

Information Security: User Precautions, Attacker Efforts, and Enforcement

Ivan P.L. Png*
ipng@nus.edu.sg

Qiu-Hong Wang*
wangqiu@comp.nus.edu.sg

Abstract

We analyze the strategic interactions among end-users and between end-users and attackers in mass and targeted attacks. In mass attacks, precautions by end-users are strategic substitutes. This explains the inertia among users in taking precautions even in the face of grave potential consequences.

Generally, information security can be addressed from two angles – facilitating end-user precautions and enforcement against attackers. We show that, enforcement is more effective as an all-round policy to enhance information security.

Facilitating user precautions leads to increased precautions and increased end-user demand, which have conflicting effects on the total harm suffered by end-users. Hence, reduced form estimates of the impact of facilitating precautions may over- or underestimate the impact, depending on which effect is stronger. Further, in targeted attacks, the outcome of interaction between users and attackers depends on the specific cost functions. Attackers may target low-valuation users as they take fewer precautions.

1. Introduction

Information security is a critical policy and business issue [24]. In the Computer Security Institute's 12th annual survey, 52% of respondents reported experiencing up to 10 security incidents while 26% reported 10 or more incidents [27]. The second and fourth largest categories of security incidents were viruses and phishing [27].¹ The average losses to

financial fraud, viruses, and phishing were \$21.1 million, \$8.4 million, and \$2.7 million respectively [26].

Against the backdrop of viruses and worms, denial of service attacks, and phishing, it is now recognized that information security is as much a technical issue as one of economic incentives [28]. Academic scholarship has provided important normative analyses of economic incentives: how much end-users should invest in information security [12][13][21], vendor policies towards user patching [32] and vulnerability disclosure [8][17], and government policy towards investigation of vulnerabilities [20].

The normative analyses have been supported by various empirical studies showing that deterrent measures do reduce information security incidents [3][4], security efforts reduce virus attacks [5], and government enforcement deters on-line attacks generally [15].

However, most normative analyses assumed the actions of violators of information security (for brevity, "attackers") to be exogenous. In particular, attackers were assumed not to respond or adjust in any way to user actions. While there has been some research into the incentives of attackers [22][29], there has been little scholarly analysis of the strategic interaction between users and attackers.² Realistically, however, "Attackers continuously look for easy targets, those that will provide them with the maximum return on the time they invest in writing malicious code" ([31], page 55).

Likewise, end-users adjust precautions in response to changes in attacks. For over 22% of Straub's [4] sample, the main influence on security effort was past incidents. Among computer security professionals who experienced a security intrusion, 48%-54% installed patches, 36% installed additional security

* School of Business, National University of Singapore. Corresponding author: Qiu-hong Wang, tel: +65 6516-2831. The authors gratefully acknowledge financial support from the U.S. Air Force Asian Office of Aerospace R&D (award FA4869-07-1-4046), the Academic Research Fund (grant R-313-000-076-112), and the School of Computing in the National University of Singapore. This is a substantially revised and expanded version of an earlier draft with Candy Q. Tang, to whom we are very grateful. We thank Anindya Ghose and participants at WEIS 2006 and IOMS 2006 for very helpful advice and suggestions.

¹ "Phishing" is the activity of sending emails to mislead victims into visiting fraudulent websites and entering personal information such as credit card or bank account information, which is then used to steal from the victim.

² An exception is the recent contribution of Ghose and Hausken (2006), which focuses on the incentive of attackers to share information.

service, and 34% adjusted organizational policies [27]. Generally, where two variables influence each other simultaneously, i.e., in the presence of bi-directional causation, a structural model is necessary to correctly identify the separate effects [26].

Further, previous normative analyses did not distinguish between mass (one-to-many) and targeted (one-to-one) attacks. Threats to information security differ in the intended scope of harm. Mass attacks are aimed at an entire class of users, identified by technological platform, for instance, all users of a particular operating system (e.g., Win-32, MAC, or Linux), or all users of a particular browser (e.g., Internet Explorer, or Mozilla Firefox). The class could also be identified by business purpose, e.g., all banks, or demographic characteristic, e.g., all Viagra users or all Citibank customers. Targeted attacks, such as denial-of-service attacks, are aimed at a particular victim. Leading security vendor, Symantec, has observed a trend, “Large Internet worms targeting everything and everyone have given way to smaller, more targeted attacks focusing on fraud, data theft, and criminal activity” [32]. Hence, it is important to understand the differences in attacker behavior and user response between mass and targeted attacks.

In this paper, we model the strategic interaction between end-users and attackers in the presence of government enforcement. We consider both mass and targeted attacks and address important issues in end-user behavior, business strategy, and public policy.

First, although threats to information security pose grave potential consequences, end-users seem quite sluggish in taking precautions. For instance, among computer security professionals who experienced an intrusion, 46% did not patch the relevant hole [27]. How can such inertia among professional IT managers be explained? We show that user precautions against mass attack are strategic substitutes – if one user increases precautions, others will have incentive to reduce their precautions.

The second issue concerns the strategic interaction between end-users and attackers. Using our structural model, we show that reduced-form estimates of the impact of changes in the user cost of precaution and the enforcement rate may be too low or too high, depending on the balance between conflicting effects. With targeted attacks, we show that attackers target low-valuation users as they invest less in precaution than high-valuation users.

Third, information security can be and is addressed from two angles – facilitating end-user precautions and enforcement against attackers. Which policy should the government prefer? We show that facilitating user precaution may have different effects in mass vis-à-vis targeted attacks. However, increased enforcement

leads attackers to reduce attacking effort. This suggests that enforcement is more effective as an all-round policy to enhance information security.

2. Background literature

The economics of information security has focused on two normative issues. One is the policies of software vendors, CERT/CC and other security specialists to disclose security flaws and provide the appropriate patches (for instance, [2][6][11][17][18]).

The other strand of normative analysis has focused on the user’s optimal behavior, including investment in information security [21], sharing information [8], and implementation of detection systems [9].

In this vein, [13] modeled a positive network externality among users in taking precautions against attack. The expected loss to any user increases with others’ precautions and hence user precautions are strategic complements [19]. For a wide range of cost and risk parameters, there are two equilibria – either all users invest in precautions or no one does [10].

August and Tunca [33] consider the incentive of users to patch security flaws. In a finding that is reminiscent of the public-health literature on infectious diseases, they show that mandatory patching is not optimal. With commercial software, the optimal policy is a subsidy on patching when security risk and patching cost 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.

By contrast with the previous research, we focus on the strategic interaction among end-users and attackers. Our analysis shows how users’ precautionary effort depends on attackers’ effort and vice versa. Accordingly, we can show how changes in policy toward attackers will affect user behavior, and, also how policy changes toward users will influence attacker behavior.

3. Basic setting

Consider the market for some service,³ which is provided by a monopoly at a uniform price p . (We assume a simple market structure, in order to focus on the interaction between end-users and attacker.)

End-users derive benefit, $v \in [0, \bar{v}]$, from use of the service, which is distributed according to the cumulative distribution, $\Phi(v)$, with \bar{v} representing

³ The analysis is applicable to software, hardware, as well as services.

the highest possible benefit. All users are risk-neutral. The vendor would set price such that $\bar{v} \geq p$, else there would be no demand.

A user sustains an attack with probability $[1-f]a$, where $[1-f]$ is a probability that depends on the user's effort, $f \in [0,1]$, in precautions such as installing patches, scanning suspicious emails, or properly configuring their firewall, and where a is a probability that depends on the attacker's effort.

If the user sustains an attack, she will not derive any benefit, and in addition, will incur some harm, vh .⁴ The user's cost of effort f in precautions is $\gamma C_f(f)$. The properties of $C_f(f)$ are:

$$C_f(0) = 0, \quad dC_f/df > 0, \quad d^2C_f/df^2 > 0. \quad (1)$$

Each potential user decides whether to buy the service, and, if so, chooses precautions to maximize her expected net benefit.⁵

The attacker chooses attacking effort, $a \in [0,1]$, which is the probability of successful attack without considering user's precaution. The attacker derives benefit, which could be monetary or non-monetary, from an attack on a user, provided that he is not subject to enforcement. We assume that the attacker's benefit is $[1+h]v$, i.e., positively related to the users' valuation of the service. With probability, η , the authorities would subject the attacker to enforcement, impose a penalty with monetary value, t , and prevent the attacker from realizing the benefit from attack. Further, the cost of attacking effort is $C_a(a)$.

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

The attacker chooses effort to maximize his expected net benefit. This modeling assumption is consistent with Symantec's ([31], page 55) observation that attackers direct efforts against targets that provide the maximum return. We further assume that attacker has no resource constraints.

For tractability, we assume that all attackers are identical. Accordingly, in equilibrium, all attackers choose the same level of effort and so, are subject to enforcement with the same probability.⁶

Table 1 describes all the notation used in our model.

Table 1. Analytical notation

Variable	Definition
----------	------------

$v \in [0, \bar{v}]$	End user's benefit from the service,
\bar{v}	Highest possible benefit from the service
p	Service price
f	User's effort in precautions, $f \in [0,1]$
a	Attacker's attacking effort, $a \in [0,1]$
h	Parameter which characterizes the additional harm (vh) that a user sustains from an attack in addition to losing the benefit from the service
C_f	User's cost of effort f in precautions
C_a	Attacker's cost of effort a in attacking
η	Authorities' enforcement rate against attackers
t	Monetary value of the penalty imposed on attackers who are subject to enforcement

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

- Mass attacks (one-to-many): The attacker chooses attacking effort, a , and broadcasts the attack, hence applies to all end-users equally. Examples include viruses, worms, spyware, and bots.
- 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 phishing (redirection of traffic from a particular web address to a bogus website).

Depending on the locus of the victim, some attacks may be considered to be either mass or targeted attacks. For instance, phishing emails directed at Citibank customers may be viewed as a mass attack against Citibank customers, or a targeted attack against Citibank, being one of many banks. Similarly, phishing of the IFRCS (International Federation of Red Cross and Red Crescent Societies), may be viewed as a mass attack against end-users whose computers are infected with re-direction, or a targeted attack against the IFRCS, being one of many international non-profit organizations.

The authorities can address information security through either facilitating end-user precautions (reducing γ) or enforcement against attackers (increasing η). To focus on the issue of information security, specifically, the interaction between end-users and attackers, and for tractability, in this study, we assume the price of the service price, p , to be exogenous.

Figure 1 shows the sequence of events. Given the service price, the authorities' enforcement rate against attackers and its facilitation of end user precaution, all

⁴ This set-up is similar to that in the literature on enforcement against copyright piracy (see, for instance, [34]).

⁵ We implicitly assume that end-users simultaneously decide whether to buy the service, and if so, how much effort to take in precautions. In reality, end users might be myopic, and consider precautions only after purchase. This scenario would be much simpler to analyze.

⁶ As indicated below in equation (7), the probability of being subject to enforcement increases with the attacker's effort.

users first make the purchase decision, and then decide precaution effort. The attackers choose attacking effort simultaneously with the users' decision on precaution.⁷

- Policy maker sets enforcement rate against attackers and facilitation of end user precautions.
- Vendor sets price.

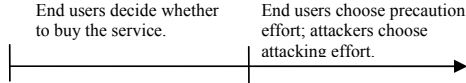


Figure 1. Model timeline

Consider the end-user with valuation, v . Given the attacker's effort, a , if the end-user buys the service, her expected net benefit would be

$$B(v|a) = v - p - v[1+h]a[1-f] - \gamma C_f(f), \quad (3)$$

Maximizing with respect to f ,

$$dC_f(f)/df = v[1+h]a/\gamma, \quad (4)$$

which defines her net-benefit maximizing effort in precaution, $f(v)$, as a function of the user type. By inspection of (4), we have⁸

Observation 1. For both mass and targeted attacks, user effort in precaution, f , is continuous and increasing in valuation, v , continuous and decreasing in the cost of precaution, γ , independent of price, p , and continuous and increasing in attacker attacking effort, a , such that, if $a=0$, then $f(v)=0$, and there exists $f_1(v)>0$, such that $f(v|a=1)=f_1(v)$.

In the following sections, we investigate mass and targeted attacks. We first consider the direct effects of changes in the cost of end-user precautions, enforcement rate, and price of the service, and then consider the combination of direct and indirect effects.

4. Mass attacks

We next characterize the demand for the service. By (3), every user for whom $B(v)\geq 0$ will buy the service. For mass attacks, it is relatively straightforward to prove that $B(v)$ is increasing in v . Accordingly, we have

Observation 2. With mass attacks, either no users buy the service or there exists a marginal user, \hat{v} , defined by

$$B(\hat{v}|a) = \hat{v} - p - \hat{v}[1+h]a[1-f] - \gamma C_f(f) = 0, \quad (5)$$

and such that only users with $v \geq \hat{v}$ buy.

The demand for the service arises from the users with $v \geq \hat{v}$, hence the quantity demanded (equal to the vendor's sales) is

$$Q_m = \int_{\hat{v}}^1 d\Phi(v). \quad (6)$$

The following result shows how the demand for the service depends on attacker's effort and the vendor's price.

Observation 3. With mass attacks, the marginal user type, \hat{v} , is continuous, increasing and concave in the user cost of effort in precaution, γ , the attacking effort, a , and the price, p . In addition, $\hat{v}(a=0)=0$ and $\hat{v}(a=1)=\hat{v}_1$, where $0 \leq \hat{v}_1 \leq 1$.

Having analyzed user behavior (choices of whether to buy the service, and, if so, effort in precaution) as a function of the attacker's effort, we now 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,

$$H(a|f(v)) = [1-\eta][1+h]a \int_{\hat{v}}^1 v[1-f]d\Phi(v) - \eta t - C_a(a), \quad (7)$$

By (2) and since $C_a(a)$ is convex, the function H is concave in a . Maximizing H with respect to a , the first-order condition is

$$dC_a(a)/da = [1-\eta][1+h] \int_{\hat{v}}^1 v[1-f]d\Phi(v). \quad (8)$$

Observation 4. With mass attacks, the attacker's effort, a , is continuous and decreasing in the enforcement rate, η . Further, the attacker's effort, a , is continuous and decreasing in the marginal user type, \hat{v} , and, if $\hat{v}=1$, then $a=0$, and there exists some $\tilde{a} > 0$ such that if $\hat{v}=0$, then $a=\tilde{a}$. In addition, the attacking effort, a , is continuous and decreasing in user effort in precaution, f .

User-Attacker Equilibrium

For the analysis to be meaningful, we must show that there exists a non-trivial equilibrium. To prove existence, it is useful to consider the rate at which end-users are subject to attack, conditional on attacker effort, a , i.e., the *conditional loss*,

⁷ This simultaneous setting is similar to the Cournot model where competing producers decide on output simultaneously and non-cooperatively

⁸ We prove all results in the Appendix.

$$L(a) = [1+h] \int_{\hat{v}(a)}^1 v [1-f(v|a)] d\Phi(v). \quad (9)$$

Accordingly, the function, $L(a)$, is the amount or harm that end-users actually suffer from attack, i.e, the *effective loss of users*.

Lemma 1 proves the existence of equilibrium by considering the relation between $L(a)$ and the attacking effort, a . The conditional loss is a continuous, decreasing function of the attacking effort, and similarly, the attacking effort is a continuous, increasing function of the user's conditional loss. Figure 2 illustrates the result.

Lemma 1. There exists a non-trivial equilibrium between end-users and attackers, a^* , $\hat{v}(a^*)$ and $f^*(v|a^*)$.

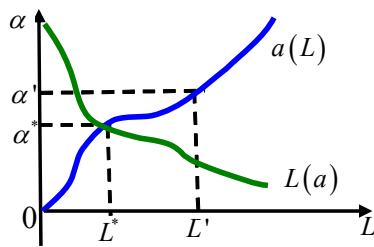


Figure 2. User-attacker equilibrium

Our first substantive result focuses on the strategic interaction among end-users. Proposition 1 shows that, given attacker behavior, users' precautions are strategic substitutes [19].

Proposition 1. With mass attacks, given attacker behavior, user precaution efforts are strategic substitutes: The higher the precaution efforts of others, the lower will be the precaution effort of any particular individual.

Proposition 1 implies that a free-rider problem exists in user security. If other users raise their precautions, they will reduce the expected harm to any particular user, and she will rationally respond by reducing her precaution. This free-rider problem is reminiscent of that arising from concealed precautions by potential crime victims [14][16]. In the context of information security, August and Tunca [33] also identify a free-rider problem in user precautions. Our result is consistent with broad empirical evidence, reviewed below in Section 6, that users are slow to take precautions against mass attack.

Direct and indirect effects

So far, we have considered only the direct effects of changes in vendor strategy and government policy, and ignored the indirect (feedback) effects through the actions of the other side of the situation. To fully appreciate the effects of changes in vendor strategy and government policy, we now consider both direct and indirect effects.

Our analysis points to some unintended effects: specifically, actions to reduce user cost of precaution such as automatic updating of patches need not enhance overall information security. A reduction in end-user's cost of precaution has two effects on the conditional loss, L : increasing the end-users' effort in precaution and increasing the end-user's demand for the service. The increase in demand raises the attacker's expected benefit, and so, leads attackers to increase their attacking effort, hence, increasing the conditional loss. By contrast, the increase in end-user efforts in precautions would reduce the conditional loss, but also, induce attackers to reduce their attacking effort. Consequently, the net impact on the users' conditional loss depends on the balance of the two effects.⁹

Next, consider an increase in the rate of enforcement against attackers, η . This directly leads attackers to reduce their attacking effort. However, there is also an indirect effect: users would respond to the reduced attacking effort by reducing their precaution efforts, and the demand for the service would increase. As reported in Proposition 2 below, the net impact on the effective user loss depends on the balance of the direct and indirect effects, and is ambiguous.

Similarly, an increase in the price, p , has direct and indirect effects on the demand for the service. It would directly reduce the demand, as users with relatively low valuation cease to buy the service. However, an increase in price also has an indirect (consequential) effect through attackers' response to user choices. With fewer users of the service, the attackers would reduce attacking effort, which reduces the probability of attack and therefore raises users' expected net benefit. In turn, all users would reduce precaution effort and more users would purchase the service. Thus, the indirect effect (from the attackers) tends to offset the direct effect of the price increase. Accordingly, the demand for the service is less elastic than it would appear from studying the direct effect

Deleted: raise

⁹ August and Tunca [31] employ a discrete model to study user incentives on patching and find that to offer patching rebates can enhance the security of the service. This result is due to the binary choice setting of users in a discrete model.

alone, and, the net impact on the effective loss is ambiguous.

Proposition 2. With mass attacks, the effective user loss, aL , is: increasing in the user cost of precaution, γ , if the effect through lower precautions outweighs the effect through shrinking demand; and ambiguous in the rate of enforcement against attackers, η , and the price of the service, p .

Table 2 summarizes the net effect of changes in the user cost of precaution, γ , enforcement rate, η , and the price, p , on users' precautions, attackers' effort, and users' demand for the service¹⁰.

Table 2. Mass attack: empirical implications¹¹

Impact on	Attackers' effort, a	End-users' precaution effort, f	No. of buyers, $1-\hat{v}$
Increase in			
Cost of precaution, γ	conditional	↓	↓
Enforcement rate, η	↓	↓	↑
Price, p	↓	↓	↓

Studies assuming exogenous attacker behavior or using a reduced form ignore indirect (feedback) effects. Accordingly, they may underestimate the impact of changes in the cost of precautions or enforcement rate on effective losses and the number of attacks. Further, since attackers respond to the aggregate effort in precaution by all users rather than the efforts of individual users, the impact of any security measure may be over-estimated if it does not reduce the overall loss of the whole user base. Proposition 3 highlights these findings.

Proposition 3. With mass attacks, compared to the case of exogenous attacker behavior, if attacker behavior is endogenous, then: (i) the demand for the service is less elastic, and (ii) assuming that the effect of facilitating end-user precaution through lower end-user precautions outweighs the effect through shrinking demand, then facilitation of user precaution has a weaker impact on end-user precaution and stronger impact on demand for the service.

¹⁰ The results in Table 2 follow from the proofs of Propositions 2 and 3 as presented in the appendix.

¹¹ The up arrow represents a positive impact, while the down arrow represents a negative impact.

5. Targeted attacks

In mass attacks, all end-users are subject to the same attacker effort, a . By contrast, in targeted attacks, the attackers design specific schemes against each targeted victim, as characterized by valuation, v .

With targeted attacks, the end-users' behavior is still characterized by (3) and (4). With regard to attackers, we suppose that they choose attacking effort, $a(v)$, to maximize expected benefit as a function of the end-user valuation, v :

$$H(a|f(v), v) = a(v)[1-\eta]v[1-f(v)] - \eta t - C_a(a). \quad (10)$$

Maximizing H with respect to a , the first-order condition is

$$v[1-\eta][1-f(v)] = dC_a(a)/da. \quad (11)$$

We now consider how end-users and attackers respond to changes in their environment and each other's behavior.

Observation 5: With targeted attacks, attacking effort increases in end-user valuation, v , and decreases in precaution effort, $f(v)$, and enforcement rate, η .

Unlike mass attacks, however, users' net benefit as measured by (3) is not monotone in v . Observation 6 reports the finding.

Observation 6: With targeted attacks, end-users' net benefit increases in their valuation, v , if and only if the elasticity of attacking effort with respect to user's valuation is low enough, i.e.,

$$\frac{\partial a}{\partial v} \frac{v}{a} < \frac{1}{a[1+h][1-f]} - 1. \quad (12)$$

User-Attacker Equilibrium

Under targeted attacks, there are no externalities among end-users. The net benefit of each end-user is independent of other end-users' efforts in precautions. The next result shows that there exists a non-trivial equilibrium in the strategic interaction between end-users and attackers.¹²

Lemma 2. There exists a non-trivial equilibrium between end-users and attackers, $a^*(v)$ and $f^*(v|a^*)$.

Direct and indirect effects

¹² The proof is similar to that of Lemma 1.

Table 3 summarizes the net effects of changes in cost of effort in precaution, γ , enforcement rate, η , and price, p , on users' effort in precautions, attackers' effort, and demand for the service.¹³ In Table 3, the grey-shaded cells highlight differences in the impacts of cost of precaution and price between the scenarios of mass vis-à-vis targeted attacks (Tables 2 and 3).

With targeted attacks, attackers direct efforts at specific victims. An increase in the end-user cost of effort in precaution would directly lead users to reduce precautions. Then, clearly, attackers targeting those users would increase their attacking effort. By contrast, with mass attacks, the attackers adjusted their efforts in ambiguous directions.

With targeted attacks, the price of the service affects only the end-users' purchase decision and has no impact on attacker effort, and hence, it has no effect on users' effort in precaution. By contrast, with mass attacks, an increase in the price of the service leads attackers to decrease attacking effort and end-users to decrease effort in precaution.

Table 3. Targeted attacks: empirical implications

Impact on Increase in	Attackers' effort, a	End-users' precaution effort, f	No. of buyers, D_t
Cost of precaution effort, γ	↑	↓	↓
Enforcement rate, η	↓	↓	↑
Price, p	none	none	↓

An important issue that arises with targeted attacks is which users will be targeted. We have implicitly assumed that attackers have unlimited resources, hence they target any user that offers positive expected benefit, i.e., $H \geq 0$. In turn, this depends on whether the user buys the service, and, if so, the user's valuation and effort in precaution.

Superficially, high-valuation users would seem to present good targets because of their high v . However, they would take more effort in precaution, $df/dv > 0$, considering both direct and indirect effects. Proposition 4 shows that, under a specific condition, attackers target low-valuation users. Although their valuation is low, they take less effort in precaution. Hence, on balance, attackers prefer to target low-valuation users.

Proposition 4. With targeted attacks,

(i) attackers target low valuation users if the elasticity of end-user effort in precautions with respect to their valuation is relatively high, i.e.,

$$\frac{v}{f} \frac{\partial f}{\partial v} > \left[\frac{1}{f} - 1 \right]; \quad (13)$$

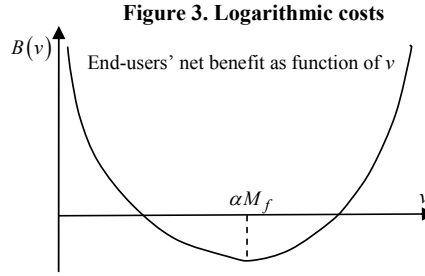
(ii) demand for the service decreases in the end-user cost of effort in precaution, γ , and price, p , and increases in the enforcement rate, η .

Specific cost functions

To further explore the strategic interaction between end-users and attackers, we consider two specific functional forms that have been used in previous studies of information security for the cost of end-user precaution and attacker's effort.

Suppose that costs are logarithmic [25]. Then $C_f(f) = -M_f \log[1-f]$; $C_a(a) = -M_a \log[1-a]$.

The attacker's effort and net benefit would be constant with respect to users' valuation. As depicted in Figure 3, if the price, p , is high enough, end-users with moderate valuation would not purchase the service.



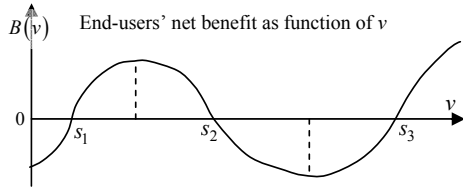
The other common specification is quadratic costs

[8][20]. Then, $C_f(f) = M_f f^2$; $C_a(a) = M_a a^2$.

The attacking efforts and attacker's benefits first increase with end-user valuation, then decrease. End-users with $v = 2\sqrt{\alpha M_f M_a / [1+h][1-\eta]}$ are targeted with the highest attacking effort. As depicted in Figure 4, if the price, p , is high enough, only end-users with $s_1 \leq v < s_2$ or $v \geq s_3$ would buy, where $s_1 < s_2 < s_3$.

Figure 4. Quadratic costs

¹³ The results in Table 3 are according to the proof of Proposition 4 as in the appendix.



6. Implications

Propositions 1 and 4 show that the effect of one user's precautions on the precautions of others depends on the nature of attack. With mass attacks, user precautions are strategic substitutes, as also shown by [12][13]. By contrast, with targeted attacks, end-user precautions are independent of each other.

There is considerable empirical evidence of sluggishness among users in taking precautions. A "war-drive" of residential wireless access points in a college town revealed that, despite the well-publicized risks, almost 40% of the access points were not secured [23]. Even server administrators, who are professionals, suffer from inertia. Rescorla [7] monitored responses to the announcement of a remote buffer overflow vulnerability in Open SSL on July 30, 2002: fixes were installed in 16% of the sample population within the first day, and 20% within the first week, but 60% were never fixed. Among respondents to the Computer Security Institute's 12th annual survey who experienced an intrusion, 46% did not patch the relevant hole [27]. To the extent that the threats in these cases were perceived to be mass rather than targeted, the failure of some users to take precautions is consistent with such precautions being strategic substitutes – some users decided to let others incur the effort to deter the attackers¹⁴.

Our analysis also has implications for the design of experiments and empirical studies. Thus far, survey instruments and empirical measures of information security have not made clear the nature of potential attack – whether mass or targeted (see, for instance, [3][4][5][15][30]). Given that users respond differently to mass vis-à-vis targeted attacks, it is important that survey instruments and empirical measures clearly identify the nature of the threat. Secondly, our analysis shows that even for pure mass or targeted attacks, using a reduced form without consideration of the interactions between end-users and attackers may generate biased results. Particularly, a model with exogenous attacking activity may over-estimate the impact of facilitating precaution on user

¹⁴ The applicability of our analysis to these settings does depend on the assumption that users were aware of other users' precautions.

precaution effort if the effect on demand outweighs the effect on precaution, while it may over-estimate the impact on demand if the effect on precaution outweighs the effect on demand. Table 4 summarizes the potential biases.

Several previous studies of information security assumed specific functional forms for the end user cost of precautions or attacker cost [8][20][25]. Using logarithmic and quadratic functions, we have shown that the strategic interaction between end-users and attackers may be quite sensitive to the assumed cost function. With targeted attacks, attacking effort can be constant over user valuation if costs are logarithmic, but concave if costs are quadratic. Hence, findings based on specific cost functions may not be robust.

Lastly, the government can address information security in two ways – facilitating end-user precautions and enforcement against attackers. By comparing the combination of direct and indirect effects of the two security measures in mass vis-a-vis targeted attacks, we show that facilitating end user precaution may not deter attackers in mass attacks. However enforcement against attackers unambiguously deters attackers in both mass and targeted attacks.

Table 4. Potential biases in reduced form estimates

Bias of the partial impact on	Facilitating end-user precaution		Enforcement against attackers	
	Mass attacks	Targeted attacks	Mass attacks	Targeted attacks
End-user effort in precaution	Under-estimated when lower precaution effect dominates; Over-estimated when shrinking demand effect dominates	Under-estimated	—	—
Attacking effort	—	—	Under-estimated	Under-estimated
Demand for the service	Over-estimated when lower precaution effect dominates; Under-estimated when shrinking demand effect dominates	?	—	—

7. Future work

Our analysis is subject to several limitations. First, we assumed that attackers' benefit is directly related to the end-users' loss. This may not accurately represent some classes of attacks such as where attackers infect end-users' computers with bots which are then

remotely controlled to conduct malicious activities against other machines.

Second, with targeted attacks, we assumed that attackers had unlimited resources. If they were subject to resource constraints, then they would select targets which offer higher expected benefit. In this case, end-user efforts in precautions would be strategic complements. If other end-users increase their precautions, they would become less attractive to attackers, and then attackers would re-direct their effort.

Third, we assumed the price of the service to be exogenous. Future research could consider how the vendor would endogenously adjust price in response to changes in the security environment.

8. References

- [1] Anindya Ghose and Kjell Hausken, "A Strategic Analysis of Information Sharing Among Cyber Attackers", working paper, 24-Aug-2006.
- [2] Ashish Arora, Jonathan Caulkins, Rahul Telang, "Sell First, Fix Later: Impact of Patching on Software Quality", *Management Science*, 52(3), 2006, pp. 465-471.
- [3] Atreyi Kankanhalli, H.H. Teo, B.C.Y. Tan and K.K. Wei (2003), "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management*, 23(2), pp.139-154.
- [4] D. W. Straub, "Effective IS security: An empirical study", *Inf. Syst. Res.* 1, 3, 1990, pp. 255--276.
- [5] Debin Liu, Farzaneh Asgharpour and L. Jean Camp, "Risk Communication in Security using Mental Models", *Usable Security 07*, (Tobago) 16 February 2007.
- [6] Dmitri Nizovtsev and Marie Thursby, "Economic Analysis of Incentives to Disclose Software Vulnerabilities", Working Paper, 2005.
- [7] E. Rescorla, "Security Holes... Who cares?" *Proceedings of the 13th USENIX Security Symposium*, (August 2003), pp.75-90.
- [8] Esther Gal-Or, and Anindya Ghose, "The Economic Incentives for Sharing Security Information", *Information Systems Research*, Vol. 16, No. 2, June 2005, pp.186-208.
- [9] H., B. Mishra Cavusoglu, B. and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture", *Information Systems Research*, Vol. 16 No. 1, 2005, pp.28-46.
- [10] Hal R. Varian, "System reliability and free riding", University of California, Berkeley, November 2004.
- [11] Hasan Cavusoglu, Huseyin Cavusoglu, and Srinivasan Raghunathan, "Analysis of Software Vulnerability Disclosure Policies", *Sauder School of Business*, 2004.
- [12] Howard Kunreuther and Geoffrey Heal, "Interdependent Security: A General Model", Working Paper 10706, National Bureau of Economic Research, August 2004.
- [13] Howard Kunreuther and Geoffrey Heal, "Interdependent Security", *Journal of Risk and Uncertainty*, Vol. 26 Nos. 2-3, March 2003, pp.231-249.
- [14] Hui-wen Koo, and I.P.L. Png, "Private Security: Deterrent or Diversion?" *International Review of Law and Economics*, Vol. 14, March 1994, pp. 87-101.
- [15] I.P.L. Png, Chen-yu Wang and Qiu-Hong Wang, "The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence", *Journal of Management Information Systems*, (forthcoming), 2008.
- [16] Ian Ayres, and Steven D. Levitt, "Measuring the Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack", *Quarterly Journal of Economics*, Vol. 113, No. 1, 1998, pp. 43-77.
- [17] Jay Pil Choi, Chaim Fershtman, and Neil Gandal, "Network Security: Vulnerabilities and Disclosure Policy", The 6th Workshop on the Economics of Information Security, Carnegie Mellon University, The U. S., June 7-8, 2007.
- [18] Jeevan Jaisingh, and Q. Li, "The optimal time to disclose software vulnerability: Incentive and commitment", working paper, November 2005.
- [19] Jeremy Bulow, John Geanakoplos, and Paul Klemperer, "Multimarket Oligopoly: Strategic Substitutes and Complements," *Journal of Political Economy*, Vol. 93 No. 3, June 1985, pp.488-511.
- [20] K. Kannan and Telang, R., "Market for Software Vulnerabilities? Think Again", *Management Science*, Vol. 51, 5 (May 2005), pp.726-740.
- [21] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, (Nov. 2002), pp. 438-457.
- [22] Marco Cremonini and Dmitri Nizovtsev, "Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies", The 5th Workshop on the Economics of Information Security, University of Cambridge, England, 26-28 June 2006.
- [23] Matthew Hottell, Drew Carter and Matthew Deniszczuk, "Predictors of Home-Based Wireless Security", The 5th Workshop on the Economics of Information Security, University of Cambridge, England, 26-28 June 2006.
- [24] Michael E. Whitman, "Enemy at the gate: Threats to information security", *Communications of the ACM*, Vol. 46 No. 8, August 2003, pp.91-95.
- [25] Mohammad S. Rahman, Karthik Kannan and Mohit Tawarmalani, "The Countervailing Incentive of Restricted Patch Distribution: Economic and Policy Implications", working paper, Oct.31, 2006.
- [26] P. Reiss and F. Wolak, "Structural Econometric Modeling: Rationales and Examples from I.O." *Forthcoming in the Handbook of Econometrics*, 2007.
- [27] R. Richardson. 2007 *CSI Computer Crime and Security Survey*, The 12th Annual Computer Crime and Security Survey (Computer Security Institute).
- [28] Ross Anderson and Tyler Moore, "The Economics of Information Security", *Science* 27 October 2006, Vol.314 no. 5799, pp. 610-613.
- [29] S.E. Schechter and M.D. Smith, "How Much Security Is Enough to Stop a Thief?" *Proc. 7th Int'l Financial Cryptography Conf.*, LNCS 2742, Springer-Verlag, 2003, pp. 122-137.
- [30] Scott Boss, "Control, Risk, and Information Security Precautions", *Katz Graduate School of Business*, University of Pittsburgh, 2005.

[31] Symantec, Internet Security Threat Report: Trends for January 05–June 05, Volume VIII, September 2005.
 [32] Symantec, Internet Security Threat Report: Trends for January 06–June 06, Volume X, September 2006.
 [33] Terrence August and Tunay I. Tunca, “Network Software Security and User Incentives”, Management Science, Vol. 52, No. 11, (Nov. 2006), pp. 1703-1720.

9. Appendix¹⁵

Proofs of Observations 1, 3, 4, 5 and 6. The proofs are quite straightforward, thus we ignore the details and only report the results.

For Observation 1, differentiating (4) with respect to v , a , and γ , and hence by (1), we have $\partial f/\partial v > 0$, $\partial f/\partial a > 0$, and $\partial f/\partial \gamma < 0$. For Observation 3, differentiating (5) with respect to a , γ , and p , and hence by (4), we have $\partial \hat{v}/\partial a > 0$, $\partial \hat{v}/\partial \gamma > 0$, and $\partial \hat{v}/\partial p > 0$. For Observation 4, differentiating (7) with respect to η , f , and \hat{v} , and hence by (8), we have $\partial a/\partial \eta < 0$, $\partial a/\partial f < 0$, and $\partial a/\partial \hat{v} < 0$. For Observation 5, differentiating (10) with respect to η , f , and v , and hence by (11), $\partial a/\partial \eta < 0$, $\partial a/\partial f < 0$, and $\partial a/\partial v > 0$. For Observation 6, differentiating (3) with respect to v , and hence by (4), we have $\partial B(v|a)/\partial v > 0$ if and only if,

$$v/a \times \partial a/\partial v < 1/a[1+h][1-f]-1. \quad (\text{A1}). \quad []$$

Proof of Observation 2. We first prove that $B(v)$ is monotone increasing in v . Consider v_1 and v_2 such that $v_1 < v_2$. Let user v_2 choose precautions, $f(v_2)$, associated with user v_1 . Since $v_1 < v_2$, her expected net benefit would be:

$$\begin{aligned} & v_2 - v_2[1+h][1-f(v_1)]a - p - \gamma C_f(f(v_1)) \\ & > v_1 - v_1[1+h][1-f(v_1)]a - p - \gamma C_f(f(v_1)) \equiv B(v_1|a), \end{aligned} \quad (\text{A2})$$

By (3), the precaution $f(v_2)$ must provide user v_2 with the maximum expected net benefit, and, in particular,

$$\begin{aligned} B(v_2|a) &= v_2 - v_2[1+h][1-f(v_2)]a - p - \gamma C_f(f(v_2)) \\ &\geq v_2 - v_2[1+h][1-f(v_1)]a - p - \gamma C_f(f(v_1)). \end{aligned} \quad (\text{A3})$$

Hence, by (A2) and (A3), $B(v_2|a) > B(v_1|a)$, which is the result. Since $B(v)$ is monotone increasing in v , the demand for the service is characterized as follows. Consider the highest valuation user with $v = \bar{v}$. By (4), her precaution effort will be the highest among users, so is her net benefit. If $B(\bar{v}) \leq 0$, then, $B(v) < 0$ for all $v > 0$ and all other users would not buy. However, if $B(\bar{v}) > 0$ but $B(0) < 0$, there exists users with \hat{v} , such that the other users with $\hat{v} \leq v < \bar{v}$ would buy. []

Proof of Lemma 1. By Observations 1 and 3 respectively, f is increasing in a and \hat{v} is decreasing in a . Accordingly,

[34] Yeh-ning Chen, and I.P.L. Png, “Information Goods Pricing and Copyright Enforcement: Welfare Analysis”, Information Systems Research, Vol. 14 No. 1, March 2003, pp.107-123.

$L(a)$ is monotonically decreasing in a . Further, if $a=0$, all users would choose $f=0$. By (3), we get $B(v)=v-p > 0$ and all

users would buy the service, and so $L(0) > 0$. With regard to attacker’s effort, by Observation 4, a is monotonically increasing in L . Further, if $L=0$, then attacker will not target the service, $a=0$. Since the functions $L(a)$ and $a(L)$ are continuous as shown in Figure 2, they have a non-trivial intersection, say (a^*, L^*) . []

Proof of Proposition 1. Expanding (8) to distinguish between the precaution of end-user v' denoted $f(v')$ and the precautions of all other users, f ,

$$[1-\eta] \left\{ \begin{aligned} & \int_{[v',v']} v[1-f]d\Phi(v) \\ & + v'[1-f(v')]d\Phi(v') + \int_{(v',1]} v[1-f]d\Phi(v) \end{aligned} \right\} = \frac{dC_a}{da}. \quad (\text{A4})$$

By (A4), an increase in precautions, f , by all other users except v' would reduce the overall conditional loss represented in the brackets of the left-hand side, and hence induce attacker to reduce attacking effort. This would imply a decreasing in the attacking effectiveness a . User v' adjusts her precaution following the net-benefit maximizing function represented by equation (4). A decreasing in a shifts down the left-hand side in (4). Therefore, user v' would reduce $f(v')$. []

Proofs of Propositions 2 and 3. We first investigate the combined direct and indirect effects of precaution cost on attacker’s effort, end-users’ precaution and demand.

$$\frac{da}{d\gamma} = \frac{\partial a}{\partial \gamma} + \frac{\partial a}{\partial L} \frac{dL}{d\gamma} = \frac{\partial a}{\partial L} \frac{dL}{d\gamma}, \quad (\text{A5})$$

$$df/d\gamma = \partial f/\partial \gamma + \partial f/\partial a \times da/d\gamma, \quad (\text{A6})$$

$$d\hat{v}/d\gamma = \partial \hat{v}/\partial \gamma + \partial \hat{v}/\partial a \times da/d\gamma. \quad (\text{A7})$$

By solving the above equations, we have

$d\hat{v}/d\gamma > 0$ and $df/d\gamma < 0$. $da/d\gamma > 0$ if and only if $\partial L/\partial \gamma > 0$, or

$$\hat{v}[1-f(\hat{v})] \frac{d\Phi(\hat{v})}{d\hat{v}} \frac{\partial \hat{v}}{\partial \gamma} < - \int_{\hat{v}}^1 v \frac{\partial f}{\partial \gamma} d\Phi(v). \quad (\text{A8})$$

Increasing precaution cost has two effects: lower precaution and shrinking demand. (A8) implies that the attacker’s effort increases in γ if and only if the lower precaution effect (the right-hand side of (A8)) dominates the shrinking demand effect. (the left-hand side of (A8)).

Further $\frac{da}{d\gamma} = \left[\frac{d\hat{v}}{d\gamma} - \frac{\partial \hat{v}}{\partial \gamma} \right] / \frac{\partial \hat{v}}{\partial a} = \left[\frac{df}{d\gamma} - \frac{\partial f}{\partial \gamma} \right] / \frac{\partial f}{\partial a}$. Thus,

the sign of $da/d\gamma$ is the same as the signs of

$[d\hat{v}/d\gamma - \partial \hat{v}/\partial \gamma]$ and $[df/d\gamma - \partial f/\partial \gamma]$. When the

¹⁵ Due to limitations of space, we present only sketches of the proofs here. The complete proofs are available upon request.

shrinking demand effect is dominated, $d\hat{v}/d\gamma > \partial\hat{v}/\partial\gamma$ and $df/d\gamma < \partial f/\partial\gamma$. When the reducing precaution effect is dominated, $d\hat{v}/d\gamma < \partial\hat{v}/\partial\gamma$ and $df/d\gamma > \partial f/\partial\gamma$.

Following the similar process, we have $da/d\eta < 0$, $d\hat{v}/d\eta < 0$ and $df/d\eta < 0$; $da/dp < 0$, $df/dp < 0$; $d\hat{v}/dp > 0$ but $d\hat{v}/dp < \partial\hat{v}/\partial p$. []

Proof of Proposition 4. Differentiating f and a with respect to v , we have

$$df/dv = \partial f/\partial v + \partial f/\partial a \times da/dv, \quad (A9)$$

$$da/dv = \partial a/\partial v + \partial a/\partial f \times df/dv, \quad (A10)$$

By solving the above equations, we have $df/dv > 0$, $da/dv > 0$ if and only if

$$v/f \times \partial f/\partial v < [1/f - 1]. \quad (A11)$$

Now consider the impact of precaution cost and enforcement rate on demand of the service. Following similar process as (A9) and (A10), we can derive $df/d\gamma < 0$ and $da/d\gamma > 0$. Denote \hat{v} as the valuation of users with $B(\hat{v}) = 0$. Note that $B(v)$ is not monotone in v . Thus, the total demand of the service can be represented as:

$$Q_t = \sum_{v_1, v_2}^{v_2} \int_{v_1} d\Phi(v) + \sum_{v_3, v_4}^{v_4} \int_{v_3} d\Phi(v) \quad (A12)$$

where $B(v_1) = 0$, $B(v_2) > 0$, $dB(v)/dv > 0$ for $v \in [v_1, v_2]$; $B(v_3) > 0$, $B(v_4) = 0$, $dB(v)/dv < 0$ for $v \in (v_3, v_4]$. The parameterization $[v_1, v_2]$ and $(v_3, v_4]$ represent any small region of v where $B(v)$ is monotone in v . The total demand of the service is the sum of the integrations of all these regions. Hence the sufficient condition for $dQ_t/d\gamma < 0$ are:

For all v_1 and v_4 , $dv_1/d\gamma > 0$ and $dv_4/d\gamma < 0$. (A13)

The same rationale can be applied to the impacts of η and p . Differentiating $a(\hat{v})$, $f(\hat{v})$, and \hat{v} with aspect to γ , and combining the equations, we have

$$\left[1 - \frac{\partial \hat{v}}{\partial a} \frac{da}{dv} \right] \frac{d\hat{v}}{d\gamma} = \frac{\partial \hat{v}}{\partial \gamma} + \frac{\partial \hat{v}}{\partial a} \frac{\partial a}{\partial f} \frac{df}{d\gamma} > 0. \quad (A14)$$

The sign of $d\hat{v}/d\gamma$ is the same as $[1 - \partial\hat{v}/\partial a \times da/dv]$.

Differentiating (5) with aspect to a and substituting $\partial\hat{v}/\partial a$ into (A14), we have $d\hat{v}/d\gamma > 0$ if and only if

$$1 - [1 + h][1 - f][a + \hat{v} da/dv] > 0. \quad (A15)$$

Further, $dB(v|a)/dv > 0$ if and only if (A15). Thus, if

$dB(\hat{v})/dv > 0$, $d\hat{v}/d\gamma > 0$; if $dB(\hat{v})/dv < 0$, $d\hat{v}/d\gamma < 0$.

Following (A13), we have $dQ_t/d\gamma < 0$.

Similarly, if $dB(\hat{v})/dv > 0$, $d\hat{v}/d\eta < 0$; if $dB(\hat{v})/dv < 0$, $d\hat{v}/d\eta > 0$. Following (A13), we have $dQ_t/d\eta > 0$.

Finally, if $dB(\hat{v})/dv > 0$, $d\hat{v}/dp > 0$; if $dB(\hat{v})/dv < 0$, $d\hat{v}/dp < 0$. Following (A13), we have $dQ_t/dp > 0$. []

Proofs of specific cost functions: Briefly, we substitute the specific cost functions of user precaution and attacker's effort into (4) and (11) respectively to derive the optimal f^* , a^* , and $B^*(v)$ as functions of v . Then by differentiating the functions f^* , a^* , and $B^*(v)$ with aspect to v , we have:

- For logarithmic cost function, $da/dv=0$, $dB^2(v)/dv^2 > 0$, and $dB(v)/dv > 0$ if and only if $v > \gamma M_f$.
- For quadratic cost function, $df/dv > 0$, $da/dv > 0$ if and only if $v \leq 2\sqrt{\gamma M_f M_a} / [1 + h][1 - \eta]$. Either $dB(v)/dv > 0$ for all v ; or there exist v_1 and v_2 , such that for $v \leq v_1$ or $v > v_2$, $dB(v)/dv > 0$; for $v_1 < v \leq v_2$, $dB(v)/dv \leq 0$. []