Who is responsible for the onus of proof on online fraud transactions? In perspectives of the eCommerce Law and Privacy Investment (온라인 거래에서 사고 발생시 누가 이의 입증책임을 질 것인가?)

Se-Hak Chun[a], Woo-je Cho[b], Jae-Cheol Kim[c]

aDepartment of e-Business Management, Seoul National University of Technology, 172, Gongreung 2-Dong, Nowon-Gu, Seoul, 139-743, Korea
Tel: +82-2-970-6114, Fax: +82-2-970-6088, E-mail: realsteed@snut.ac.kr
bUniversity of Illinois at Urbana-Champaign, Department of Business Administration 1206 S. Sixth Street, Champaign, IL 61820, USA
cKAIST, Graduate School of Management, 207-43 Cheongryangri-dong, Dongdaemoon-gu, Seoul 130-012, Korea

Abstract

In this study, we examine why there exist different legal systems in electronic commerce or online financial trading. When a fraud online transaction occurs and the online customer disputes the transaction, the online customer takes responsibility for the proof of her/his argument in many European countries while in the U.S., the burden of proof lays on the firm. This paper analyzes how these two different legal systems exist and how these can be applied to electronic commerce law. In particular, this paper intends to find the optimal level of e-commerce firms' investment on security and analyzes how security investments can be related to firm's profits and consumer's welfare depending on IT infrastructure and social trust environment. More on, this paper can be contributed to provide guidelines for regulatory framework on ecommerce online transactions and discuss social welfare implications.

Keywords

Security and Privacy; Onus of Proof, Electronic Commerce; E-commerce Law; Electronic Commerce Regulation

I. Introduction

Internet has changed many of the forms in which we do business and encourages many firms to get involved or shift into e-commerce. The compound annual growth rate of e-commerce in the U.S. is 25 % during the past five years, and it accounts for more than 2% of all retail sales. At the same time, the growth rates in South Korea and the U.K. are 50% and 80%, respectively (Mientka, 2006). As the size of e-commerce economics increases, e-commerce security is still a critical obstacle that hinders faster growth of e-commerce. The security risk of e-commerce is growing in similar scope and scale with the growth of e-commerce. For example, according to a study in 1999 by Meridien Research, credit card frauds charged merchants more than $40 million per year, and $60 billion was estimated for the loss in 2005 (Tribunella, 2002). Although much effort has been made for secure online transactions, serious security accidents, such as credit card frauds and hackings, are still occurring.

There are several factors that have caused e-commerce security risks. Ghosh (2004) addresses three main factors of e-commerce security problems: first, the dependency on the electronic medium for firms' core business, second, the growing complexity needed to support complex e-commerce transactions, and third, the high value of the digital assets flowing through the Internet. Kim et al. (2005) suggest three high-level categorizations of e-commerce security: security managerial issues, fundamental security issues, and security technology issues. In general, e-commerce security problems can be approached from three perspectives: technical issues, managerial/policy issues, and legal issues. The three issues should be equally stressed; lack of caution in one among the three could cause irreversible security accidents. But, since few e-commerce security works encompass legal issues in analyzing e-commerce framework, we focus on the e-commerce law as a determinant of e-commerce firms and online customers' decisions.

The purpose of this study is to investigate the effects of several countries' legal environment on e-commerce security risks and to discuss e-commerce firms' behavior in regard to their security. In particular, we intend to study the e-commerce firms' decision on the level of investment on security and consumers' participation in e-commerce under different laws in the U.S. and European countries.

II. Research Background and Framework

E-Commerce Framework

The e-commerce framework consists of three main entities: e-commerce firms, online customers, and governments that provide e-commerce laws. First, e-commerce firms create electronic markets and sell their products to intermediate buyers and sellers. The objective of the firm is to achieve the highest profit through its e-commerce channel, so their decision on investments on security will align with the objective. Second, online customers determine demands on electronic markets. The customer's payoff obtained by participating in e-commerce would be determined by various factors, including the perceived convenience and the perceived security risk. Third, governments provide regulatory skeletons to promote e-commerce or minimize risks occurring in e-commerce transactions. Today, countries

have their own e-commerce laws and some of them have contrary provisions. In this study, we argue that different legal systems for e-commerce will lead to different outcomes in e-commerce in terms of the level of firms' investment on security and consumers' participation in e-commerce.

E-commerce Security

From e-commerce firms' perspective

E-commerce security could influence the firm's performance in various ways. For example, insecure e-commerce systems may result in a decrease of sales revenue by discouraging potential customers from purchasing goods or may cause security accidents that could lead to a huge financial loss on the part of the firm. Thus, the firm has an incentive to invest on security. However, the level of investment could vary depending on the e-commerce legal system under which the firm is regulated. For instance, if the law is more favorable to e-commerce firms when fraud transactions are disputed, the firm has less incentives to invest on security. Vise versa, if the law is more favorable to online consumers, the firm has a stronger incentive.

In this study, we focus on the e-commerce firm's decision on investments on security as a decision variable because it is one of the most fundamental decisions that the firm makes when determining the level of its e-commerce security. To enhance the security of e-commerce systems, firms need to approach the issue from both a managerial and technical perspective. In addition, they need to understand laws and regulations for e-commerce. Typical managerial security issues include risk analysis management, privacy and ethics, security evaluation, and security policy; technical issues include database security, web security, network security, system security management (Kim et al, 2005). The firm needs to consider all of the issues above to enhance its security, but the fundamental decision that the e-commerce firm has to make is the amount of investment or budget allocation for its security. The detailed technical and managerial issues would be planned and conducted within the budget. Without senior level managers' support in the form of budget, it would be hard to have highly secured e-commerce systems even though an e-commerce firm may have the ability to conduct each security task well. Thus, we focus on the level of investment on security as the firms' decision variable.

E-commerce firms are more likely to be victims of fraud online transactions, such as credit card fraud and privacy problems, rather than online customers. Credit card frauds, in most cases, result in e-commerce companies' financial loss because the company has to take responsibility for fraud payments made with stolen credit cards in many countries. Although many online customers fear potential credit card frauds, in most cases, merchants become a victim of the fraud, while off-line credit card frauds generally end up in card holders' loss if merchants follow proper procedures. For example, Expedia.com lost more than $4 million when airline tickets were purchased with stolen credit cards (Laudon & Traver, 2002, p. 229). In this regard, e-commerce firms have strong incentives to enhance security and prevent credit card frauds.

From customers' perspective

E-commerce definitely gives consumers some benefits, such as lowering search costs and overcoming regional distances. But there are some challenges in e-commerce from the customers' perspective. Among the challenges, customers' trust in e-commerce sites is one of the critical factors. In general, the trust is determined by the security level of e-commerce sites. Suh and Han (2003) identify that the customer's perception of security control has influence on the customer's e-commerce acceptance, mediated by trust. We argue that the perceived security level or trust of an e-commerce site can vary with different e-commerce laws. For instance, if the law is more favorable to e-commerce firms when fraud transactions are in dispute, consumers have less incentive to participate in e-commerce. Vise versa, if the law is more favorable to online consumers, consumers will have stronger incentives.

Discussion of credit card frauds is very meaningful because it is perhaps the most frequent form of e-commerce crimes. Credit card fraud is a major threat that online customers fear when they pay with their credit card, though, in most cases, merchants have to pay for credit card frauds (Laudon & Traver, 2000). An e-commerce company cannot attract customers unless they give them trust about the security of their e-payment. In this regard, many small e-commerce sites outsource e-payment systems, such as to yahoo e-payment, to give online customers the trust though it costs them lots of fees compared to the size of their sales. The exposure of private information as a challenge to the e-commerce growth is also an important issue in our study because credit card frauds may result from exposure of personal financial information. Since exposure risks of private information do not appear to be reduced despite outstanding technological advance in Internet security, customers are reluctant to provide their private information to e-commerce sites (Keen et al, 2000; Ott, 2000). The amount of spam mail delivered to Internet users and calls from telemarketers never seem to decrease or even worse, seem to increase. Most e-commerce sites require customers to register and sign into their sites, and they have a number of required personal information. The private information could be exposed by hackers, intentionally be sold by someone in the e-commerce site, or be uncovered due to the lack of appropriate internal security policies. The private information might include very crucial information, such as the user's SSN, bank account information, password, etc. Thus, many Internet users prefer purchasing goods from a well-known and reliable site rather than small-size sites even when the well-known site sells the good at a higher price. As the perceived threat increases, more customers refrain from participating in e-commerce. However, the threat can be mitigated if ex post risks are lowered by e-commerce regulation.

In summary, we can perceive that different laws about fraud online transactions would induce e-commerce firms and online customers to behave differently. The e-commerce laws more favorable to consumers in case of fraud online transactions will motivate firms to spend more on security and drive consumers to participate more in e-commerce. On the other hand, e-commerce laws more favorable to

e-commerce firms in the same case will drive firms to invest less on security and drive consumers to participate less in e-commerce.

However, the amount of a firm's expenditure on security does not mean the superiority of one type of e-commerce regulation over the other. We also intend to see whether a lower level of a firm's investment in security under one type of e-commerce laws will create greater profit than a higher level of a firm's investment on security under the other type of e-commerce law.

E-Commerce Law in the U.S. and Europe

E-commerce laws define and clarify regulatory framework. Parties participating in the transaction make their decisions under these laws. The legal systems in the U.S. and in Europe are often compared to each other since the laws in these two regions are some contrary provisions. We intend to examine how the different legal systems regarding e-commerce affect e-commerce firms' investments on their security and online consumer behaviors. In particular, when a fraud online transaction, laws in the U.S. and some European countries are quite different; the U.S. e-commerce law appears to be more favorable to customers, but the e-commerce of law in the U.K. and some other countries is likely to be more favorable to e-commerce firms (Anderson, 1994; Anderson, 2002).

III. The Model

We analyze two different e-commerce legal systems regarding whether the onus of proof should lied on customers or firms when a security accident occur. In the U.S., when a dispute regarding an online transaction arises between a customer and an e-commerce site, the burden of proof is given to the e-commerce site. If the e-commerce site cannot prove the transaction is correct, it has to accept the customer's argument and it has to refund money to the consumer. But, in the U.K., Norway, and the Netherlands, the burden of proof is given to online customers (Anderson, 2002). We analyze two situations depending on the onus of proof in the transaction dispute between customers and firms.

When the Onus of Proof is on E-commerce Firm

We assume that consumers are uniformly distributed along $[0, V]$ according to their reservation prices, P, and consumers purchase one unit of product. A consumer, $v \in [0, V]$ will obtain the surplus, $U(v) = v\text{-}P$, in consuming a product and will buy the product if $v\text{-}P>0$. Thus, the demand, Q, will be $V\text{-}P$.

We assume that there is an e-commerce firm which sells a product through the Internet and there are two cost types when a security accident occurs. The first type can be general security costs related to security accident or disaster, which is denoted by $R(\bullet)$. The second type can be proof costs when a firm spends to prove the accident is not its responsibility, which is denoted by $S(\bullet)$. Both costs are reduced when a firm invests more on security level and these are assumed to have negative relationships with the amount of the investment, denoted by I. Thus, $\frac{\partial R(\bullet)}{\partial I}<0$ and $\frac{\partial S(\bullet)}{\partial I}<0$. Also these are slowly reduced as a firm increases the investment level, thus $\frac{\partial^2 R(\bullet)}{(\partial I)^2}<0$ and $\frac{\partial^2 S(\bullet)}{(\partial I)^2}<0$.

$R(\bullet)$ and $S(\bullet)$ can be affected by other external security factors in a micro perspective such as the unit cost per proof and the initial probability of security accident when there are no investment on security. These factors affect on the security level according to individual firm's various situations such as culture, security and privacy policy, etc,. We denote a degree of the monetary loss from the onus of proof by a and the initial risk probability exposed to security accident when the firm does not invest on any kinds of security by s. Thus, as a and s increase the overall security costs increase. Last, $R(\bullet)$ and $S(\bullet)$ can be affected by other external factors in a macro perspective, thus these are related to national level such as national culture, behavior, and IT infrastructure, etc,. rather than individual firm's level. We denote these factors by k relating to a elasticity of investment. Thus, low k means the unit effect of the investment is low and it represents the society has higher IT infra level, K. While high k means that the unit effect of the investment is high and represents the society has low K because a little increase in investment can make the security risk lower. For example, if one country increases investments in the fundamental IT infra level or has more positive morality or attitude, the firm will have less experience on security disaster and overall security costs will decrease. Then, the firm in this case will find an optimal security investment level to maximize its profit and the profit function can be represented as below.

$$\Pi_1 = P_1 Q_1 - R(I_1; a_1, s_1, k_1) - S(I_1; a_1, s_1, k_1) - I_1 \quad (1)$$

,where the subscript 1 means the first case we analyze, P is price of the goods, Q is the demand or sales, $R(\bullet)$ is the general security disaster costs, $S(\bullet)$ is the proof costs for security accidents, and I is the amount of the investment on its security. Without loss of generality we can assume that the security disaster costs, $R(\bullet)$, and proof costs, $S(\bullet)$, have a positive relationship with the sales size. That is, if the number of the transaction and the amount per transaction increase there exist more possibilities that security costs occur higher. We can interpret the number of the transaction as quantities or demands and the amount per transaction as a price, thus, $R(\bullet)$ and $S(\bullet)$ have a direct relationship with total sales level. Considering all these factors we can represent $R(\bullet)$ as follows;

$$R(I;a,s,k,P,Q) = dprob \times sales = \frac{s}{1+kI} PQ(P) = \frac{s}{1+kI} P(V-P) \quad (3)$$

The first part of security disaster costs means a probability when a security accident occurs. The security costs decrease as a firm invests more on security depending on the initial s and I level. The latter part means total sales level. Without loss of generality we can assume that the security disaster costs and proof costs have a positive relationship with the sales size. This is because if the number of the transaction

and the amount per transaction increases there exist more possibilities that security costs occur higher. Also we can represent $S(\bullet)$ by a positive linear relationship with $R(\bullet)$. Thus, $S(\bullet)$ is the portion of the $R(\bullet)$ denoted by α' and $\alpha' < 0$. $S(\bullet)$ can be shown as follows.

$$S(I;a,s,k,P,Q) = \alpha' \frac{s}{1+kI} P(V-P) \quad (4)$$

Since the proof costs are simply assumed to have a positive relation with security damage costs, from (1) through (4) the firm's profit function can be represented as follows.

$$\begin{aligned} \Pi_1 &= P_1 Q_1 - R(I_1;a_1,s_1,k_1) - S(I_1;a_1,s_1,k_1) - I_1 \\ &= P_1(V-P_1) - \frac{s}{1+kI} P_1(V-P_1) - \alpha' \frac{s}{1+kI} P_1(V-P_1) - I_1 \quad (5) \\ &= P_1(V-P_1) - (1+\alpha')\frac{s}{1+kI} P_1(V-P_1) - I_1 \\ &= P_1(V-P_1) - \alpha \frac{s}{1+kI} P_1(V-P_1) - I_1 \end{aligned}$$

,where $\alpha = \alpha' + 1$ and $\alpha > 1$.

The term $\frac{\alpha s}{1+kI} P_1(V-P_1)$ represents the overall costs for security accidents including proof costs those firms like an e-commerce firm bear when firms invest the amount of I on security. From the first order condition we find an optimal price and the level of investment on security that maximizes the firm's profit as follows.

$$P_1^* = \frac{V}{2} \quad (6)$$

$$I_1^* = -\frac{1}{k_1} + \frac{1}{2}\sqrt{\frac{\alpha s_1}{k_1}} V \quad (7)$$

When the Onus of Proof is on Online Customers

When the onus of proof for security accident lies on consumers' side, the firm does not worry about the proof burden for the fraud online transaction. Thus, the proof cost term, $S(\bullet)$, is not in the firm's profit as follows;

$$\Pi_2 = P_2 Q_2 - R(I_2;a_2,s_2,k_2) - I_2 \quad (8)$$

,where the subscript *2* means the second case we are analyzing.

Under the regulation that the burden of proof lies on the customer side, the value which customers feel when they buy goods through the online transaction decrease as security disaster risk increases, thus, net consumer utility, U, who has valuation v, can be written as follows;

$$U = v - P_2 - \frac{\alpha s_2}{1+k_2 I_2} P_2. \quad (9)$$

Thus, a consumer whose net utility is nonnegative will buy goods and the demand will be

$$Q = V - P_2 - \frac{\alpha s_2}{1+k_2 I_2} P_2. \quad (10)$$

Then, the firm's profit is

$$\begin{aligned} \Pi_2 &= P_2 Q_2 - R(I_2;a_2,s_2,k_2) - I_2 \\ &= P_2\left(V - P_2 - \frac{\alpha s_2}{1+k_2 I_2}\right) - \frac{s_2}{1+k_2 I_2} P_2\left(V - P_2 - \frac{\alpha s_2}{1+k_2 I_2} P_2\right) - I_2 \end{aligned} \quad (11)$$

From the first order condition, we find an optimal price and security investment that maximizes the firm's profit as follows;

$$P_2^* = \frac{V}{2} - \frac{\alpha\sqrt{s_2}}{\sqrt{(1+\alpha)k_2}} \quad (12)$$

$$I_2^* = -\frac{1+\alpha s_2}{k_2} + \frac{1}{2}\sqrt{\frac{(1+\alpha)s_2}{k_2}} V \quad (13)$$

IV. Strategic Implications for Ecommerce Law and Optimal Security Investment Policy

In this section we discuss the conflict question that why the onus of proof in security accident or fraud transaction in electronic commerce or e-banking areas can be different across countries or culture or IT infrastructure level etc., and we suggest new guidelines for countries which have not prepared a specific ecommerce law or e-banking transaction law. Also we discuss recently U.S government enforce any companies to have privacy departments, which drives firms to increase security investment amount. Our results show this enforcement does not make worse in firm's profit, but rather in some conditions, an increase in security investment can guarantee better profit for firms.

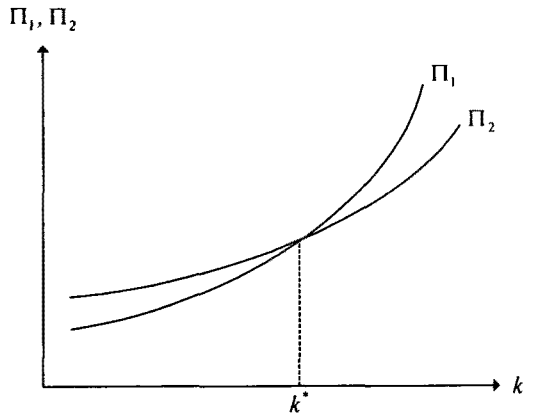
Why does different regulations exist?–Implications in an ecommerce perspective

From optimal prices and security investment level we can draw firms' profits and compare two cases with discussion implications. For compare two regulation effects we set $s_1 = s_2 = s$ and $k_1 = k_2 = k$, then, the following proposition is derived as follows;

Proposition 1.

$$\Pi_1^* \underset{<}{\geq} \Pi_2^* \quad \text{if } \sqrt{k} \underset{<}{\geq} \frac{\alpha\left(\sqrt{\alpha+1}+\sqrt{\alpha}\right)\sqrt{s}}{V}.$$

Proof. Omitted because it can derived from a comparison of the firm's profits for each case. □



[Figure 1]. Profits and k (when V is relatively lower)

Proposition 1 means that if k is enough the profit of the case 1 is more profitable than the case 2 while if k is not enough situation the profit of the case 1 is less than the case 2. Since we interpreted the factor, k as a elasticity of the investment in national security level or overall unit investment effect on the security risk or a measure of the morality or attitude, if the country or society has lower k(in case that society has more Infra Level, K), the government will tend to choose the case 1 regulation and if the country or society has higher k, the government will tend to choose the case 2. This proposition can be applied to ecommerce or e-banking situations. If k is higher situation, even the government can burden the onus of proof on the firm, the firm will have no loss experiences.

Corollary 1. $\frac{\partial k^*}{\partial \alpha} > 0, \frac{\partial k^*}{\partial s} > 0, \frac{\partial k^*}{\partial V} < 0$

Corollary 1 means that if α , s becomes increase, the firm wants to be in case 2. In this case if government give the burden of the proof on consumer side the consumer will resist[1] and if government give the burden of the proof on firm side the firm will resist, which always results in conflicting situation. Thus, the government should invest more on IT security or some Infrastructure in this situation. However, when the V is larger, the firm will have burden the onus of the proof. This can be very strict conclusion, when the product is very expensive and the security disaster happens if the government gives the burden the onus proof the consumer's resistance will be very high and market can be no longer exist. This means if the product is more expensive the case 1 will be more often, thus, firm will burden the onus of the proof.

The Regulation on security investment level can be enforced?-In a firm's profit perspective: relationship between security investment level and profit

From the above results we can draw the following proposition.

Proposition 2.

$$I_1^* \underset{>}{\overset{\leq}{}} I_2^* \quad \text{if} \quad \sqrt{k} \underset{<}{\overset{\geq}{}} \frac{2\alpha\left(\sqrt{1+\alpha}+\sqrt{\alpha}\right)\sqrt{s}}{V}.$$

Proof. Omitted because of simple calculation of comparison between two investment levels.

[1] We also need to check consumer's welfare for the case 2.

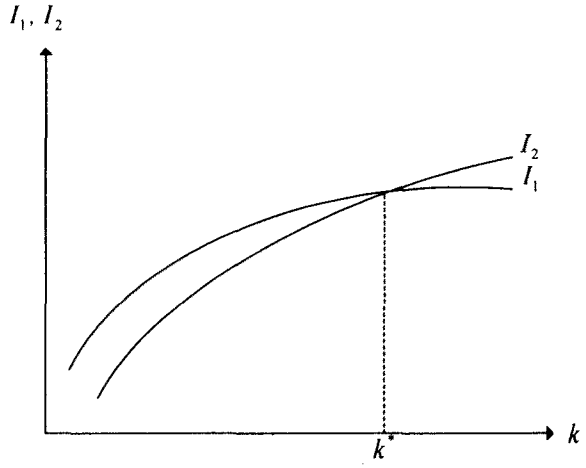


Figure 2. Optimal Investement and Infra level

The proposition 2 is very related to the first proposition 1. This means that if the society has better Infra level (low k), the firm will tend to increase investment on security level when government enforces the onus of the proof on the firm side while the society has worse Infra level (high k) , the firm will tend to increase on security when government enforce the onus of the proof on consumer side.

Proposition 3.

$$\text{If} \frac{\alpha\left(\sqrt{1+\alpha}+\sqrt{\alpha}\right)\sqrt{s}}{V} \leq \sqrt{k} \leq \frac{2\alpha\left(\sqrt{1+\alpha}+\sqrt{\alpha}\right)\sqrt{s}}{V}, \Pi_1 \geq \Pi_2 \text{ for } I_1 \geq I_2.$$

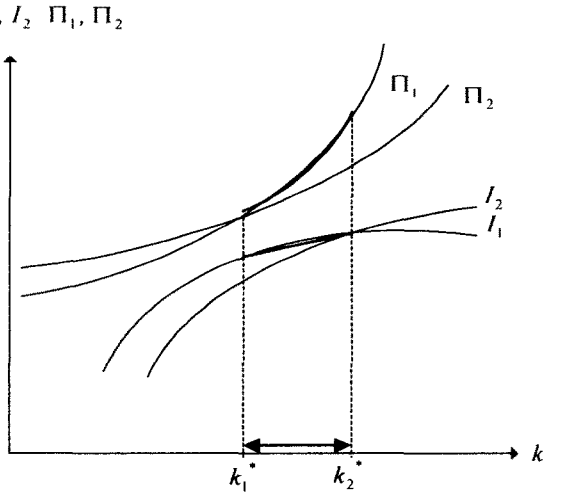


Figure 3. The Condition of the Government enforcement on Security Investment.

The proposition 3 means there exists the condition that even though the firm spends more money on security level the firm can attain better profitability. Within some area of the k in figure 3, if the firm will have a incentive to invest more on security to secure its profit. This is in line with that recently U.S. government tends to enforce that firms should have spend more on security and privacy level. This result can give some guideline for some country which still does not prepare electronic commerce law on fraud transactions.

V. Conclusion and Future Work

There are a number of papers that address firms' security issues qualitatively either with a technical approach or with a managerial approach. However, there are few studies that provide the optimal level of firms' investment on security with analytical mathematical models. Thus, the value of our study lies in making a contribution to the academic stream of security by exploring an analytical mathematical model that may be helpful in understanding the nature of security issues.

In industry, firms' investment on security is a very difficult decision because the uncertainty of security accidents is very high and the scope of financial damage for each security accident is very wide. Therefore, most companies spend more money ex post security costs rather than ex ante security costs. However, our model may provide a guideline for e-commerce firms to find an appropriate level of investment on security.

Our study may be useful for governments in regulating the e-commerce industry of their countries. Many countries are still refining their regulations about e-commerce since e-commerce is quite a new area and keeps changing in scope, magnitude, and form. Using our model, governments may understand how their regulations affect the behavior of e-commerce firms and online consumers, and Pareto efficiency.

VI. Reference

Anderson, R. "Why Cryptosystems Fail," Communications of the ACM, (37:11), 1994, pp. 32-40.

Anderson, R. "Why Information Security is Hard," University of Cambridge, working paper, 2002

Ghosh, A. K. "E-commerce Security and Privacy," Kluwer Academic Publishers, 2001.

Hiller, J. S., and Cohen, R. *Internet Law & Policy*, Upper Saddle River, Prentice Hall, New Jersey, 2002.

Keen, P.; Balance, C; Chan, S.; and Schrump, S. *Electronic Commerce Relationships: Trust by Design.* Upper Saddle River, NJ: Prentice-Hall, 2000.

Kim, H., Han,Y. Kim, S. and Choi, M. "A curriculum design for E-commerce security," Journal of Information Systems Education, (16:1), 2005, pp. 55-64.

Laudon, K. C., and Traver, C. G. *E-commerce: Business, Technology, Society*, Addison Wiley, 2001

McClure, S. and Scambray, J, "Growing vulnerabilities in e-commerce apps present the latest challenge to security," *InfoWorld*, (22:17), 2000, pp. 52.

McCusker, R. "E-commerce security: The birth of technology, the death of common sense?" *Journal of Financial Crime*, (9:1), 2001, pp. 79.

Mientka, M. - Behavioral biometrics to improve E-commerce security, AFP Exchange, Jan/Feb 2006.

Ott, R. "Building trust online," Computer Fraud & Security, (2), 2000, pp. 10-12.

Raisinghani, M. S. "E-commerce security: An organizational perspective," *Journal of Electronic Commerce in Organizations*, (1:2), 2003

Spindler, G., and Borner, F. *E-Commerce Law in Europe and the USA*, Springer, 2002.

Suh, B., and Han, I. "The impact of customer trust and perception of security control on the acceptance of electronic commerce," *International Journal of Electronic Commerce*, (7:3), 2003, pp. 135-161.

Tribunella, T., and Colson, R. H. "Twenty Questions On E-Commerce Security," *CPA Journal*, (72:1), 2002, pp. 60.

Wang, W., Hidvégi, Z., and Whinston, A. B. "Designing mechanisms for E-commerce security: An example from sealed-bid auctions," *International Journal of Electronic Commerce*, (6:2), 2001, pp. 139.

Williams, D."The relevance of legal awareness in e-commerce security," *Journal of Database Marketing*, (8:3), 2001, pp. 217.

Williams, K. "How secure is e-commerce?" *Strategic Finance*, (81:9), 2000, pp. 23.

Williams, K. "Preparing your business for secure e-commerce," *Strategic Finance*, (82:3), 2000, pp. 21.

http://www.cybersource.com/news_and_events/view.xml?page_id=1313