z\} \end{aligned} \quad (15)$$

The first-order conditions are:

$$\{x\} \quad 2f'(x) + h \cdot \{c' \cdot (e_{x_1} + e_{x_2}) + e \cdot (s_{x_1} + s_{x_2}) + s \cdot (e_{x_1} + e_{x_2})\} = 0 \quad (16)$$

$$\{y_T\} \quad 1 + h \cdot \{c' \cdot e_{y_T} + e \cdot s_{y_T} + s \cdot e_{y_T}\} = 0 \quad (17)$$

$$\{z\} \quad 2g'(z) + h \cdot \{c' \cdot e_z + e \cdot s_z + s \cdot e_z\} = 0. \quad (18)$$

From the hacker's first-order conditions, we know that $c' = g$ and by definition we have $s = L - g$ and $p = \frac{h}{2}e$. Substituting these into (16), (17) and (18), we know that, respectively,

$$-(p_{x_1} + p_{x_2})L - p(s_{x_1} + s_{x_2}) = f'(x) \quad (19)$$

$$-2(p_{y_T}L + ps_{y_T}) = 1 \quad (20)$$

$$-p_z \cdot L - p \cdot s_z = g'(z) \quad (21)$$

The first term in equation (19), $-(p_{x_1} + p_{x_2})L$ represents the total marginal *diversion effect*. That is, because of the observable precaution, the probability of intrusion of a website is reduced as hackers are diverted to other sites that don't have the observable precautions. Hence, the overall expected amount of loss caused by the hacker decreases as a result of installing observable precautions. In contrast to the standard results where the marginal diversion effect equals $-p_{x_1}L$ (see Shavell 1991, p. 129), here, because of the interrelated of the security, the overall diversion effect has to account for the reduction in the probability of intrusion of a website as a result of the investments of security by the other website, $-p_{x_2}L$.

The second term in equation (19), $-p(s_{x_1} + s_{x_2}) = 1$, represents the marginal *social waste reduction effect* – it captures the expected reduction in the amount of deadweight social welfare loss as a result of the security investment. By definition, this term can be decomposed into the expected amount stolen from the firm, $-p(L_{x_1} + L_{x_2})$, i.e., the marginal *theft reduction effect* in Shavell (1991)'s terminology, *minus* the expected reduction of the gain to the hacker, $-p(g_{x_1} + g_{x_2})$. As evident from the first part of this decomposition, a website benefits from the security investment of another website which reduces the amount stolen from the first website. For example, in many cases, where compromised computers can be used to intrude into the target website, a stronger security infrastructure would decrease the amount of time the hacker would have to steal the target website's computer systems.

Thus, in contrast to previous results, equation (19) shows that with the 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 website.

Dividing equations (19) and (21) by $f'(x)$ and $g'(z)$, respectively, proves the proposition. Hence, under the socially-optimal solution, the marginal benefit to marginal cost ratios of the private security good, the public security good, and law enforcement measures are equalized:

$$\frac{-(p_{x_1} + p_{x_2})L - p(s_{x_1} + s_{x_2})}{f'(x)} = \frac{-2(p_{y_T}L + ps_{y_T})}{1} = \frac{-p_z \cdot L - p \cdot s_z}{g'(z)} \quad (22)$$

Corollary 1. The more responsive the probability and 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.

Proof. Note that equation (22) can be rewritten in elasticity form. Thus, defining $\varepsilon_{p_1} = \frac{\partial p}{\partial x} \cdot \frac{x}{p}$, and defining ε_{p_2} , ε_{s_1} , ε_{s_2} , ε_{p_1} , $\varepsilon_{s_{y_1}}$, $\varepsilon_{s_{y_2}}$, $\varepsilon_{p_{y_1}}$, $\varepsilon_{p_{y_2}}$, ε_{f_y} , ε_{p_z} , ε_{s_z} , and ε_{g_z} analogously, equation (22) becomes:

$$\frac{\left\{ \begin{array}{l} -\frac{pL}{x} \cdot (\varepsilon_{p_1} + \varepsilon_{p_2}) \\ -\frac{ps}{x} \cdot (\varepsilon_{s_1} + \varepsilon_{s_2}) \end{array} \right\}}{\frac{f}{x} \cdot \varepsilon_{f_x}} = \frac{\left\{ -2 \left[\frac{pL}{x} \cdot \varepsilon_{p_{y_T}} + \frac{ps}{y_T} \cdot \varepsilon_{s_{y_T}} \right] \right\}}{1} = \frac{\left\{ -\frac{pL}{z} \cdot \varepsilon_{p_z} - \frac{ps}{z} \cdot \varepsilon_{s_z} \right\}}{\frac{g}{z} \cdot \varepsilon_{g_z}}. \quad (23)$$

Hence, the social planner adjusts the level of private rivalrous and non-rivalrous security investments, and law enforcement expenditures, in accordance with the 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 responsive is the probability of loss and the social loss to private rivalrous investment, the higher is the optimal level of private rivalrous investment. The same thing applies to private non-rivalrous security investments, and the public expenditures on law enforcement. This is akin to price discrimination by a monopolist who sells in different markets, and charges price according to the price elasticity of demand in these markets. Of course, in the present security case, the social planner also needs to take into account the responsiveness of the costs to these changes in the level of the different security measures.

4. THE INDIVIDUAL SOLUTION

Proposition 2. The interrelatedness of the risks causes individual firms to underinvest in private security.

Proof. Given the level of police enforcement and the firm 2's level of private and public security investments, firm 1 chooses x and y to:

$$\begin{array}{l} \text{Min } p(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) + f(x_1) + y_1 + g(z) \\ \{x_1, y_1 \mid x_2, y_2, z\} \end{array} \quad (24)$$

where $y_T = y_1 + y_2$

The first-order (optimality) conditions are:

$$\begin{aligned} \{x_1\} & - p_{x_1}(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) \\ & - p(x_1, x_2, y_T(y_1, y_2), z) \cdot L_{x_1}(x_1, x_2, y_T(y_1, y_2), z) = f'(x) \end{aligned} \quad (25)$$

$$\begin{aligned} \{y_1\} & - p_{y_1}(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) \\ & - p(x_1, x_2, y_T(y_1, y_2), z) \cdot L_{y_1}(x_1, x_2, y_T(y_1, y_2), z) = 1 \end{aligned} \quad (26)$$

Comparing equation (19) with (25) proves the proposition.

For the firm, the motivation behind investing in precaution (marginal benefit) is the reduction in the expected cost of the harm to it. Equation (26) states that, for individual precaution 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.

Equation (26) implies that

$$1 = -\frac{pL}{x}(\varepsilon_p + \varepsilon_l) \quad (27)$$

where $\varepsilon_p = \frac{\partial p}{\partial x} \cdot \frac{x}{p}$, etc.

Equation (27) says that the individual will equate the 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 one's 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 to the amount of precaution, the higher is the marginal benefit of the precaution, and thus the higher is the optimal level of private precaution.

Proposition 3. The level of public security goods is also underprovided, the public good nature of the security investment causes the divergence of the level of public security expenditures from the socially-optimal amount. However, the externality effect drops out; that is, in the case of public security goods, the positive “externality” of the one's public security good investment to others is “internalized” by the firm in calculating its optimal level of public security goods.

Proof. Comparing (20) with (26) proves the proposition.

At first blush, it may seem that in the case of public security goods, there will both be the free-riding from the public good and the externality effect compounding together to worsen the underinvestment to a large extent. But upon perusal, we see that the “externality effect” drops out of the picture. The reason for this is that the individual already takes into account the positive effect upon him/her of the other person's use of his/her privately provided public security good. It is as if he/she is making the other person as his/her agent (in the legal sense of the word) in that he/she knows that if he/she invests in the public security good, that same good will be available to the other party,

which use of such good will reduce such parties' intrusion, which will then also indirectly benefit the original spender as well.

This is thus one less problem associated with the market solution and one argument in favor of it compared to the government-provided-security alternative.

Proposition 4. The amount of underinvestment in both the private security and public security goods investment worsens as the number of firms increases.

Proof. See the Appendix.

The question that I address next is how a website's choice of x^* and y^* changes with a change in the level of law enforcement expenditures, z .

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

Proof. The second website will face a similar optimization problem as the first website. I assume that the two firms are symmetrical so that $x_1 = x_2$ and $y_1 = y_2$ in equilibrium. Totally differentiating the first-order conditions given in equations (25) and (26), and, imposing symmetry, we arrive at a system of two equations, thus:

$$\begin{aligned} & \left[(p_{x_1x_1} + p_{x_1x_2}) \cdot L + p_{x_1} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{x_1} + p \cdot (L_{x_1x_1} + L_{x_1x_2}) + f''(x) \right] \cdot dx \\ & + 2 \cdot \left[p_{x_1y_T} \cdot L + p_{x_1} \cdot L_{y_T} + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1y_T} \right] \cdot dy \\ & + \left[p_{x_1z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1z} \right] \cdot dz = 0 \end{aligned}$$

$$\begin{aligned} & \left[(p_{y_Ty_T} + p_{y_Ty_2}) \cdot L + p_{y_T} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{y_T} + p \cdot (L_{y_Tx_1} + L_{y_Tx_2}) \right] \cdot dx \\ & + 2 \cdot \left[p_{y_Ty_T} \cdot L + p_{y_T} \cdot L_{y_T} + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_Ty_T} \right] \cdot dy \\ & + \left[p_{y_Tz} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_Tz} \right] \cdot dz = 0 \end{aligned}$$

This is a system of implicit functions. Assuming that the determinant of the coefficient matrix at $\{x^*, x^*, y^*, y^*, z\}$ is non-zero, by the implicit function theorem, we can solve for:

$$dx = -dz \cdot \frac{\begin{pmatrix} \left[p_{x_1z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1z} \right] \cdot \left[2 \cdot \begin{pmatrix} p_{y_Ty_T} \cdot L + p_{y_T} \cdot L_{y_T} \\ + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_Ty_T} \end{pmatrix} \right] \\ - \left[p_{y_Tz} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_Tz} \right] \cdot \left[2 \cdot \begin{pmatrix} p_{x_1y_T} \cdot L + p_{x_1} \cdot L_{y_T} \\ + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1y_T} \end{pmatrix} \right] \end{pmatrix}}{D}$$

and

$$dy = -dz \cdot \frac{\begin{matrix} \left[p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot \left((p_{x_1 x_1} + p_{x_1 x_2}) \cdot L + p_{x_1} \cdot (L_{x_1} + L_{x_2}) \right. \\ \left. + (p_{x_1} + p_{x_2}) \cdot L_{x_1} + p \cdot (L_{x_1 x_1} + L_{x_1 x_2}) + f''(x) \right) \\ - \left[p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1 z} \right] \cdot \left((p_{y_T x_1} + p_{y_T x_2}) \cdot L + p_{y_T} \cdot (L_{x_1} + L_{x_2}) \right. \\ \left. + (p_{x_1} + p_{x_2}) \cdot L_{y_T} + p \cdot (L_{y_T x_1} + L_{y_T x_2}) \right) \end{matrix}}{D}$$

where

$$D = \begin{matrix} \left(\left[(p_{x_1 x_1} + p_{x_1 x_2}) \cdot L + p_{x_1} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{x_1} + p \cdot (L_{x_1 x_1} + L_{x_1 x_2}) + f''(x) \right] \cdot \right. \\ \left. 2 \cdot \left[p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \right] \right) \\ - \left(\left[(p_{y_T x_1} + p_{y_T x_2}) \cdot L + p_{y_T} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{y_T} + p \cdot (L_{y_T x_1} + L_{y_T x_2}) \right] \cdot \right. \\ \left. 2 \cdot \left[p_{x_1 y_T} \cdot L + p_{x_1} \cdot L_{y_T} + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1 y_T} \right] \right) \end{matrix}$$

From the equations above, it is clear that $\frac{dx}{dz} < 0$ $\left(\frac{dy}{dz} < 0 \right)$, so long as it is not the case

that both (a) the cross effects between x and y are so great and (b) the elasticity of substitution between z and y (z and x) is much greater than that between z and x (z and y), as to overwhelm the effect of reduction x (y) as a result of increase in z . Thus, in general, public expenditures on law enforcement has a moral hazard effect: if reduces the propensity of firms of invest in private and public security goods for its own protection.

Proposition 6. (a) The government decidedly lowers the level of police enforcement in order to induce private firms to invest more in individual precautions. (b) As the number of firms, n , increases, and the amount of the underinvestment in private and public security goods investment correspondingly increase, the government also tailor-fits its adjustment according to the size of the underinvestment.

Proof. Imposing symmetry, we have $x_1^* = x_2^* = x^*$ and $y_1 = y_2 = y^*$, which are both functions implicitly of z .

The government thus chooses z in order to

$$\begin{aligned} \text{Min } & 2 \cdot [f(x^*(z)) + y^*(z) + g(z)] \\ & + h \cdot \left\{ c [e(x^*(z), x^*(z), y_T^*(y^*(z)), y^*(z)), z)] + \right. \\ & \left. e(x^*(z), x^*(z), y_T^*(y^*(z)), y^*(z), z) \cdot s(x^*(z), x^*(z), y_T^*(y^*(z)), y^*(z), z) \right\} \end{aligned} \quad (28)$$

where $y_T^* = y_1^*(z) + y_2^*(z)$.

The first-order (optimality) condition is:

$$2 \left[f' \cdot \frac{\partial x^*}{\partial z} + \frac{\partial y^*}{\partial z} + g'(z) \right] + h \cdot \left[c'(e) \cdot \left(e_{x_1} \frac{\partial x^*}{\partial z} + e_{x_2} \frac{\partial x^*}{\partial z} + 2e_{y_T} \frac{\partial y^*}{\partial z} + e_z \right) \right] \quad (29)$$

$$+ h \cdot e \cdot \left(s_{x_1} \frac{\partial x^*}{\partial z} + s_{x_2} \frac{\partial x^*}{\partial z} + 2s_{y_T} \frac{\partial y^*}{\partial z} + s_z \right) + h \cdot s \cdot \left(e_{x_1} \frac{\partial x^*}{\partial z} + e_{x_2} \frac{\partial x^*}{\partial z} + 2e_{y_T} \frac{\partial y^*}{\partial z} + e_z \right) = 0.$$

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

$$-p_z L - ps_z - \frac{\partial x^*}{\partial z} [f'(x) + (p_{x_1} + p_{x_2})L + p(s_{x_1} + s_{x_2})] - \frac{\partial y^*}{\partial z} [1 + 2p_{y_T} L + 2ps_{y_T}] = g'(z). \quad (30)$$

Substituting in for the firm's first order conditions, equation (30) becomes:

$$-p_z L - ps_z - \frac{\partial x^*}{\partial z} [p_{x_2} L + pL_{x_2} - p \cdot (g_{x_1} + g_{x_2})] - \frac{\partial y^*}{\partial z} [p_{y_T} L + ps_{y_T} - pg_{y_T}] = g'(z) \quad (31)$$

Thus, by comparing (31) with (21), we know that the government will deliberately underprovide on public law enforcement expenditures by 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 (19) minus (25) and (20) minus (26)), weighted by the responsiveness of these security investments to law enforcement expenditures.

The proof of the second part of the proposition (n -firm case) is in the Appendix.

5. THE COOPERATIVE SOLUTION

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.

Proof. The cooperative's problem is to

$$\text{Min}_{x, y_T} 2 \cdot p(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) + 2 \cdot f(x) + y_T + 2 \cdot g(z) \quad (32)$$

The first-order conditions are:

$$\{x\} \quad -[(p_{x_1} + p_{x_2})L + p(L_{x_1} + L_{x_2})] = f'(x) \quad (33)$$

$$\{y_T\} \quad -2[p_{y_T} L + pL_{y_T}] = 1 \quad (34)$$

which implies that

$$\frac{-[(p_{x_1} + p_{x_2})L + p(L_{x_1} + L_{x_2})]}{f'(x)} = -2[p_{y_T} L + pL_{y_T}] \quad (35)$$

Government

$$\begin{aligned} \text{Min } & 2[f(x^{**}(z)) + g(z)] + y_T^{**}(z) \\ & + h \cdot \left\{ c[e(x^{**}(z), x^{**}(z), y_T^{**}(y^{**}(z), y^{**}(z)), z)] + \right. \\ & \left. e(x^{**}(z), x^{**}(z), y_T^{**}(y^{**}(z), y^{**}(z)), z) \cdot s(x^{**}(z), x^{**}(z), y_T^{**}(y^{**}(z), y^{**}(z)), z)) \right\} \end{aligned} \quad (36)$$

The first-order condition is equal to

$$-p_z L - ps_z - \frac{\partial x^{**}}{\partial z} [f'(x) + L(p_{x_1} + p_{x_2}) + p(s_{x_1} + s_{x_2})] - \frac{\partial y^{**}}{\partial z} [1 + 2p_{y_T} L + 2ps_{y_T}] = g'(z) \quad (37)$$

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

$$-p_z L - ps_z = g'(z). \quad (38)$$

As can be seen from the results of this section, a cooperative solution promises to approximate well the socially-optimal solution. This finding is consistent with the present move of the U.S. government to encourage the formation of ISACs. The question that now arises however is how ISAC group members among themselves can allocate the costs associated with generating the (public) security goods. Other than the ISAC member bargaining among themselves, one mechanism that could 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. Thus, under this scenario, the overall level of externalities that will be allowed will be determined on the basis on optimization by the collective, and then, the distribution of allowable externalities among the members will be priced out the members – i.e., those desirous to "use" the externality will purchase the externality permit by bidding for it.

If such "market-based" allocation of the externality would prove to be unwieldy in practice, then another solution that can be considered is the allocating among the members on the basis of his or her Shapley value:

$$\psi_i = \sum_C \frac{(n-k)!(k-1)!}{n!} [v(C) - v(C - \{i\})] \quad (39)$$

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 pay-offs 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, e.g., Suzuki

and Nakayama 1976; Young, Okada, and Hashimoto 1982), building airport runways (see, e.g., Littlechild 1974, Littlechild and Owen 1973), and minimum cost spanning tree games (see, e.g., Granot and Huberman 1981, Granot and Huberman 1984, Megiddo 1978).

Another form of decentralized group solution that can be utilized is one of the Buchanan (1965; 1999) type where 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, some form of decentralized group formation can be used to help address the problem of Internet security. Thus, it does not necessarily mean that just because there is a market failure arising from the public goods and externalities aspects of Internet security, government role is automatically prescribed to the exclusion of the private sector. Instead, both public and private sector initiatives can be utilized together.

In Table 2 below, I summarize the amounts of privately-provided private and public security goods, and the level of government-provided law enforcement expenditures, under different scenarios.

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	$-p_z L - ps_z - \frac{\partial x^*}{\partial z} [p_{x_2} L + pL_{x_2} - p \cdot (g_{x_1} + g_{x_2})]$ $- \frac{\partial y^*}{\partial z} [p_{y_T} L + ps_{y_T} - pg_{y_T}] = g'(z)$	z^*
Collective	$-p_z L - ps_z = g'(z)$	z^{**}
Socially Optimal	$-p_z L - ps_z = g'(z)$	z^o

6. EXAMPLES AND SIMULATIONS

$$L(x_1, x_2, y_T, z) = A[(1-q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c] \quad (40)$$

$$g(x_1, x_2, y_T, z) = \lambda(x_1, x_2, y_T, z) \cdot A[(1-q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c] \quad (41)$$

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

$$s(x_1, x_2, y_T, z) = [1 - \lambda] \cdot A[(1-q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c] \quad (42)$$

$$p(x_1, x_2, y_T, z) = (1-q)e^{-(\alpha x_1 y_T + \theta z)} + qe^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)} \quad (43)$$

Assume $0 < \alpha, \beta, \theta \leq 1$.

I decompose the attack into direct attacks and attacks staged indirectly through other compromised computers. Thus, equation (43) 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 attacks and viruses coming from computer 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 1/2, signifying that direct attacks always account for the greater portion of attacks than indirect attacks.

The parameters α , β , and θ measure the relative effectiveness of own private precautions, other's private precaution, and police protection, respectively, in reducing computer intrusions in one's systems.

$$L_{x_1} = A[(1-q)ax_1^{a-1} y_T^a z^c + qax_1^{a-1} y_T^a (x_2 y_T)^b z^c] \quad (44)$$

$$L_{x_2} = Aq(x_1 y_T)^a bx_2^{b-1} y_T^b z^c \quad (45)$$

$$L_{y_T} = A \left[(1-q)x_1^a a y_T^{a-1} z^c + q x_1^a x_2^b (a+b) y_T^{a+b-1} z^c \right] \quad (46)$$

$$L_z = A \left[(1-q)(x_1 y_T)^a c z^{c-1} + q (x_1 y_T)^a (x_2 y_T)^b c z^{c-1} \right] \quad (47)$$

$$p_{x_1} = -\alpha y_T \cdot \left[(1-q) \cdot e^{-(\alpha x_1 y_T + \theta)} + q \cdot e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} \right] \quad (48)$$

$$p_{x_2} = -\beta y_T \cdot \left[q \cdot e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} \right] \quad (49)$$

$$p_{y_T} = -\alpha x_1 (1-q) e^{-(\alpha x_1 y_T + \theta)} - (\alpha x_1 + \beta x_2) q e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} \quad (50)$$

$$p_z = -\theta \left[(1-q) \cdot e^{-(\alpha x_1 y_T + \theta)} + q \cdot e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} \right] \quad (51)$$

$$L_{x_1 x_1} = A \left[(a-1)(1-q) \alpha x_1^{a-2} y_T^a z^c + q a (a-1) x_1^{a-2} y_T^a (x_2 y_T)^b z^c \right] \quad (52)$$

$$L_{x_1 x_2} = A q \alpha x_1^{a-1} y_T^a \beta x_2^{b-1} y_T^b z^c \quad (53)$$

$$L_{x_1 y_T} = A \left[(1-q) \alpha x_1^{a-1} a y_T^{a-1} z^c + q \alpha x_1^{a-1} x_2^b (a+b) y_T^{a+b-1} z^c \right] \quad (54)$$

$$L_{x_1 z} = A \left[(1-q) \alpha x_1^{a-1} y_T^a c z^{c-1} + q \alpha x_1^{a-1} y_T^a (x_2 y_T)^b c z^{c-1} \right] \quad (55)$$

$$p_{x_1 x_1} = (\alpha y_T)^2 \left[(1-q) e^{-(\alpha x_1 y_T + \theta)} + q e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} \right] = (\alpha y_T)^2 \cdot p \quad (56)$$

$$p_{x_1 x_2} = (\alpha y_T)(\beta y_T) \left[q e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} \right] \quad (57)$$

$$\begin{aligned} p_{x_1 y_T} &= -\alpha \left[(1-q) e^{-(\alpha x_1 y_T + \theta)} + q e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} \right] \\ &\quad - (\alpha y_T) \left[(1-q) e^{-(\alpha x_1 y_T + \theta)} (-\alpha x_1) + q e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} (-\alpha x_1 - \beta x_2) \right] \\ &= -\alpha \cdot p - (\alpha y_T) \cdot p_{y_T} \end{aligned} \quad (58)$$

$$p_{x_1 z} = -(\alpha y_T) \left[(1-q) e^{-(\alpha x_1 y_T + \theta)} (-\theta) + q e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)} (-\theta) \right] = -(\alpha y_T) \cdot p_z \quad (59)$$

Notice also that an increase in the security investment of firm 2, decreases the indirect attack probability (i.e., $\frac{\partial e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)}}{\partial x_2} < 0$), but doesn't affect the direct attack

probability, as $\frac{\partial e^{-(\alpha x_1 y_T + \theta)}}{\partial x_2} = 0$. 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 $\frac{\partial e^{-(\alpha x_1 y_T + \theta)}}{\partial x_1}$ and $\frac{\partial e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta)}}{\partial x_1}$ are negative. The simulations below illustrate these points.

Simulations

Applying the above parameter specification, I generate the following simulations.

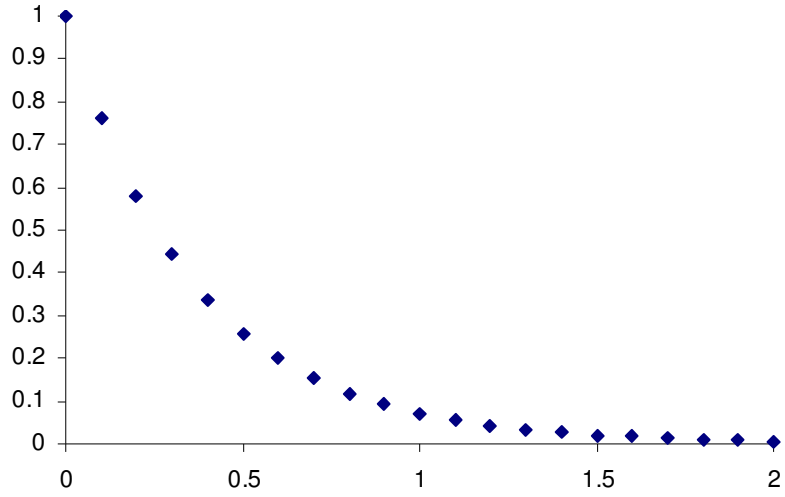


Figure 2. $p(x_1, x_2, y_T, z)$ when $x_1 = x_2 = z, y_T = 1$

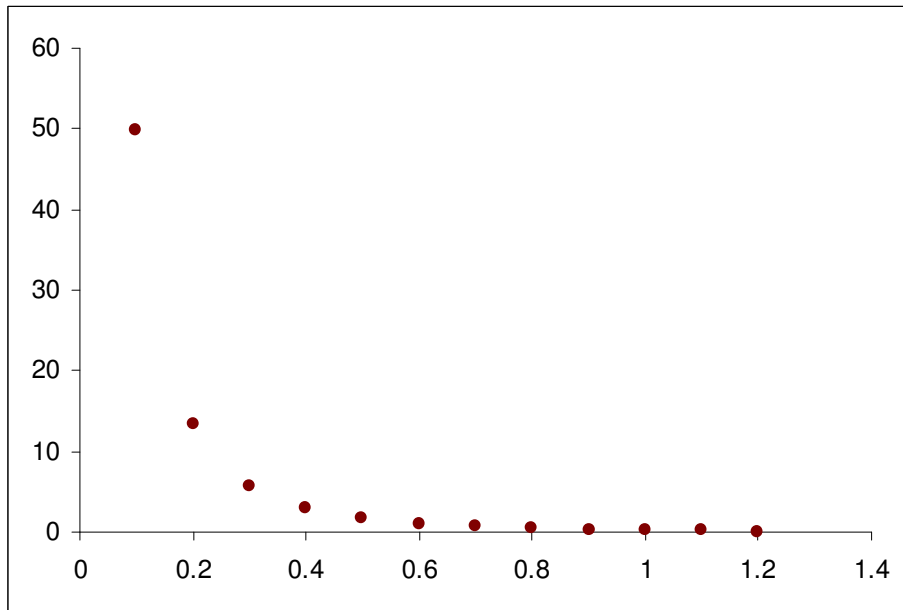


Figure 3. $p(x_1, x_2, y_T, z) \cdot L(x_1, x_2, y_T, z)$ when $x_1 = x_2 = z, y_T = 1$

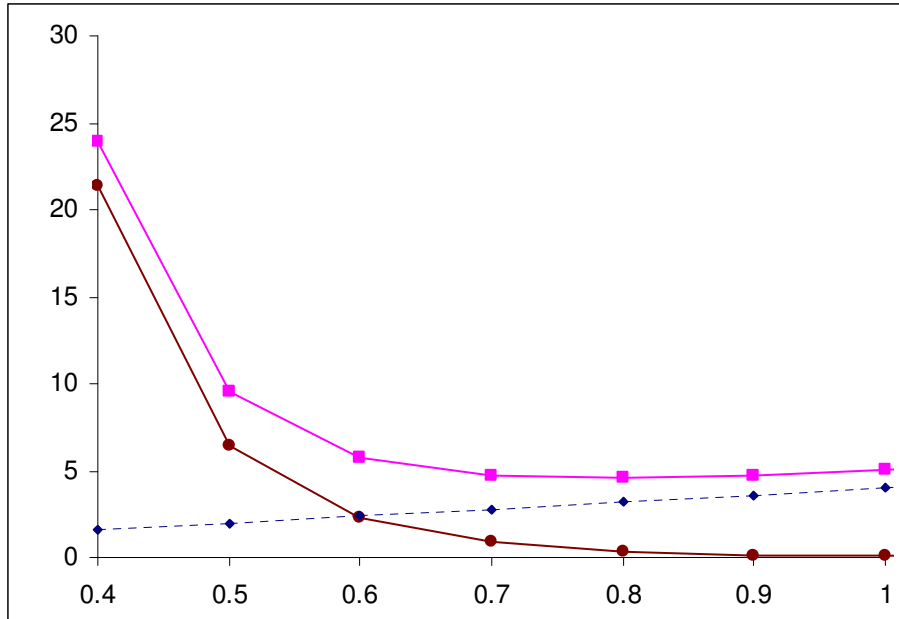


Figure 4. $p \cdot L + f(x_1) + y_T + g(z)$ when $x_1 = x_2 = z$, $y_T = 1$, $f(x_1) = 4x_1$

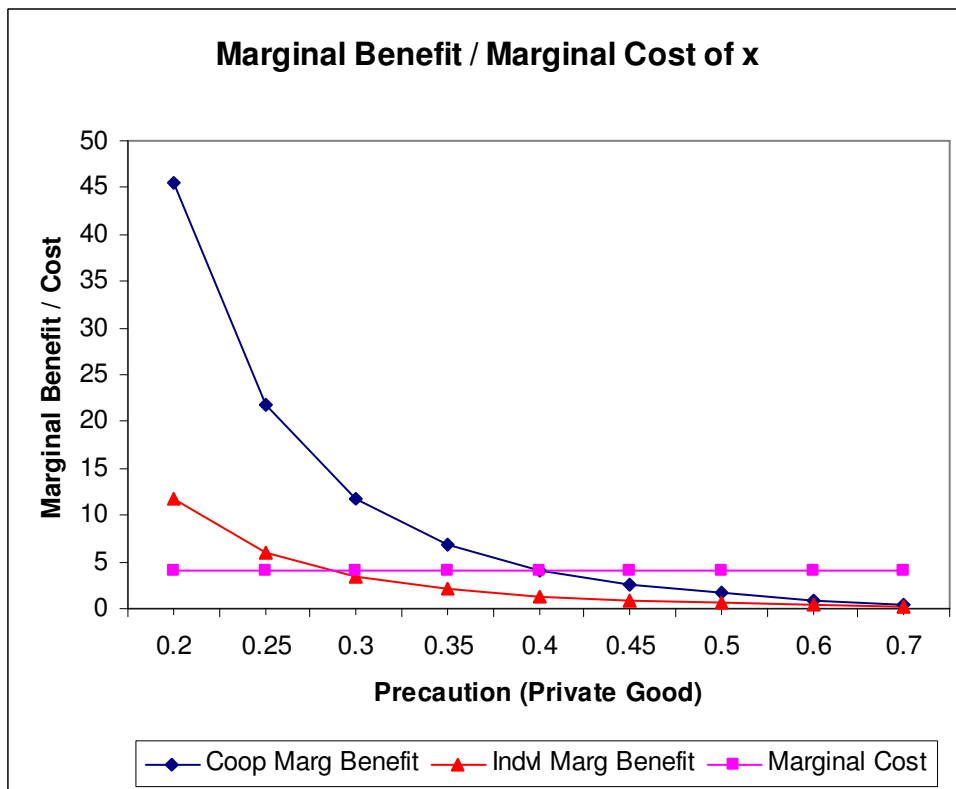


Figure 5. Optimal private precaution: cooperative vs. individual solution

Figure 2 shows that under the above functional specification, the probability of intrusion is decreasing at a decreasing rate. The same is true for the probability times the magnitude of the loss, as shown by Figure 3. Figure 4 shows that the optimal level of Internet security should be determined by balancing the trade-off between the reduction in the probability times 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.

The simulations² also show 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 . The reason for this is that, looking at the first-order conditions y_T and x , we see that the marginal benefit of the public and private security goods are differentiated by the terms $\beta x_2 \cdot q e^{-(\alpha_1 y_T + \beta x_2 y_T + \theta x)}$ 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 in being used by other firm, which use in turn benefit firm 1. Hence, although firm 2 is technically free-riding on firm 1's investment in public security good, such free ride is actually benefiting firm 1, because the more secure firm 2 is, the less firm 1 is affected by attacks intrusion coming its way through firm 2. Hence, the more interrelated cybersecurity is, the higher is an individual firm's the public security investment relative to private security investment tends to be.

7. CONCLUSIONS

In reality, crimes are solved by a combination of private precautions and public enforcement of the law. Thus, in this paper, I study a model where crimes are addressed through a combination of private and public measures. By so doing, the paper captures the substitutability between the private and public responses, and the optimal combination of these approaches can be determined.

In addition, the 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 non-rivalrous 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 are significant interrelatedness of risks, which give rise to externalities among individual websites. Thus, in this paper, I 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.

² Thus, for $\alpha = 1.5, \beta = 1, \theta = 0.5, \lambda = 0.5, a = -1.5, b = -1, c = -0.5, f'(x) = 4, g'(z) = 0.5, x = 0.1923, 0.2141, \text{ and } 0.2355$ for $q = 0.2, 0.5, \text{ and } 0.8$ respectively, while $y_T = 1.0232, 1.2626, \text{ and } 1.49$, for the same values of q . I 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 α , high/low θ , high λ /low λ , high/low $|\lambda|$, etc.) and the result remains the same.

I 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, non-rivalrous security investment, and law enforcement measures. Furthermore, the interrelatedness of Internet risks causes individual firms to underinvest in private and public security goods. The government thus decidedly lowers the level of police enforcement expenditures in order to induce firms to invest more in individual precautions. I also find that, under certain conditions, cooperation results in socially-optimal levels of expenditures in private and public security goods expenditures. The simulations illustrate the results of the model under several scenarios.

APPENDIX

General Case: n firms: Social Planner

$$\begin{array}{l} \text{Min} \\ \{x, y_T, z\} \end{array} \quad n[f(x) + g(z)] + y_T + h \cdot \left\{ \begin{array}{l} c[e(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z)] \\ + e(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \cdot s(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \end{array} \right\}$$

where:

$$y_T = y_1 + y_2 + \dots + y_n$$

FOCs:

$$\begin{array}{l} \{x\} \quad nf'(x) + h \cdot \{c' \cdot (e_{x_1} + e_{x_2} + \dots + e_{x_n}) + e \cdot (s_{x_1} + s_{x_2} + \dots + s_{x_n}) + s \cdot (e_{x_1} + e_{x_2} + \dots + e_{x_n})\} = 0 \\ \{y_T\} \quad 1 + h \cdot \{c' \cdot e_{y_T} + e \cdot s_{y_T} + s \cdot e_{y_T}\} = 0 \\ \{z\} \quad ng'(z) + h \cdot \{c' \cdot e_z + e \cdot s_z + s \cdot e_z\} = 0. \end{array}$$

Applying

$$c' = g; s = L - g; p = \frac{h}{n}e \Rightarrow e = \frac{np}{h}, e_{x_1} = \frac{n}{h}p_{x_1}, \text{ etc.},$$

we have:

$$\begin{array}{l} - \left(\sum_{i=1}^n p_{x_i} \right) \cdot L - p \cdot \left(\sum_{i=1}^n s_{x_i} \right) = f'(x) \\ - n(p_{y_T} L + ps_{y_T}) = 1 \\ - p_z \cdot L - p \cdot s_z = g'(z) \end{array}$$

General Case: n firms: Individual

$$\begin{aligned}
 & \text{Min} \quad p(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \cdot L(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \\
 & \quad \quad \quad + f(x_1) + y_1 + g(z) \\
 & \left. \begin{array}{l} \{x_1, y_1\} \\ \{x_2, y_2, \dots, x_n, y_n, z\} \end{array} \right\} \\
 & \{x_1\} \quad - p_{x_1} \cdot L - p \cdot L_{x_1} = f'(x) \\
 & \{y_1\} \quad - p_{y_T} \cdot L - p \cdot L_{y_T} = 1
 \end{aligned}$$

Notes: As n increases, underinvestment worsens!

Also, the “public good effect” worsens.

Totally differentiating the FOCs and imposing symmetry, we have:

$$\begin{aligned}
 & \left[\left(\sum_{i=1}^n p_{x_i x_i} \right) \cdot L + p_{x_1} \cdot \left(\sum_{i=1}^n L_{x_i} \right) + \left(\sum_{i=1}^n p_{x_i} \right) \cdot L_{x_1} + p \cdot \left(\sum_{i=1}^n L_{x_i x_i} \right) + f''(x) \right] \cdot dx \\
 & + n \cdot \left[p_{x_1 y_T} \cdot L + p_{x_1} \cdot L_{y_T} + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1 y_T} \right] \cdot dy \\
 & + \left[p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1 z} \right] \cdot dz = 0
 \end{aligned}$$

$$\begin{aligned}
 & \left[\left(\sum_{i=1}^n p_{y_T x_i} \right) \cdot L + p_{y_T} \cdot \left(\sum_{i=1}^n L_{x_i} \right) + \left(\sum_{i=1}^n p_{x_i} \right) \cdot L_{y_T} + p \cdot \left(\sum_{i=1}^n L_{y_T x_i} \right) \right] \cdot dx \\
 & + n \cdot \left[p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \right] \cdot dy \\
 & + \left[p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot dz
 \end{aligned}$$

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

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

and

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

where

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

The government chooses z in order to

$$\begin{aligned} \text{Min } n \cdot [f(x^*(z)) + y^*(z) + g(z)] \\ + h \cdot \left\{ c[e(x^*(z), \dots, x^*(z), y_T^*(y^*(z), \dots, y^*(z)), z)] + \right. \\ \left. e(x^*(z), \dots, x^*(z), y_T^*(y^*(z), \dots, y^*(z)), z) \cdot s(x^*(z), \dots, x^*(z), y_T^*(y^*(z), \dots, y^*(z)), z) \right\} \end{aligned}$$

where $y_T^* = y_1^*(z) + y_2^*(z) + \dots + y_n^*(z)$.

The first-order condition is:

$$\begin{aligned} n \cdot \left[f' \cdot \frac{\partial x^*}{\partial z} + \frac{\partial y^*}{\partial z} + g'(z) \right] + h \cdot \left[c'(e) \cdot \left(\left(\sum_{i=1}^n e_{x_i} \right) \cdot \frac{\partial x^*}{\partial z} + n \cdot e_{y_T} \frac{\partial y^*}{\partial z} + e_z \right) \right] \\ + h \cdot e \cdot \left(\left(\sum_{i=1}^n s_{x_i} \right) \cdot \frac{\partial x^*}{\partial z} + n \cdot s_{y_T} \frac{\partial y^*}{\partial z} + s_z \right) + h \cdot s \cdot \left(\left(\sum_{i=1}^n e_{x_i} \right) \cdot \frac{\partial x^*}{\partial z} + n \cdot e_{y_T} \frac{\partial y^*}{\partial z} + e_z \right) = 0. \end{aligned}$$

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

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

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

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

Conclusion: The government also adjusts the adjustment by the size of the underinvestment.

Cooperative Solution

$$\text{Min } n \cdot p(x_1, \dots, x_n, y_T(y_1, \dots, y_n), z) \cdot L(x_1, \dots, x_n, y_T(y_1, \dots, y_n), z) + n \cdot f(x) + y_T + n \cdot g(z)$$

x, y_T

FOCs:

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

$$\{y_T\} - n \cdot [p_{y_T} L + p L_{y_T}] = 1$$

Id: Government

$$\text{Min } n \cdot [f(x^{**}(z)) + g(z)] + y_T^{**}(z) + h \cdot \left\{ c[e(x^{**}(z), \dots, x^{**}(z), y_T^{**}(z), \dots, y_T^{**}(z), z)] + e(x^{**}(z), \dots, x^{**}(z), y_T^{**}(z), \dots, y_T^{**}(z), z) \cdot s(x^{**}(z), \dots, x^{**}(z), y_T^{**}(z), \dots, y_T^{**}(z), z)] \right\}$$

FOC:

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

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

$$-p_z L - ps_z = g'(z).$$

REFERENCES

- Buchanan, James. 1999. Three Research Programs in Constitutional Political Economy: Discussion of Political Science and Economics. In Alt, J., M. Levi, and E. Ostrom (Eds.), *Competition and Cooperation: Conversations with Nobelists About Economics and Political Science*. New York: Russel Sage Foundation.
- Buchanan, James. 1965. An Economic Theory of Clubs. *Economica* 32:1-14.
- Fabella, Raul, V. 2005. A Nozick-Buchanan Contractarian Governance as Solution to Some Invisible Hand Failures. *Quarterly Review of Economics and Finance* 45:284-295.
- 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, Geoffrey, and Howard Kunreuther. 2003. You Only Die Once: Managing Discrete Interdependent Risks, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=419240.
- Kobayashi, Bruce H. 2005. An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Pubic 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-Collell, Andrew, Michael D. Whinston, and Jerry R. Green. 1995. *Microeconomic Theory*. New York, N.Y.: Oxford University Press.
- Megiddo, N. 1978. Cost Allocation for Steiner Trees. *Networks* 8:1-6.
- Ortzag, Peter R. and Joseph Stiglitz, Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities, Working Paper 2002, *available at* <http://www.brookings.org/views/papers/orszag/20020104.pdf>
- Pauly, Martin V. 1970. Cores and Clubs. *Public Choice* 9:53-65.
- Pauly, Martin V. 1967. Clubs, Commonality, and the Core: An Integration of Game Theory and the Theory of Public Goods. *Economica* 34:314-24.
- Shapley, Lloyd. 1953. A Value of n -person Games. *Annals of Mathematics Studies* 28:307-318.
- Shavell, Steven. 1991. Individual Precautions to Prevent Theft: Private Versus Socially Optimal Behavior. *International Review of Law and Economics* 11:123-132.
- Suzuki, Mitsuo and Mikio Nakayama. 1976. The Cost Assignment of the Cooperative Water Resource Development: A Game Theoretical Approach. *Management Science* 22:1081-1086.
- Varian, Hal R. 1992. *Microeconomic Analysis*. 3d ed. W. W. Norton & Company.
- Young, H., N. Okada, and T. Hashimoto. 1982. Cost Allocation in Water Resources Development. *Water Resources Research* 18:463-475.