Information Security: Facilitating User Precautions Vis-à-Vis Enforcement Against Attackers

IVAN P.L. PNG AND QIU-HONG WANG

IVAN P.L. PNG is the Lim Kim San Professor at the National University of Singapore Business School and Professor of Information Systems and Economics at the National University of Singapore. His research focuses on the economics of intellectual property, privacy, and pricing. He is the coauthor of *Managerial Economics,* which has been published in multiple editions. Dr. Png is an independent director of Hyflux Water Trust Management Pte Ltd. and Healthway Medical Corporation Ltd. He was a nominated Member of Parliament (10th Parliament of Singapore) in 2005–6.

QIU-HONG WANG is an Assistant Professor in the School of Management and Huazhong University of Science and Technology. She received her Ph.D. in information systems from the National University of Singapore in 2007. Her research focuses on pricing, the economics of information security, the economics of intellectual property, and virtual economy.

ABSTRACT: We compare alternative information security policies—facilitating end-user precautions and enforcement against attackers. The context is mass and targeted attacks, taking account of strategic interactions between end users and attackers. For both mass and targeted attacks, facilitating end-user precautions reduces the expected loss of end users. However, the impact of enforcement on expected loss depends on the balance between deterrence and slackening of end-user precautions. Facilitating end-user precautions is more effective than enforcement against attackers when the cost of precautions and the cost of attacks are lower. With targeted attacks, facilitating end-user precautions is more effective for users with relatively high valuation of information security, while enforcement against attackers is more effective for users with relatively low valuation of security.

KEY WORDS AND PHRASES: enforcement, facilitation, information security, mass attacks, targeted attacks.

INFORMATION SECURITY IS A CRITICAL POLICY and business issue [39]. In the Computer Security Institute's twelfth annual survey [29], 52 percent of respondents reported

Qiu-Hong Wang is the corresponding author.

Journal of Management Information Systems / Fall 2009, Vol. 26, No. 2, pp. 97–121.

0742–1222 / 2009 $9.50 + 0.00.
DOI 10.2753/MIS0742-1222260205

experiencing up to 10 security incidents and 26 percent reported 10 or more incidents, suffering average losses of $350,424.

Against the backdrop of viruses and worms, phishing and pharming, denial of service attacks, and other infringements of information security, it is now recognized that information security is as much a technical issue as one of economic incentives [1].[1] Academic scholarship has provided important normative analyses: how much end users should invest in information security [14, 22, 23], vendor policies toward user patching [2] and vulnerability disclosure [12, 13], and government policies toward investigation of vulnerabilities [21] and disclosure [4, 30, 38]. The normative analyses have been supported by various empirical studies showing that deterrent measures do reduce information security incidents [20, 32] and that security efforts reduce virus attacks [25].

Obviously, information security presents externalities that warrant government intervention. However, academic studies of information security have tended to focus on the government's role in regulating disclosure of vulnerabilities and encouraging patching. They have tended to overlook the government's enforcement function. Information security is like any other aspect of security in the sense that externalities are sufficiently severe as to warrant the application of criminal law. Indeed, empirical studies show that governments worldwide do actively enforce information security [28].

Here, we consider that information security can be and is addressed by government, vendors, and other parties in two ways—facilitating end-user precautions and enforcement against violators of information security (for brevity, we call them "attackers"). Facilitation of end-user precautions includes information and publicity, training and education, technical assistance such as provision of automatic security updates, as well as subsidies. Enforcement includes investigation, prosecution, and punishment of those who infringe information security. Which policy is more cost-effective?

We address this question in the context of both mass (one-to-many) and targeted (one-to-one) attacks and considering strategic interaction between end users and attackers. Mass attacks do not discriminate between specific users and are aimed at an entire class of users, identified by technological platform (e.g., users of a particular operating system—Win32, Mac, or Linux), business purpose (e.g., all bank customers, all Viagra users), or some other way. By contrast, targeted attacks, such as denial-of-service attacks and system intrusion, are aimed at a particular victim.

Our analysis makes three contributions. First, we show that, for both mass and targeted attacks, facilitating user precaution does unambiguously reduce the expected loss incurred by end users. However, enforcement against attackers has conflicting effects on expected loss: it deters attackers but induces end users to slacken precautions. Hence, the net effect on end users' expected loss depends on the balance between deterring attackers and slackening of end-user precautions.

Second, focusing on end-user welfare under mass attacks, we show that facilitating end-user precautions is more cost-effective than enforcement against attackers the lower the cost of precaution and the cost of attacks. It may seem counterintuitive that facilitation should be more cost-effective when the cost of attacks is lower. The intuitive reason is that when attacks are less costly, attackers would increase attacking effort,

which would induce end users to take more effort in precaution. Hence, facilitation would be relatively more effective.

Third, focusing on end-user welfare under targeted attacks, we show that the policy that optimizes consumer (end-user) welfare is rather nuanced with respect to the end user's valuation of security. Facilitating end-user precautions is more effective on users with relatively high valuation for security—because they value security highly, facilitation gives bigger "bang for the buck." By contrast, enforcement against attackers is more effective on users with relatively low valuation for security—they do not value security and so are insensitive to facilitation.

Background Literature

ACADEMIC SCHOLARSHIP INTO THE ECONOMICS of information security has focused on two normative issues. One is policies to prevent security violation and reduce security loss, including policies of software vendors, CERT/CC, and other security specialists to disclose security flaws and provide the appropriate patches [2, 8, 12, 19, 27], and laws that require disclosure of information security incidents [4, 30, 38].[2]

The other strand is users' optimal behavior, including investment in information security [10, 14, 16], insuring against security breaches [6, 15], sharing information [5, 13], and implementation of detection systems [9, 40]. In this vein, Kunreuther and Heal [22, 23] emphasized that individuals' efforts in precautions might yield positive externalities for one another. The expected loss to any user decreases with others' precautions, and hence user precautions are strategic complements.[3] For a wide range of cost and risk parameters, there are two equilibria—either all users invest in precautions or no one does (see also [37]). To the extent that individuals underinvest in precautions, the government should intervene to subsidize precautions.[4]

August and Tunca [3] considered the incentive of users to patch security flaws. In a finding that was reminiscent of the public health literature on infectious diseases, they showed that mandatory patching is not optimal. With commercial software, the optimal policy is a subsidy on patching when security risk and patching costs are high, and no policy otherwise. However, with open source software, the optimal policy is a subsidy on patching when both security risk and patching costs are low, and a tax on software usage otherwise.

Accordingly, with respect to public policy, previous research tended to focus on the government's role in facilitating user precautions, specifically disclosure of vulnerabilities and encouraging patching. Previous research gave relatively little attention to the government's role in enforcement or other forms of facilitation. Even for previous research that directly addressed the economic incentives of violators of information security, countermeasures were focused on technical strategies rather than enforcement [24, 26].

Given that the government can address information security policies through end-user facilitation and enforcement against attackers, an important yet unanswered question is how it should choose between these policies. It is essential to address this question with due consideration for the context. One aspect is strategic interaction

among users and attackers. While previous normative analyses tended to assume the behavior of attackers to be exogenous [10, 15], this would not make sense in analyzing government enforcement. The other aspect is the nature of attacks and the intended scope of harm. Most previous normative analyses did not consider that attacks could be mass or targeted attacks, and that user and attacker behavior would differ significantly between the two.[5] For effective public policy, it is important to understand the differences in the behavior of attackers and the response of users between mass and targeted attacks.

Basic Setting

End users differ in their valuation of information security, $v \in [0, \bar{v}]$, which is distributed according to the cumulative distribution function, $\Phi(\bar{v})$, with $v < \infty$ being the highest value of information security. Each user knows his or her own valuation, v, and all users are risk neutral.

A user sustains an attack with probability $[1 - p]a$, where $p \in [0, 1]$ is a probability that depends on the user's effort in precautions such as installing patches, scanning suspicious e-mails, or properly configuring a firewall, and a is the attacker's effort. If the user sustains an attack, his or her benefit will be $[1 - h]v$, where $h < 1$ measures the harm caused by an attack.[6] The user's cost of effort, p, in precautions is $[1 - f]C_p(p)$, which has the properties

$$C_p(0) = 0,\ dC_p / dp > 0,\ d^2C_p / dp^2 > 0, \tag{1}$$

and where f represents facilitation of user precautions by the government, vendors, or third parties.[7] With a higher f, the user's cost of precautions would be lower. Each potential user chooses precautions to maximize his or her expected net benefit.[8]

The attacker chooses attacking effort, $a \in [0, 1]$, which is the probability of successful attack, given user's precautions and government enforcement. The attacker derives benefit, which could be monetary or nonmonetary, from an attack on a user, provided that he or she is not subject to enforcement. We assume that the attacker's benefit is bv, where $0 < b < \infty$; that is, his or her benefit is finite and positively related to the user's valuation of information security.[9] With probability, η, the authorities would subject the attacker to enforcement, impose a penalty of t, and prevent the attacker from realizing the benefit from attack. Further, the cost of attacking effort is $C_a(a)$, where

$$C_a(0) = 0,\ dC_a / da > 0,\ d^2C_a / da^2 > 0. \tag{2}$$

The attacker chooses effort to maximize his or her expected net benefit. This modeling assumption is consistent with Symantec's [33, p. 55] observation that attackers direct efforts against targets that provide the maximum return. We further assume that attackers are identical.

We consider two extreme scenarios that typify various forms of information security attacks:

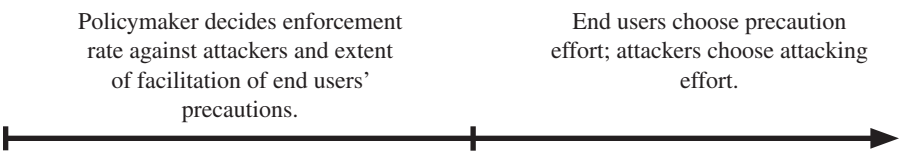

Figure 1. Model Time Line

1. *Mass attacks (one-to-many):* The attacker chooses attacking effort, a, which applies to all end users equally. Examples include spam, viruses, worms, spyware, and bots.
2. *Targeted attacks (one-to-one):* The attacker targets individual end users as characterized by their valuation, v, with effort, $a(v)$. Examples include denial of service attacks, system intrusion, and pharming.

The key difference between mass and targeted attacks is whether the attack differentiates among victims [31]. In our setting, victims are end users. Hence, phishing e-mails directed at all Citibank customers should be viewed as a mass attack as there is no discrimination among "Citibank customers." (Of course, if the victims were considered to be banks, then phishing e-mails directed at all Citibank customers could be viewed as a targeted attack against Citibank.)

The authorities can address information security through either facilitating end-user precautions (increasing f) or enforcement against attackers (increasing η). The sequence of events is shown in Figure 1.

Consider the end user with valuation, v. Given the attacker's effort, a, the user's expected net benefit from security would be

$$\begin{aligned} B(v|a) &= \{1-a[1-p]\}v + \{a[1-p]\}[1-h]v - [1-f]C_p(p) \\ &= v - a[1-p][hv] - [1-f]C_p(p). \end{aligned} \tag{3}$$

By Equation (1), $C_p(p)$ is convex, and so $B(v|a)$ must be concave in p. Maximizing with respect to p,

$$\frac{dC_p(p)}{dp} = \frac{ahv}{1-f}, \tag{4}$$

which defines his or her effort in precaution, $p(v)$, as a function of user valuation. Let $g_p(.)$ denote the inverse of $C'_p(.)$, which, by Equation (1), exists, and

$$\gamma \equiv \frac{h}{1-f}. \tag{5}$$

Then, Equation (4) yields the user's best response:

$$BR_p(a,v) = g_p(\gamma a v). \tag{6}$$

This leads us to make the following observation:

Observation 1 (User Precaution Efforts): Considering both mass and targeted attacks, for users with positive valuation, $v > 0$, user effort in precaution, p, is continuous and increasing in valuation, v, and facilitation, f; and it is also continuous and increasing in attacker's effort, a, such that, if $a = 0$, then $p(v) = 0$, for all v, and there exists $p_1(v) > 0$, such that $p(v \mid a = 1) = p_1(v)$.

The proofs of this and all other results are presented in the Appendix.

Mass Attacks

IN THIS SECTION, WE ANALYZE MASS ATTACKS. We first establish the equilibrium between end users and attackers, and then use the equilibrium to analyze the direct effects of changes in the facilitation of end-user precautions and enforcement rate on user and attacker behavior. Then, we consider the indirect (feedback) effects as users respond to attackers and vice versa.

By Observation 1, we know that user effort in precaution increases in the attacker's effort. Next, we consider the attacker's effort as a function of user behavior. We suppose that the attacker chooses attacking effort, a, to maximize expected net benefit,

$$H\left(a\middle|p(v)\right) = \left[1-\eta\right]b\int_0^{\bar{v}} av\left[1-p(v)\right]d\Phi(v) - \eta t - C_a(a). \tag{7}$$

By Equation (2), $C_a(a)$ is convex, and so $H(a \mid p(v))$ must be concave in a. Maximizing with respect to a,

$$\frac{dC_a(a)}{da} = b\left[1-\eta\right]\int_0^{\bar{v}} v\left[1-p(v)\right]d\Phi(v). \tag{8}$$

Let $g_a(.)$ denote the inverse of $C'_a(.)$, which, by Equation (2), exists, and let

$$\beta \equiv b\left[1-\eta\right]. \tag{9}$$

Then, Equation (8) yields the attacker's best response:

$$BR_a(p) = g_a\left(\beta\int_0^{\bar{v}} v\left[1-p(v)\right]d\Phi(v)\right), \tag{10}$$

where $p(v)$ is a function that maps a user's type, v, and attacker's effort to his or her precaution, p, for all $v \in [0, \bar{v}]$.

Thus, a pure strategy Nash equilibrium, (a^*, p^*), is such that $a^* = BR_a(p^*)$ and $p^*(v) = BR_p(a^*, v)$ for all $v \in [0, \bar{v}]$. Hence, the equilibrium is determined by

$$a^* = g_a\left(\beta\int_0^{\bar{v}} v\left(1-BR_p\left(a^*, v\right)\right)d\Phi(v)\right) \tag{11}$$

and

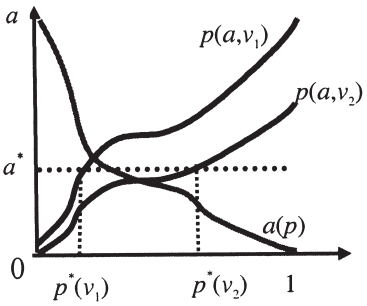

Figure 2. User–Attacker Equilibrium

$$p^*(v) = g_p\left(\gamma v BR_a\left(p^*\right)\right). \tag{12}$$

In equilibrium, the end users' combined expected loss from mass attacks is

$$L_m = ah\int_0^{\bar{v}} v\left[1-p(v)\right]d\Phi(v). \tag{13}$$

User–Attacker Equilibrium

For the analysis to be meaningful, Lemma 1 shows that there exists a nontrivial equilibrium between user effort in precautions, $p(v)$, and the attacking effort, a. Figure 2 illustrates the equilibrium.

> *Lemma 1 (User–Attacker Equilibrium): With mass attacks, there exists a unique, nontrivial equilibrium between end users and attacker, $p^*(v)$ and a^*.*

A further implication of Equation (8) is that, with mass attacks, the level of information security is determined by the class of users as a whole—a result also shown in Varian [37]. Hence, given attacker behavior, user efforts in precaution efforts are strategic substitutes. If other users raise their precautions, the attacker would reduce his or her effort, which would reduce the expected harm to any particular user, and so the user would rationally respond by reducing his or her effort in precaution. This free-rider problem is consistent with findings by August and Tunca [3] and explains user inertia in taking precautions [17].

Direct and Indirect Effects

Changes in government policy—facilitation of user precautions, f, and enforcement against attackers, η—directly affect user and attacker behavior. To fully appreciate the effects of changes in government policies, we must also consider the indirect (feedback) effects as users respond to the attacker and vice versa.

Proposition 1 (Mass Attack Effects): With mass attacks, the net effects (taking account of both direct and indirect effects) of an increase in facilitation, f, are to reduce attacker effort, increase end-user precaution effort, and reduce end-user expected loss, while the net effects of an increase in enforcement, η*, are to reduce attacker effort and end-user precaution, and are ambiguous on end-user expected loss.*

Table 1 summarizes the results in Proposition 1. Our analysis points to some unintended effects: specifically, enforcement against attackers need not enhance overall information security. An increase in the rate of enforcement against attackers, η, directly leads the attacker to reduce his or her attacking effort. However, there is also an indirect effect: users would respond to the reduced attacking effort by reducing their efforts in precaution. Consequently, the net effect on the expected loss to users depends on the balance between deterring the attacker and slackening of end-user precautions.

By contrast, actions to facilitate user precautions such as education and automatic updating of patches unambiguously reduce expected losses and so improve information security. Facilitation of end-user precautions encourages end users to increase effort in precautions. Further, the increase in user precautions reduces the attacker's expected benefit, and so leads him or her to reduce attacking effort. Accordingly, facilitation unambiguously reduces the users' expected loss.[10]

The results presented in Table 1 also shed light on analytical studies which assume that attacker behavior is exogenous and empirical studies that use a reduced form to estimate the impact of information security policy. Any analysis of end-user facilitation which assumes that attacker behavior is exogenous would overlook the indirect effect of the increase in user precautions on attacker effort. Hence, it would underestimate the impact of the facilitation on expected loss to users.

By contrast, any reduced-form analysis or estimate of enforcement against attackers which ignores the indirect effect on user precautions would overestimate the impact of enforcement. Such analysis would overlook that enforcement against attackers would induce attackers to reduce their effort, and so, indirectly, lead users to reduce effort in precautions.

Targeted Attacks

In this section, we analyze end-user and attacker behavior in the context of targeted attacks. In mass attacks, all end users are subject to the same attacker effort, a. By contrast, in targeted attacks, the attacker may design a specific scheme against each targeted victim, as characterized by the victim's valuation of information security, v.

In targeted attacks, the end-users' behavior is still characterized by Equations (3) and (4). With regard to the attacker, suppose that, with respect to any end user with valuation v, the attacker can choose attacking effort, $a(v)$, to maximize expected benefit. The attacker's expected benefit from all end users is

Table 1. Mass and Targeted Attacks: Empirical Implications

Increase in	Impact on Attacker's effort, a	Impact on End-users' precaution effort, p	Impact on Expected loss, L_m
Facilitation of precaution, f	↓	↑	↓
Enforcement rate, η	↓	↓	Ambiguous

$$H\left(a|p,v\right)=b\left[1-\eta\right]\int_{0}^{\bar{v}}\left\{a\left(v\right)\left[1-p\left(v\right)\right]v-C_{a}\left(a\left(v\right)\right)\right\}d\Phi\left(v\right)-\eta t. \tag{14}$$

Comparing Equation (7) with (14), the essential difference is that, in the case of targeted attacks, attacking effort, a, is a function of end-users' valuation of information security, v. Technically, in Equation (14), the attacker's cost is part of the integrand rather than outside the integral. The attacker maximizes H by choosing $a(v)$ that maximizes the expected benefit from each end user with valuation v. Hence, the first-order condition is

$$\frac{dC_{a}\left(a\right)}{da}=b\left[1-\eta\right]\left[1-p\left(v\right)\right]v. \tag{15}$$

We now consider how end users and attacker respond to changes in public policies and each other's behavior. Our next result compares end users' precautions against mass vis-à-vis targeted attacks.

> *Proposition 2: End users take more effort in precaution against mass attacks than targeted attacks.*

Recall that end users free-ride in precaution against mass attacks; hence, they underinvest in precautions against mass attacks. Proposition 2 shows that end users take even less effort in precaution against targeted attacks. The reason is that the attacker prefers mass attacks to targeted attacks since, *other things equal (including the net benefit per end user attacked),* mass attacks reach more users and hence yield higher expected benefit to attackers. Equivalently, mass attacks are more cost-effective for the attacker. End users, anticipating the higher probability of sustaining a mass attack, would take more effort in precaution against mass attacks than targeted attacks.

Proposition 2 emphasizes how the nature of potential attacks may influence end users' effort in precaution. Indeed, among 484 respondents to the 2007 U.S. CSI Computer Crime and Security Survey [29], 98 percent installed antivirus software (precaution against a mass attack), but only 47 percent installed intrusion prevention systems (precaution against targeted attack). The obvious implication of our analytical result and the survey evidence is that information security policy must be tailored to the threat—one size for all would not be optimal.

User–Attacker Equilibrium

With targeted attacks, there are no externalities among end users. Each end-user's net benefit is independent of other end-users' efforts in precautions. Using Equation (15) and g_a, the inverse of $C'_a(.)$, the attacker's best response, for each v,

$$BR_a\left(p|v\right) = g_a\left(\beta v\left[1-p\left(v\right)\right]\right). \tag{16}$$

Thus, a pure strategy Nash equilibrium (a^*, p^*) is such that, by Equations (6) and (16), $a^*(v) = BR_a(p^*|v)$ and $p^*(v) = BR_p(a^*, v)$, for all $v \in [0, \bar{v}]$, and the equilibrium is defined by

$$a^*\left(v\right) = g_a\left(\beta v\left[1-p^*\left(v\right)\right]\right). \tag{17}$$

The following result shows that the analysis is meaningful.[11]

Lemma 2 (Targeted Attacks Equilibrium): With targeted attacks, there exists a unique nontrivial equilibrium between attackers and end users, $a^*(v)$ and $p^*(v)$.

It is useful to define the end users' combined expected loss from targeted attacks,

$$L_t = h\int_0^{\bar{v}} v\left[1-p\left(v\right)\right]a\left(v\right)d\Phi\left(v\right). \tag{18}$$

Note that L_t differs from L_m in Equation (13) as the attacker's effort varies with user valuation, v.

With targeted attacks, a central issue is which users will be targeted. We suppose that the attacker would target any user that offers positive expected benefit—that is, $H \geq 0$.[12] Hence, the targeting depends on the user's valuation and effort in precaution. Superficially, high-valuation users, with their high v, would seem to present better targets. However, by Observation 1, they would take more effort in precaution. In Observation 2, we present a specific condition under which attackers target low-valuation users. Although their valuation is low, they take less effort in precaution, and hence, on balance, attackers prefer to target low-valuation users. This is consistent with Symantec's report (January–June 2006) [34, p. 47] that home users were the most highly targeted sector, accounting for 93 percent of all targeted attacks.

Observation 2 (Targeted Attacks of Low-Valuation Users): With targeted attacks, attackers target low-valuation users if the elasticity of end-user effort in precautions with respect to their valuation is relatively high—that is,

$$\frac{v}{p^*}\frac{\partial p^*}{\partial v} > \frac{1}{p^*} - 1. \tag{19}$$

Direct and Indirect Effects

With targeted attacks, attackers direct efforts at specific victims. An increase in facilitation would directly lead users to increase precautions. These users would become

less attractive and attackers targeting those users would reduce their attacking effort. Combining the direct and indirect effects, the expected loss from targeted attacks is decreasing in the facilitation of precautions.

An increase in enforcement rate has conflicting effects on the expected loss. It would deter attackers, leading them to reduce their attacking effort. However, this would then lead users to reduce their precautions. The net effect on the expected loss depends on the balance between deterrence of attackers and slackening of user precautions.

Proposition 3 (Targeted Attacks Effects): With targeted attacks, the net effects (taking account of both direct and indirect effects) of an increase in facilitation, f, are to reduce attacker effort, increase end-user precaution effort, and reduce end-user expected loss, while the net effects of an increase in enforcement, η*, are to reduce attacker effort and end-user precaution, and ambiguous on end-user expected loss.*

By Propositions 1 and 3, the net effects of facilitation and enforcement, taking account of both direct and indirect effects, are consistent across mass and targeted attacks. We summarize the analytical findings in the following proposition:

Proposition 4 (Common Effects of Facilitation and Enforcement in Mass and Targeted Attacks): With both mass and targeted attacks, facilitating user precautions reduces end users' expected loss. The net effect of enforcement on expected loss depends on the balance between deterring attackers and slackening of user precautions.

Social Welfare

How should society choose between facilitating end-user precautions and enforcement against attackers? We address this question from the standpoint of social welfare. In general, welfare could possibly include the net benefits of both end users as well as attacker. However, we exclude the attacker's benefits and costs from the measure of welfare [36]. Accordingly, social welfare for mass and targeted attacks simplifies to

$$W_m = \int_0^{\bar{v}} \left\{ v - ah[1-p]v - [1-f]C_p(p) \right\} d\Phi(v) - C_f(f) - C_\eta(\eta) \qquad (20)$$

and

$$W_t = \int_0^{\bar{v}} \left\{ v - a(v)h[1-p]v - [1-f]C_p(p) \right\} d\Phi(v) - C_f(f) - C_\eta(\eta), \qquad (21)$$

respectively. In Equations (20) and (21), the integrands are end-users' net benefit, while $C_f(f)$ and $C_\eta(\eta)$ represent the costs to the government of facilitating user precautions and enforcement against attackers, respectively.

A direct implication of Equations (20) and (21) is that end users have insufficient incentive to invest in precautions. When choosing their efforts in precaution, victims ignore the government's costs of facilitation and enforcement. Accordingly, they underspend on precautions. This implication parallels the literature on externalities and crimes in general (see [18]).

To compare the relative impact of facilitation vis-à-vis enforcement on welfare, we need some basis of comparison. Although cost is an important factor in comparing alternative policies, we consider it more insightful to focus on the differences in the effectiveness of the alternative policies. Accordingly, we focus on end-user welfare, ignoring the government's cost of facilitation and enforcement. Further, in order to derive closed-form solutions for simple analysis, we assume that the costs of the two policies are quadratic:[13]

$$C_a(a) = c_a a^2,\ C_p(p) = c_p p^2. \tag{22}$$

In the following result, we compare the marginal effects of facilitation vis-à-vis enforcement to derive:

Proposition 5 (Conditions for Achieving End-User Welfare): Considering end-user welfare, (a) with mass attacks, facilitating end-user precautions is more cost-effective than enforcement against attackers when the cost of precaution and cost of attacking effort are sufficiently low:

$$\frac{4c_p c_a [1-f]^2}{bh[1-\eta]^2} < \int_0^{\bar{v}} v^2 d\Phi(v); \tag{23}$$

(b) with targeted attacks, facilitating end-user precautions is more effective on users with relatively high valuation for security, $v > \tilde{v}$, while enforcement against attackers is more effective on users with relatively low valuation for security, $v \leq \tilde{v}$, where

$$\tilde{v} \equiv \sqrt{\frac{4c_p c_a [1-f]^2}{bh[1-\eta]^2}}. \tag{24}$$

Regarding the first result (Proposition 5a), it may seem counterintuitive that facilitation should be more cost-effective when the cost of attacks is lower. The intuitive reason is that when attacks are less costly, attackers would increase attacking effort, which would induce end users to take more effort in precaution. Hence, facilitation would be relatively more effective. The intuition with respect to the cost of precautions is simpler. A lower cost of precaution directly encourages end-user precautions and so reduces attackers' benefit from attacking and indirectly reduces attackers' effort. Accordingly, the lower cost of precaution clearly makes facilitation relatively more effective.

A striking implication of Proposition 5b is that information security policy should differentiate between users according to their value for security. This is intuitive because for high-value users, their elasticity with respect to facilitation is higher (simply because they get more "bang for the buck" out of effort in precaution); hence, facilitation is more effective with them. By contrast, facilitation is less effective with low-value users, and so the best policy must be enforcement.

Concluding Remarks

BY COMPARING THE COMBINATION OF DIRECT AND INDIRECT EFFECTS of the two security measures in mass vis-à-vis targeted attacks, we show that facilitating end-user precautions unequivocally reduces end-users' expected loss from both mass and targeted attacks. However, the net effect of enforcement on expected loss depends on the balance between deterring attackers and slackening of end-user precautions.

Commercial malware is fast growing. An online search quickly reveals numerous offers of software or services to crack passwords, provide dictionary attacks, log keystrokes, and capture screens. Like legitimate things, the Internet is reducing the cost of malicious activities as well. Our analysis suggests that, to surely reduce expected loss, facilitation of end-user precautions would be more effective than increasing enforcement.

We also showed that, with targeted attacks, the information security policy should be differentiated according to the users' valuation for security. The optimal policy is facilitation of precautions for high-value users and enforcement against attackers for low-value users. Cybercriminals definitely distinguish targets by value: in the underground market for bank account credentials, accounts containing more money command a higher selling price [35, p. 20].[14] Our analysis suggests that information security policy should focus on facilitating precautions among such high-value users.

Of necessity and for simplicity, our study is subject to several limitations. We implicitly assumed that end users perceived the information security risk to be sufficiently low as not to affect their participation in the activity exposing them to risk; for instance, the risk of phishing did not deter any consumer from using online banking. While this assumption is common in studies of information security, its validity is an empirical issue. Accordingly, an important direction for future analytical work is to endogenize the participation of end users in the activity exposing them to information security risk.

We couched the analysis and discussion in terms of the government's information security policy. But the government is not alone in facilitating user precautions and enforcement against attackers. Vendors play a large role in both, and, indeed, possibly a larger role in facilitation. We should emphasize that, to the extent that vendors are concerned with user welfare, our analytical results apply to vendors' information security policy subject to one proviso. Proposition 5 focused on consumer welfare and ignored the costs of facilitation and enforcement. Clearly, a vendor would not ignore these costs. Hence, our results should be interpreted as being relative to the costs of facilitation vis-à-vis enforcement.

We separately analyzed scenarios of mass attacks and targeted attacks. However, attackers may actively choose the nature and scope of attacks. Further, mass attacks and targeted attacks may differ in cost and detection mechanisms. Hence, another possible direction for future analytical work is to endogenize attackers' choice between mass and targeted attacks.

Finally, our analysis is subject to the limitation that end users and attackers were assumed to be risk neutral. Allowing risk aversion would considerably increase the

complexity of the analysis. The impact of risk aversion is not a priori obvious. Among users, those choosing high precautions (p close to 1) would reduce their risk by increasing their precautions toward $p = 1$, while those choosing low precautions (p close to 0) would reduce their risk by reducing their precautions toward $p = 0$. Accordingly, allowing for risk aversion is an important but challenging direction for future work.

Acknowledgments: An earlier draft of this paper appeared in the *Proceedings of the Forty-Second Annual Hawaii International Conference on System Sciences* (IEEE Computing Society Press, Los Alamitos, CA, 2009). It also draws upon "Information Security: User Precautions and Hacker Targeting," with Candy Q. Tang, to whom the authors are very grateful. The authors are pleased to acknowledge financial support from the U.S. Air Force Asian Office of Aerospace R&D (award FA4869-07-1-4046), the National University of Singapore Academic Research Fund (grant R-313-000-076-112), and School of Computing. They thank the guest editors, Eric K. Clemons, Robert J. Kauffman, and Thomas A. Weber, and participants and reviewers in the HICSS 2009 track on "Competitive Strategy, Economics, and Information Systems," the *JMIS* Editor-in-Chief, and the reviewers. They also benefited from helpful discussions and advice from Anindya Ghose, their NUS colleagues, and participants at the 2006 Workshop on the Economics of Information Security in Cambridge, UK.

Notes

1. "Phishing" is the activity of sending e-mails to mislead victims into visiting fraudulent Web sites and entering personal information such as credit card or bank account information, which is then used to steal from the victim. "Pharming" is the redirection of traffic from a particular legitimate Web address to a bogus Web site, where victims are misled into entering personal information.

2. CERT/CC is the Computer Emergency Response Team Coordination Center at Carnegie Mellon University.

3. For the definition of strategic complements and substitutes, see Bulow et al. [7].

4. The analysis by Kunreuther and Heal [23] implicitly focused on mass attacks. The problem of underinvestment would not arise with targeted attacks.

5. Grossklags et al. [15] studied users' incentives in self-protection and self-insurance in five threat models but assumed the behavior of attackers to be exogenous.

6. This setup is similar to that in the literature on enforcement against copyright piracy (see [11]). Full harm is the case of $h = 1$. Insurance is one reason the user might sustain less than full harm, $h < 1$.

7. This is generalized from the quadratic cost function as widely assumed in economic analyses of information security [13, 21].

8. For simplicity, we implicitly assume that all end users engage in the activity that exposes them to the information security risk. Equivalently, end users perceive the information security risk to be sufficiently low as not to affect their participation. This assumption is common in economic analyses of information security.

9. According to Symantec's [35, p. 21] report on the underground economy, credentials of bank accounts with larger amounts of funds commanded higher prices. This shows that the attacker's potential profit is directly associated with the user's loss. However, the attacker's benefit may be larger than the user's loss; e.g., for computers enslaved into a botnet, their owners' loss may be trivial compared to the benefit of the perpetrator.

10. August and Tunca [3] employed a discrete model to study user incentives to patch and showed that offering rebates for patching could enhance security. Their result depends on their assumption that users' choice is binary—either patch or do not patch. By contrast, our model allows users a continuous choice.

11. We omit the proof as it is essentially similar to that of Lemma 1.

12. Note that, by Equation (14), the attacker's expected benefit H takes account of the increasing marginal cost of attacking effort, $C_a(.)$.

13. The quadratic cost function is widely used in economic analyses of information security [13, 21].

14. Note that these accounts have already been compromised, so end-users' precautions have failed. Hence, the higher price does not contradict our result that high-value users take more precautions. Our analysis focused on ex ante precautions.

References

1. Anderson, R., and Moore T. The economics of information security. *Science, 314,* 5799 (October 27, 2006), 610–613.

2. Arora, A.; Caulkins, J.; and Telang, R. Sell first, fix later: Impact of patching on software quality. *Management Science, 52,* 3 (March 2006), 465–471.

3. August, T., and Tunca, T.I. Network software security and user incentives. *Management Science, 52,* 11 (November 2006), 1703–1720.

4. Balakrishnan, K.; Ghose, A.; and Ipeirotis, P. The impact of information disclosure on stock market returns: The Sarbanes–Oxley Act and the role of media as an information intermediary. Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

5. Beautement, A.; Coles, R.; Griffin, J.; Ioannidis, C.; Monahan, B.; Pym, D.; Sasse, A.; and Wonham, M. Modeling the human and technological costs and benefits of USB memory stick security. Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

6. Bolot, J., and Lelarge, M. Cyber insurance as an incentive for Internet security. Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

7. Bulow, J.; Geanakoplos, J.; and Klemperer, P. Multimarket oligopoly: Strategic substitutes and complements. *Journal of Political Economy, 93,* 3 (June 1985), 488–511.

8. Cavusoglu, H.; Cavusoglu, H.; and Raghunathan, S. Analysis of software vulnerability disclosure policies. CORS/INFORMS Joint International Meeting, Banff, Alberta, Canada, May 2004.

9. Cavusoglu, H.; Mishra, B.; and Raghunathan, S. The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16,* 1 (March 2005), 28–46.

10. Cavusoglu, H.; Raghunathan, S.; and Yue, W.T. Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25,* 2 (Fall 2008), 281–304.

11. Chen, Y.N., and Png, I.P.L. Information goods pricing and copyright enforcement: Welfare analysis. *Information Systems Research, 14,* 1 (March 2003), 107–123.

12. Choi, J.P.; Fershtman, C.; and Gandal, N. Network security: Vulnerabilities and disclosure policy. Paper presented at the Sixth Workshop on the Economics of Information Security, Heinz School of Public Affairs and CyLab, Carnegie Mellon University, Pittsburgh, PA, June 7–8, 2007.

13. Gal-Or, E., and Ghose, A. The economic incentives for sharing security information. *Information Systems Research, 16,* 2 (June 2005), 186–208.

14. Gordon, L.A., and Loeb, M.P. The economics of information security investment. *ACM Transactions on Information and System Security, 5,* 4 (November 2002), 438–457.

15. Grossklags, J.; Christin, N.; and Chuang, J. Security investment (failures) in five economic environments: A comparison of homogeneous and heterogeneous user agents. Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

16. Herath, H.S.B., and Herath, T.C. Investments in information security: A real options perspective with Bayesian post-audit. *Journal of Management Information Systems, 25,* 3 (Winter 2008–9), 337–375.

17. Hottell, M.; Carter, D.; and Deniszczuk, M. Predictors of home-based wireless security. Paper presented at the Fifth Workshop on the Economics of Information Security, Robinson College, University of Cambridge, United Kingdom, June 26–28, 2006.

18. Hylton, K.N. Optimal law enforcement and victim precaution. *Rand Journal of Economics, 27,* 1 (Spring 1996), 197–206.

19. Jaisingh, J., and Li, Q. The optimal time to disclose software vulnerability: Incentive and commitment. Working Paper, Hong Kong University of Science and Technology, Hong Kong, November 2005.

20. Kankanhalli, A.; Teo, H.H.; Tan, B.C.Y.; and Wei, K.K. An integrative study of information systems security effectiveness. *International Journal of Information Management, 23,* 2 (2003), 139–154.

21. Kannan, K., and Telang, R. Market for software vulnerabilities? Think again. *Management Science, 51,* 5 (May 2005), 726–740.

22. Kunreuther, H., and Heal, G. Interdependent security. *Journal of Risk and Uncertainty, 26,* 2–3 (March 2003), 231–249.

23. Kunreuther, H., and Heal, G. Modeling interdependent security. *Risk Analysis, 27,* 3 (June 2007), 621–634.

24. Li, Z.; Liao, Q.; and Striegel, A. Botnet economics: Uncertainty matters. Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

25. Liu, D.B.; Asgharpour, F.; and Camp, L.J. Risk communication in security using mental models. Paper presented at the Usable Security Conference 2007, Tobago, February 16, 2007.

26. Nagaraja, S. The economics of covert community detection and hiding. Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

27. Nizovtsev, D., and Thursby, M. Economic analysis of incentives to disclose software vulnerabilities. Paper presented at the Workshop on the Economics of Information Security, New York University, New York, June 2–3, 2005.

28. Png, I.P.L.; Wang, C.Y.; and Wang, Q.H. The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems, 25,* 2 (Fall 2008), 125–144.

29. Richardson, R. The 12th annual computer crime and security survey. Computer Security Institute, San Francisco, CA, 2007.

30. Romanosky, S.; Telang, R.; and Acquisti, A. Do data breach disclosure laws reduce identity theft? Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

31. Schmugar, C. "Targeted attack" mania. McAfee Avert Labs Blog, Santa Clara, CA, March 27, 2008 (available at www.avertlabs.com/research/blog/index.php/2008/03/27/targeted-attack-mania/).

32. Straub, D.W. Effective IS security: An empirical study. *Information Systems Research, 1,* 3 (September 1990), 255–276.

33. Symantec Internet security threat report: Trends for January 05–June 05, vol. 8. White Paper, Symantec, Cupertino, CA, September 2005.

34. Symantec Internet security threat report: Trends for January 06–June 06, vol. 10. White Paper, Symantec, Cupertino, CA, September 2006.

35. Symantec report on the underground economy for July 07–08. White Paper, Cupertino, CA, November 2008.

36. Trumbull, W.N. Who has standing in cost–benefit analysis? *Journal of Policy Analysis and Management, 9,* 2 (1989), 201–218.

37. Varian, H.R. System reliability and free riding. Working Paper, University of California, Berkeley, November 2004.

38. Wang, T.W.; Rees, J.; and Kannan, K. Reading the disclosures with new eyes: Bridging the gap between information security disclosures and incidents. Paper presented at the Seventh Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, Hanover, NH, June 25–28, 2008.

39. Whitman, M.E. Enemy at the gate: Threats to information security. *Communications of the ACM, 46,* 8 (August 2003), 91–95.

40. Yue, W.T., and Çakanyildirim, M. Intrusion prevention in information systems: Reactive and proactive responses. *Journal of Management Information Systems, 24,* 1 (Summer 2007), 329–353.

Appendix

Proof of Observation 1

Differentiating Equation (4), and applying Equation (1), we have

$$\frac{\partial p}{\partial v} = \frac{ah}{1-f} \Bigg/ \frac{d^2 C_p}{dp^2} > 0 \tag{A1}$$

$$\frac{\partial p}{\partial a} = \frac{hv}{1-f} \Bigg/ \frac{d^2 C_p}{dp^2} > 0 \tag{A2}$$

$$\frac{\partial p}{\partial f} = \frac{ahv}{\left[1-f\right]^2} \Bigg/ \frac{d^2 C_p}{dp^2} > 0. \tag{A3}$$

Q.E.D.

Proof of Lemma 1

We first prove the existence of the equilibrium between end user and attacker. Referring to Equation (8), the highest effort that the attacker would possibly choose would be when $\eta = 0$ and $p(v) = 0$, for all v. That effort would be

$$g_a\left(b\int_0^{\bar{v}} v d\Phi(v)\right) \equiv \hat{a}. \tag{A4}$$

For all other values of η and $p(v)$, the attacker would choose lower effort. Accordingly, without loss of generality, we can limit the attacker's choice of effort to the interval $[0, \hat{a}]$. Now Equation (11) defines a continuous function from $[0, \hat{a}]$ to $[0, \hat{a}]$. Referring to Equation (A4), since b and $\bar{v}$ are finite, $\hat{a}$ is finite, and so the interval $[0, \hat{a}]$ is convex and compact. Thus, by the Brouwer fixed point theorem, there exists a fixed point, a^*, which proves that there exists an equilibrium.

With regard to uniqueness, suppose otherwise that there exist two equilibria, (a', p') and (a'', p''). Let

$$Z \equiv \int_0^{\bar{v}} v\left[1 - p(v)\right] d\Phi(v),$$

and suppose further that $Z(p') < Z(p'')$. By Equation (10), a is increasing in Z; hence, $a' < a''$. By Observation 1, this implies that $p'(v) < p''(v)$ for all v, which by Equation (10) implies that $Z(p') > Z(p'')$, which is a contradiction. Hence, the equilibrium is unique.

Finally, we prove that the equilibrium is nontrivial. Let a^* and $p^*(v)$ represent the unique equilibrium between end user and attacker. Suppose $a^* = 0$. Then, by Equation (4), $p^*(v) = 0$ for all v. By Equation (8), this implies $a^* > 0$, which is a contradiction.

Hence, the equilibrium cannot involve $a^* = 0$. Suppose $p^*(v) = 0$ for all v. Then, by Equation (8), $a^* > 0$. By Equation (4), this implies $p^*(v) > 0$ for all v, which is a contradiction. Thus, $p^*(v) > 0$ for at least some v.

Thus, we must have $a^* > 0$ and $p^*(v) > 0$ for at least some v, and accordingly, the equilibrium is nontrivial. Q.E.D.

Proof of Proposition 1

Substituting Equation (6) into (11), we have

$$a^* = g_a\left(\beta\int_0^{\bar{v}} v\left[1 - g_p\left(\gamma a^* v\right)\right]d\Phi(v)\right). \tag{A5}$$

Substituting Equation (10) into (12), we have

$$p^*(v) = g_p\left(\gamma v g_a\left(\beta\int_0^{\bar{v}} v\left[1 - p^*(v)\right]d\Phi(v)\right)\right). \tag{A6}$$

We derive the empirical implications by implicit differentiation with respect to γ and β. Differentiating Equation (A5) with respect to β, we have

$$\begin{aligned}\frac{\partial a^*}{\partial \beta} &= g_a'\left\{\int_0^{\bar{v}} v\left[1 - g_p\left(\gamma a^* v\right)\right]d\Phi(v) - \beta\int_0^{\bar{v}} v\left[\gamma v\frac{\partial a^*}{\partial \beta}g_p'\right]d\Phi(v)\right\}\\ &= g_a'\int_0^{\bar{v}} v\left[1 - g_p\left(\gamma a^* v\right)\right]d\Phi(v) - g_a'\gamma\beta\frac{\partial a^*}{\partial \beta}\int_0^{\bar{v}} v^2 g_p' d\Phi(v),\end{aligned}$$

by which

$$\frac{\partial a^*}{\partial \beta} = \frac{g_a'\int_0^{\bar{v}} v\left[1 - g_p\left(\gamma a^* v\right)\right]d\Phi(v)}{1 + g_a'\gamma\beta\int_0^{\bar{v}} v^2 g_p' d\Phi(v)} > 0, \tag{A7}$$

since, by Equations (1) and (2), $g_p' = 1/C_p''(.) > 0$ and $g_a' = 1/C_a''(.) > 0$. Differentiating Equation (A5) with respect to γ, we have

$$\begin{aligned}\frac{\partial a^*}{\partial \gamma} &= g_a'\left\{-\beta\int_0^{\bar{v}} v g_p'\left(\gamma v\frac{\partial a^*}{\partial \gamma} + a^* v\right)d\Phi(v)\right\}\\ &= \beta g_a'\left\{-\gamma\int_0^{\bar{v}} v^2 g_p'\frac{\partial a^*}{\partial \gamma}d\Phi(v) - a^*\int_0^{\bar{v}} v^2 g_p' d\Phi(v)\right\}\\ &= -\frac{\partial a^*}{\partial \gamma}\gamma\beta g_a'\int_0^{\bar{v}} v^2 g_p' d\Phi(v) - a^*\beta g_a'\int_0^{\bar{v}} v^2 g_p' d\Phi(v),\end{aligned}$$

by which

$$\frac{\partial a^*}{\partial \gamma} = \frac{-g_a' a^* \beta \int_0^{\bar{v}} v^2 g_p' d\Phi(v)}{1 + g_a' \gamma \beta \int_0^{\bar{v}} v^2 g_p' d\Phi(v)}, \tag{A8}$$

because $g_p' > 0$ and $g_a' > 0$. Thus, the attacker's effort is increasing in β, so decreasing in η, and decreasing in γ, so decreasing in *f*.

Differentiating Equation (A6) with respect to β,

$$\frac{\partial p^*(v)}{\partial \beta} = g_p' \left\{ \gamma v g_a' \left\{ \int_0^{\bar{v}} v \left[1 - p^*(v) \right] d\Phi(v) - \beta \int_0^{\bar{v}} v \frac{\partial p^*(v)}{\partial \beta} d\Phi(v) \right\} \right\}$$

$$= \gamma g_p' g_a' v \left\{ \int_0^{\bar{v}} v \left[1 - p^*(v) \right] d\Phi(v) - \beta \int_0^{\bar{v}} v \frac{\partial p^*(v)}{\partial \beta} d\Phi(v) \right\},$$

which implies that the sign of $\partial p^*(v)/\partial \beta$ is determined by the term in brackets. The term in braces does not vary with *v*, and hence the sign of $\partial p^*(v)/\partial \beta$ is the same for all $v \in [0, \bar{v}]$. Further simplifying,

$$\frac{\partial p^*(v)}{\partial \beta} + \gamma \beta v g_p' g_a' \int_0^{\bar{v}} v \frac{\partial p^*(v)}{\partial \beta} d\Phi(v) = \gamma v g_p' g_a' \int_0^{\bar{v}} v \left[1 - p^*(v) \right] d\Phi(v). \tag{A9}$$

Because $g_p' > 0$ and $g_a' > 0$, the right-hand side of Equation (A9) is positive and $\gamma \beta v g_p' g_a' > 0$; hence we have $\partial p^*(v)/\partial \beta > 0$.

Differentiating Equation (A6) with respect to γ,

$$\frac{\partial p^*(v)}{\partial \gamma} = g_p' \left\{ v g_a \left(\beta \int_0^{\bar{v}} v \left[1 - g_p\left(\gamma a^* v \right) \right] d\Phi(v) \right) + \gamma v g_a' \left\{ -\beta \int_0^{\bar{v}} v \frac{\partial p^*(v)}{\partial \gamma} d\Phi(v) \right\} \right\}$$

$$= v g_p' \left\{ g_a \left(\beta \int_0^{\bar{v}} v \left[1 - g_p\left(\gamma a^* v \right) \right] d\Phi(v) \right) - \gamma \beta g_a' \int_0^{\bar{v}} v \frac{\partial p^*(v)}{\partial \gamma} d\Phi(v) \right\},$$

which implies that the sign of $\partial p^*(v)/\partial \gamma$ is determined by the term in braces and thus is the same for all $v \in [0, \bar{v}]$. Further simplifying,

$$\frac{\partial p^*(v)}{\partial \gamma} + \gamma \beta v g_p' g_a' \int_0^{\bar{v}} v \frac{\partial p^*(v)}{\partial \gamma} d\Phi(v) = v g_p' g_a \left(\beta \int_0^{\bar{v}} v \left[1 - g_p\left(\gamma a^* v \right) \right] d\Phi(v) \right). \tag{A10}$$

Because $g_p' > 0$, $g_a > 0$, and $g_a' > 0$, the right-hand side of Equation (A10) is positive and $\gamma \beta v g_p' g_a' > 0$; hence we have $\partial p^*(v)/\partial \gamma > 0$.

Thus, end-user's effort in precautions is increasing in β, so decreasing in η, and increasing in γ, so increasing in *f*. Since the attacker's effort, *a*, is decreasing in facilitation, *f*, and end-user's effort in precautions, *p*, is increasing in *f*, the total expected loss, L_m, by Equation (13), is decreasing in *f*. However, the attacker's effort, *a*, is decreasing in enforcement, η, while end-user's effort in precautions, *p*, is also

decreasing in η. Hence, the impact of enforcement, η, on the total expected loss, L_m, is ambiguous. Q.E.D.

Proof of Proposition 2

Denote precaution and attacker effort in mass attacks by p_m and a_m, and precaution and attack effort in targeted attacks by p_t and a_t, respectively. In mass attacks, precaution and attacker effort are characterized by

$$\frac{dC_p(p_m)}{dp_m} = \frac{a_m h v}{1-f} \tag{A11}$$

and

$$\frac{dC_a(a_m)}{da_m} = b[1-\eta]\int_0^{\bar{v}} v\left[1-p_m(v)\right]d\Phi(v). \tag{A12}$$

In targeted attacks, precaution and attacker effort are characterized by

$$\frac{dC_p(p_t)}{dp_t} = \frac{a_t(v) h v}{1-f} \tag{A13}$$

and

$$\frac{dC_a(a_t)}{da_t} = b[1-\eta]\left[1-p_t(v)\right]v. \tag{A14}$$

Suppose $p_m(v) < p_t(v)$; then substituting into Equations (A12) and (A14), for any $v \in [0, \bar{v}]$, $v[1-p_m(v)] > v[1-p_t(v)]$. Thus,

$$\frac{dC_a(a_m)}{da_m} > \frac{dC_a(a_t)}{da_t},$$

which leads to $a_m > a_t$ by Equation (2). Further substituting $a_m > a_t$ into Equations (A11) and (A13), we have

$$\frac{dC_p(p_m)}{dp_m} > \frac{dC_p(p_t)}{dp_t}.$$

Hence, by Equation (1), $p_m(v) > p_t(v)$, which contradicts the assumption. Consequently, we must have $p_m(v) > p_t(v)$. Q.E.D.

Proof of Observation 2

Substituting Equation (6) into (17), we have

$$a^*(v) = g_a\left(\beta v\left[1-g_p\left(\gamma a^* v\right)\right]\right). \tag{A15}$$

Differentiating Equation (A15) with respect to v,

$$\frac{\partial a^*(v)}{\partial v} = g'_a\left\{\beta\left[1-g_p\left(\gamma a^* v\right)\right]-\beta v g'_p\left[\gamma a^* + \gamma v\frac{\partial a^*(v)}{\partial v}\right]\right\},$$

by which we have

$$\frac{\partial a^*(v)}{\partial v} = \frac{\beta\left[1-g_p\left(\gamma a^* v\right)\right]g'_a - \beta v g'_a g'_p \gamma a^*}{1+\gamma\beta v^2 g'_a g'_p}. \tag{A16}$$

Thus, $\partial a^*(v)/\partial v < 0$ if and only if the right-hand side of Equation (A16) is negative, which is equivalent to

$$\frac{v}{g_p\left(\gamma a^* v\right)}\left[\gamma a^* g'_p\right] > \frac{1}{g_p\left(\gamma a^* v\right)} - 1. \tag{A17}$$

By Equation (6),

$$\frac{\partial p^*}{\partial v} = \gamma a^* g'_p. \tag{A18}$$

Substituting Equations (6) and (A18) into (A17),

$$\frac{v}{p^*}\frac{\partial p^*}{\partial v} > \frac{1}{p^*} - 1, \tag{A19}$$

which is the result. Q.E.D.

Proof of Proposition 3

The pure strategy Nash equilibrium, $(a^*(v), p^*(v))$, is defined by the fixed point of Equation (A15). Similarly, by Equations (6) and (16), a fixed-point relation for $p^*(v)$ on $[0, \bar{v}]$ can be obtained from

$$p^*(v) = g_p\left(\gamma a^* v\right) = gp\left(\gamma v BR_a\left(p^* | v\right)\right)$$

or

$$p^*(v) = g_p\left(\gamma v g_a\left(\beta v\left[1-p^*(v)\right]\right)\right). \tag{A20}$$

We derive the empirical implications by implicit differentiation with respect to γ and β. As the proof is essentially similar to that of Proposition 1, we omit the intermediate steps and only report the end results.

Differentiating Equation (A15) with respect to β, and solving,

$$\frac{\partial a^*}{\partial \beta} = \frac{g_a' v\left[1 - g_p\left(\gamma a^* v\right)\right]}{1 + \gamma\beta v^2 g_a' g_p'} > 0. \tag{A21}$$

Differentiating Equation (A15) with respect to γ, and solving,

$$\frac{\partial a^*}{\partial \gamma} = \frac{-\beta a^* v^2 g_a' g_p'}{1 + \gamma\beta v^2 g_a' g_p'} < 0. \tag{A22}$$

Thus, we can see that the attacker's effort is increasing in β, so decreasing in η, and decreasing in γ, so decreasing in *f*.

Differentiating Equation (A20) with respect to β, and solving,

$$\frac{\partial p^*(v)}{\partial \beta} = \frac{\gamma v g_a' g_p' v\left[1 - p^*(v)\right]}{1 + \gamma\beta v^2 g_a' g_p'} > 0. \tag{A23}$$

Differentiating Equation (A20) with respect to γ, and solving,

$$\frac{\partial p^*(v)}{\partial \gamma} = \frac{v g_p' g_a'\left(\beta v\left[1 - g_p\left(\gamma a^* v\right)\right]\right)}{1 + \gamma\beta v^2 g_a' g_p'} > 0. \tag{A24}$$

Thus, we can see that end-user's effort is increasing in β, so decreasing in η, and increasing in γ, so increasing in *f*.

Because the attacker's attacking effort, *a*, is decreasing in facilitation, *f*, and end-user's precaution, *p*, is increasing in *f*, the total expected loss, L_t, by Equation (18), is decreasing in *f*. However, the attacker's attacking effort, *a*, is decreasing in enforcement, η, and end-user's precaution, *p*, is also decreasing in η. Hence, the impact of enforcement, η, on the total expected loss, L_t, is ambiguous. Q.E.D.

Proof of Proposition 5

With mass attacks, end-user welfare is

$$W_m = \int_0^{\bar{v}} \left\{ v - ah\left[1 - p(v)\right]v - \left[1 - f\right]C_p(p) \right\} d\Phi(v). \tag{A25}$$

Differentiating Equation (A25) with respect to *f* and substituting from Equation (4),

$$\begin{aligned} \frac{\partial W_m}{\partial f} &= \int_0^{\bar{v}} \left\{ -hv\frac{\partial a}{\partial f}\left[1 - p(v)\right] + hva\frac{\partial p}{\partial f} + C_p(p) - \left[1 - f\right]\frac{dC_p(p)}{dp}\frac{\partial p}{\partial f} \right\} d\Phi(v) \\ &= -\int_0^{\bar{v}} \left\{ hv\left[1 - p(v)\right]\frac{\partial a}{\partial f} - C_p(p) \right\} d\Phi(v) > 0, \end{aligned} \tag{A26}$$

where the inequality follows from Proposition 1. Differentiating Equation (A25) with respect to η and substituting from Equation (4),

$$\begin{aligned}\frac{\partial W_m}{\partial \eta} &= \int_0^{\bar{v}} \left\{ -hv\left[1-p(v)\right]\frac{\partial a}{\partial \eta} + hva\frac{\partial p}{\partial \eta} - \left[1-f\right]\frac{dC_p(p)}{dp}\frac{\partial p}{\partial \eta}\right\} d\Phi(v) \\ &= -h\frac{\partial a}{\partial \eta}\int_0^{\bar{v}} v\left[1-p(v)\right]d\Phi(v) > 0,\end{aligned} \tag{A27}$$

where the inequality follows from Proposition 1. Similarly, with targeted attacks, end-user welfare is

$$W_t = \int_0^{\bar{v}} \left\{ v - hva(v)\left[1-p(v)\right] - \left[1-f\right]C_p(p)\right\} d\Phi(v). \tag{A28}$$

Differentiating Equation (A28) with respect to *f* and substituting from Equation (4),

$$\begin{aligned}\frac{\partial W_t}{\partial f} &= \int_0^{\bar{v}} \left\{ -hv\frac{\partial a(v)}{\partial f}\left[1-p(v)\right] + a(v)hv\frac{\partial p}{\partial f} + C_p(p) - \left[1-f\right]\frac{dC_p}{dp}\frac{\partial p}{\partial f}\right\} d\Phi(v) \\ &= -\int_0^{\bar{v}} \left\{ hv\left[1-p(v)\right]\frac{\partial a(v)}{\partial f} - C_p(p)\right\} d\Phi(v) > 0,\end{aligned} \tag{A29}$$

where the inequality follows from Proposition 3. Differentiating Equation (A28) with respect to η and substituting from Equation (4),

$$\begin{aligned}\frac{\partial W_t}{\partial \eta} &= \int_0^{\bar{v}} \left\{ -hv\frac{\partial a(v)}{\partial \eta}\left[1-p(v)\right] + a(v)hv\frac{\partial p}{\partial \eta} - \left[1-f\right]\frac{dC_p}{dp}\frac{\partial p}{\partial \eta}\right\} d\Phi(v) \\ &= -h\int_0^{\bar{v}} v\frac{\partial a(v)}{\partial \eta}\left[1-p(v)\right]d\Phi(v) > 0,\end{aligned} \tag{A30}$$

where the inequality follows from Proposition 3.

In summary, the marginal effects are as shown in Table A1.

Mass Attacks

With mass attacks, a sufficient condition for facilitation to be more effective than enforcement is

$$\frac{\partial a}{\partial f} < \frac{\partial a}{\partial \eta}. \tag{A31}$$

By Equations (A7) and (9),

$$\frac{\partial a^*}{\partial \eta} = \frac{\partial a^*}{\partial \beta}\frac{\partial \beta}{\partial \eta} = -\frac{g_a' b\int_0^{\bar{v}} v\left[1-g_p\left(\gamma a^* v\right)\right]d\Phi(v)}{1+g_a'\gamma\beta\int_0^{\bar{v}} v^2 g_p' d\Phi(v)}. \tag{A32}$$

Table A1. Marginal Effects of Facilitation and Enforcement

	Facilitation	Enforcement
Mass attacks	$-\int_0^{\bar{v}}\left\{hv\left[1-p(v)\right]\frac{\partial a}{\partial f}-C_p(p)\right\}d\Phi(v)$	$-h\int_0^{\bar{v}}v\left[1-p(v)\right]\frac{\partial a}{\partial \eta}d\Phi(v)$
Targeted attacks	$-\int_0^{\bar{v}}\left\{hv\left[1-p(v)\right]\frac{\partial a(v)}{\partial f}-C_p(p)\right\}d\Phi(v)$	$-h\int_0^{\bar{v}}v\left[1-p(v)\right]\frac{\partial a(v)}{\partial \eta}d\Phi(v)$

By Equations (A8) and (5)

$$\frac{\partial a^*}{\partial f}=\frac{\partial a^*}{\partial \gamma}\frac{\partial \gamma}{\partial f}=\frac{h}{\left[1-f\right]^2}\frac{-g_a'a^*\beta\int_0^{\bar{v}}v^2g_p'd\Phi(v)}{1+g_a'\gamma\beta\int_0^{\bar{v}}v^2g_p'd\Phi(v)}. \tag{A33}$$

Substituting Equations (A32) and (A33) into (A31), we have that Equation (A31) is equivalent to

$$\frac{h}{\left[1-f\right]^2}\frac{-g_a'a^*\beta\int_0^{\bar{v}}v^2g_p'd\Phi(v)}{1+g_a'\gamma\beta\int_0^{\bar{v}}v^2g_p'd\Phi(v)}<-\frac{g_a'b\int_0^{\bar{v}}v\left[1-g_p\left(\gamma a^*v\right)\right]d\Phi(v)}{1+g_a'\gamma\beta\int_0^{\bar{v}}v^2g_p'd\Phi(v)},$$

which can be simplified as

$$\int_0^{\bar{v}}v\left[1-g_p\left(\gamma a^*v\right)\right]d\Phi(v)<\frac{h\left[1-\eta\right]}{\left[1-f\right]^2}a^*\int_0^{\bar{v}}v^2g_p'd\Phi(v).$$

By Equation (8), we have

$$\int_0^{\bar{v}}v\left[1-g_p\left(\gamma a^*v\right)\right]d\Phi(v)=\frac{1}{b\left[1-\eta\right]}\frac{dC_a\left(a^*\right)}{da}.$$

Thus, Equation (A31) can be further simplified as

$$\frac{dC_a(a)}{da}<\frac{bh\left[1-\eta\right]^2}{\left[1-f\right]^2}a^*\int_0^{\bar{v}}v^2g_p'd\Phi(v), \tag{A34}$$

which, by Equation (21), simplifies to

$$\int_0^{\bar{v}}v^2d\Phi(v)>\frac{4c_ac_p\left[1-f\right]^2}{bh\left[1-\eta\right]^2}, \tag{A35}$$

which is the result.

Targeted Attacks

Following the same logic, with targeted attacks, a sufficient condition for facilitation to be more effective than enforcement is

$$\frac{\partial a(v)}{\partial f} < \frac{\partial a(v)}{\partial \eta}. \tag{A36}$$

By Equations (A21) and (9),

$$\frac{\partial a^*}{\partial \eta} = \frac{\partial a^*}{\partial \beta}\frac{\partial \beta}{\partial \eta} = -\frac{g_a' bv\left[1 - g_p\left(\gamma a^* v\right)\right]}{1 + \gamma\beta v^2 g_a' g_p'}. \tag{A37}$$

By Equations (A22) and (5),

$$\frac{\partial a^*}{\partial f} = \frac{\partial a^*}{\partial \gamma}\frac{\partial \gamma}{\partial f} = \frac{h}{\left[1-f\right]^2}\frac{-\beta a^* v^2 g_a' g_p'}{1 + \beta\gamma v^2 g_a' g_p'}. \tag{A38}$$

Substituting Equations (A37) and (A38) into (A36), we have that Equation (A36) is equivalent to

$$\frac{h}{\left[1-f\right]^2}\frac{-\beta a^* v^2 g_a' g_p'}{1 + \beta\gamma v^2 g_a' g_p'} < -\frac{g_a' bv\left[1 - g_p\left(\gamma a^* v\right)\right]}{1 + \gamma\beta v^2 g_a' g_p'},$$

which can be simplified as

$$\left[1 - g_p\left(\gamma a^* v\right)\right] v < \frac{h\left[1-\eta\right]}{\left[1-f\right]^2} a^* v^2 g_p'.$$

By Equation (8), we have

$$\left[1 - g_p\left(\gamma a^* v\right)\right] v = \frac{1}{b\left[1-\eta\right]}\frac{dC_a\left(a^*\right)}{da}.$$

Thus, Equation (A36) can be further simplified as

$$\frac{dC_a\left(a^*\right)}{da} < \frac{bh\left[1-\eta\right]^2}{\left[1-f\right]^2} a^* v^2 g_p', \tag{A39}$$

which, by Equation (21), simplifies to

$$v > \sqrt{\frac{4c_a c_p \left[1-f\right]^2}{bh\left[1-\eta\right]^2}} \equiv \tilde{v}, \tag{A40}$$

which is the result. Q.E.D.