December 2005

I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security

Hyeun-Suk Rhee
University of Texas at Dallas

Young Ryu
University of Texas at Dallas

Cheong-Tag Kim
Seoul National University

I AM FINE BUT YOU ARE NOT: OPTIMISTIC BIAS AND ILLUSION OF CONTROL ON INFORMATION SECURITY

Hyeun-Suk Rhee
School of Management
University of Texas at Dallas
Dallas, TX U.S.A.
suerhee@utdallas.edu

Young U. Ryu
School of Management
University of Texas at Dallas
Dallas, TX U.S.A.
ryoung@utdallas.edu

Cheong-Tag Kim
Department of Psychology
Seoul National University
Seoul, Korea
ctkim@snu.ac.kr

Abstract

*Information security is a critically important issue in current networked business and work environments. While there is extensive publicity on the increasing incidents of numerous information security breaches and their serious consequences, recent surveys and research on information security repeatedly identify the low levels of user and managerial **awareness** as a key obstacle to achieving a good information security posture.*

The main motivation of our research emanates from this contradicting phenomenon: increased vulnerability to information security breaches yet the low level of user and managerial awareness on information security threats. In this research, we study this dissonance by addressing a cognitive bias, optimistic bias, that is, the tendency of people to believe that negative events are less likely to happen to them than to others and that positive events are more likely to happen to them than others.

Using a survey, we find that users demonstrate optimistic bias in their risk perceptions associated with information security. This self-serving bias is also found to be related to a perception of controllability with information security threats. These results have practical implications for designing security awareness programs by suggesting that risk communication and management efforts are likely to fail unless they consider this bias.

Keywords: Information security, awareness, optimistic bias, risk perception, perceived controllability, risk management

Introduction

The business environment continues to change with increasing use of the Internet. This greater connectivity has increased the vulnerability of information systems to various security threats. Several surveys have indicated that the challenges associated with information security are far from resolved. These surveys and other studies in information security repeatedly report that a lack of user and manager awareness is the number one obstacle to achieving a good information security posture (AOL/NCSA 2004; DTI 2004; Brancheau et al. 1996; GAO 1998; Goodhue and Straub 1991; Neiderman et al. 1991; Siponen 2001; Straub and Welke 1998).

Awareness of information security is the vigilance in understanding various information security threats and in perceiving one's vulnerability related to these threats. However, an understanding of threats alone seems insufficient to motivate users to take necessary action. For example, as a driver of a car, we know that there are different kinds of collisions in which one might be involved. A smoker knows that smoking is related to lung cancer. However, what really motivates one to take a precautionary and/or preventive action (e.g., wearing a seat belt or quitting smoking) is the awareness of personal risk of being involved in such a negative event. Similarly, in order for users to understand the need for information system safeguards and to exercise necessary security practices, they must perceive their own vulnerability associated with their information systems.

This difference between knowing a threat and acting on the threat is evidenced in one of the major information security surveys. According to the report of a current major information security survey (Ernst & Young 2004), managers who participated in the survey identify "lack of security awareness by user" as the top barrier to effective information security. Ironically, however, only 28 percent of these managers list "raising user information security awareness and providing training" as being a top initiative. It seems that the participating managers realize that the low level of the users' awareness as a serious problem, but do not perceive that the vulnerability related to this issue is at a sufficient level that they are motivated to take the necessary action.

People are in general responsive to actual risks imposed on them. The problem is that what we perceive is often not reality but a distorted view, either because we do not have the proper knowledge to estimate the actual risks, or we are motivated to underestimate the risk (Schwarzer 1994, p. 162). In other words, in many negative situations, people demonstrate a tendency to believe that they are less at risk than others. This underestimation of the likelihood (or probability) of experiencing negative events is called *unrealistic optimism* or *optimistic bias* (Weinstein and Klein 1996).

This optimistic bias relates to a perception of personal invulnerability. Whether it is in an absolute sense or relative to others, it represents a defensive distortion that could undermine preventive action (Schwarzer 1994) and interfere with precautionary behavior (Helweg-Larsen and Shepperd 2001). According to the health belief model, one's own vulnerability perception, the subjective probability of becoming the victim of a disease, motivates compliance behavior with a health regimen (Becker and Rosenstock 1987). Research reveals that people who believe that their risk is less than average are less likely to use contraception (Burger and Burns 1988) and more likely to engage in high risk sex (Sheer and Cline 1994).

In the context of information security, a recent field survey conducted by AOL/NCSA (2004) supports this tendency of underestimation of one's own risk. Together with NCSA (National Cyber Security Alliance), AOL (America Online) conducted in-person interviews and technical analyses with 329 adult computer users. The study participants were questioned on various aspects of online security to assess their understanding and awareness of the issue. Following the interviews, the subjects' computers were scanned by technicians to examine their actual security protection practices including firewall settings, antivirus software, and virus infections. The study reports that people underestimate their virus infection and spyware/adware programs on their computers and overestimate the frequency of updating virus protection programs than the actual numbers found from scanning their systems. As early as 13 years ago, Loch et al. (1992) also found that the managers who participated in their study believed that external networks represent the greatest risk to their information systems. Nevertheless they exhibited a low level of concern. This lower concern of a potential security breach insensitizes users to the dangers of inadequate security practices (Goodhue and Straub 1991).

Given the relevance of risk perception and taking preventive and precautionary action, investigating if users' risk perception on information security is subject to such bias has theoretical and practical implications. Therefore, the primary purpose of this research is to examine if users have an optimistic bias in perceiving their vulnerability associated with their information systems. Next, we explicate the factors influencing the extent of the optimistic bias. Relying on social comparison theory and literature on psychology and information systems, research hypotheses are investigated through an empirical study using individual users.

The remainder of this paper is organized as follows. The following section describes the theoretical background for the study and develops the research hypotheses. The subsequent section describes the research methods. The research findings are then presented. The final section discusses the overall research findings and concludes with the theoretical and practical implications that ensue.

Theoretical Background and Research Hypotheses

Traditional measures of risk—expected probabilities of incident occurrence multiplied by disutility or seriousness of consequences—are not easily applicable in measuring risk assessment in an information security context. This is because many losses

are never discovered and others are never reported. Accordingly, few quantified data are available on the likelihood of an incident occurring or on the amount of damage that is likely to result from a particular type of incident (GAO 1998). Even if the quantified data are available for risk estimation, it is questionable whether users and managers indeed utilize such information in their risk assessment in their daily work environment. Executives participating in a study for measuring managerial perception of risk (March and Shapira 1987) argued that there was no way to translate a multidimensional phenomenon into one number and claimed that they don't quantify the risk, but have to *feel* it.

Optimistic Biases in Risk Perception

Subjective probabilities, defined as "degree of belief" (Laplace 1951), are not determined solely by cognitive factors. Motivational factors, such as defensiveness or wishful thinking and estimator preferences, are also found to affect probability assessment (Miller and Ross 1975). One of the major influential motivational factors is the desirability of an event as determined by its outcome value (Zakay 1984). For an unfavorable event, people tend to assign a lower probability. For a positive outcome event, people tend to assign a higher probability. This phenomenon has been variously referred to as *unrealistic optimism* (Weinstein 1980), *optimistic bias* (Weinstein 1989), or *self-favoring bias* (Hoorens 1996). With this systematic bias, people interpret ambiguous information or uncertain situations in a self-serving direction.

Studies on biases in risk perception have shown that most people demonstrate this optimistic bias when predicting their vulnerability to various negative events. For example, research shows a strong tendency for people to underestimate their own health risks as compared to the risks of others of the same age and sex. Such optimistic bias related to one's own health risks has been shown for a variety of health issues such as cardiac disease, AIDS, influenza, and various chronic and infectious illnesses (Hoorens and Buunk 1993; Weinstein 1987).

The presence of optimistic bias is also well documented with positive events. For instance, Cooper et al. (1988) found that 81 percent of 2,994 entrepreneurs believe that their chances of survival are greater than 70 percent and 33 percent of them believe their success is certain. The actual survival rate, however, was less than 25 percent. Buehler et al. (1994) found that people anticipate their project completion time to be shorter than the actual time. Weinstein (1980) found that the students estimate their own chances of owning their home, having a good starting salary, and living past 80 years of age as higher than their peer students.

The most direct way of assessing optimistic bias is comparing one's subjective probability with the actual figure. However in many cases, measures for actual likelihood of an event occurring in the future are not readily available (Rothman et al. 1996) and individuals have difficulty in expressing their probability in a certain number (Weinstein and Klein 1996). These problems led researchers to use a comparative likelihood (e.g., the perceived risk to self and the perceived risk to others) instead of using absolute estimates as a way to measure optimistic bias (e.g., Perloff and Fetzer 1986). The comparison target would vary depending on the research context. It is usually either a peer or an average other of similar demographic profile. This social comparison process aims at finding out whether people perceive their risk lower (higher) than the others' risks, rather than the actual risk.

A theoretical justification for comparing oneself with others to measure optimistic bias can be found in social comparison theory (Festinger 1954). According to the theory, people have a need to evaluate their standings and abilities and prefer to evaluate themselves using objective measures. However, when objective measures are unavailable, people compare themselves with other people (Wood 1989). Whereas the original conceptualization of social comparison theory postulates that the primary reason of social comparison is to make accurate self-evaluation, studies in social comparison reveal that competing motives of self enhancement prevail over the need of self-evaluation (Wayment and Taylor 1995). In his model of downward comparison, Will (1981) claims that people tend to compare themselves to others who are doing worse on the same dimension under evaluation. By doing so, people keep their self-esteem, enhance their subjective well-being, feel comparatively fortunate, less distressed, and better about their own situation.

As are health risks, information security risks are risks that individuals and firms all face. Yet information security risks are highly subjective and difficult to quantify. When people are in need of evaluating their risks related to information security, they are likely to be engaged in a social comparison process to estimate comparative likelihood of their own vulnerability. In such a case, as shown in the above studies, the motive of self-enhancement may prevail over the need for self-evaluation.

Factors Influencing Optimistic Biases

Researchers have expended considerable effort to identify factors that influence optimistic bias in risk perception. The two key factors influencing the extent of optimistic bias are perceived controllability and the nature of a comparison target.

Perceived Controllability

Perceived controllability reflects the fundamental human need for competence, which refers to the extent to which a person believes he is capable of producing desired, and preventing undesired, events (Patrick et al. 1993). Skinner (1995) made a distinction between three sets of beliefs that construct perceived controllability: *control belief*s refer to generalized expectancies about the extent to which the self can produce desired or prevent undesired events; *capacity belief*s refer to generalized expectancies about the extent to which the self possesses or has access to certain means; and *strategy belief*s refer to generalized expectancies about the extent to which certain means are sufficient conditions for the production of ends or outcomes (pp. 30-31). Harris (1996) categorized control and capacity beliefs related to personal controllability and strategy belief to general controllability. The concept of personal controllability is similar to that of perceived coping efficacy, that is self-efficacy to exercise control over potentially threatening events (Bandura et al. 1982).

Similar to risk perception, studies have also found a self-serving tendency in controllability perception. This exaggeration of perceived controllability is called illusion of control (Hoorens 1996). In everyday situations such as driving, Svenson (1981) found that 80 percent of the drivers among the study participants believe their driving ability is better than average driver. This illusion of control is also documented in the situation where the occurrence of an event is purely random. For example, Langer (1975) reported people strongly prefer lottery tickets they picked themselves as compared to randomly assigned ones. In a business domain, Larwood and Whittaker (1977) found both managers and management students rate their own managerial skills to be higher than those of their respective peers.

Many studies have found evidence that perceived controllability of a negative event is a significant predictor of optimistic bias. A meta-analysis of 21 studies examining the relationship between controllability and optimistic bias shows that controllability has a large effect (effect size $r = .49$) on risk perception (Klein and Helweg-Larsen 2002). For example, Weinstein (1980) reported that when people perceive that negative events are controllable, self probabilities are found to be significantly lower than others' probabilities. DeJoy (1989) reported that people show higher comparative optimism and less concern when they feel a greater ability to control different types of vehicle accidents. This evidence suggests that as controllability increases, so does the optimistic bias. The relationship between perceived controllability and vulnerability perception has also been studied by a group of social cognitive theorists. According to Ozer and Bandura (1990), perceived coping efficacy operates as a cognitive moderator of perceived personal vulnerability.

This evidence supports relational arguments between perceived controllability and risk perception. As perceived controllability increases, risk perception decreases and comparative optimism increases. Regarding various information security threats, if people have a general belief in the existence of means to control threats to their information systems and in their ability to access those means, then it is logical to believe that the vulnerability perception associated with various information security threats would be likely adjusted down.

Comparison Target

In addition to the perception of controllability, researchers have identified the nature of comparison target influences to the degree to which people display optimistic bias. Researchers note the possibility that social and/or psychological distance between an estimator and comparison target affect the probability estimation (Alicke et al. 1995; Zakay 1984). When subjects are asked to compare themselves with an average other, they display greater optimistic bias than when they are asked to compare themselves with a specific target, such as a friend (Harris and Middleton 1994). Researchers suggest that when a vague and abstract target is used as a comparison target, individuals tend to select inferior comparison others (Levine and Green 1984; Perloff and Fetzer 1986) and to derogate other's abilities and attributes (Will 1981). However, when a specific target is used, the tendency to see self as better than others is attenuated somewhat (Brown 1986). Familiarity and likeness of the target may prevent the distortion of one's own risk perception (Harris and Middleton 1994). This tendency of evaluating one's friends more positively and less negatively than average others also exists at the group level (Brewer 1991).

Based on the converging evidence summarized above, when people are asked to estimate vulnerability associated with their information systems, we expect people to demonstrate a tendency to see that their vulnerability with their information systems are lower than others. Since motivational factors such as wishful thinking or defensiveness are not as strong as with a distant target and mass media report negative things happening to other unknown people (Zakay 1984), it would be much easier for people inclined to portray themselves and their close associates or business partners much more positive and less negative ways than they apprise most other people.

Research Hypotheses

In this study, we first intend to examine if users demonstrate optimistic bias in their risk perceptions in an information security domain. Second, we investigate the self-serving tendencies of users' perceptions on their controllability against information security threats. Then, we explore the impact of social distance of a comparison target and relationships between the two research variables, perceived controllability and risk perception. Based on the previous discussions, we propose the following hypotheses:

Hypothesis 1: **Optimistic Bias in Risk Perception**

- H1a: Users have an optimistic bias in their vulnerability perception related to information security.
- H1b: Such optimistic bias increases as social/psychological distance with a comparison target increases.

Hypothesis 2: **Illusion of Control in Perceived Controllability**

- H2a: Users show a self-serving tendency in their perceptions of controllability related to information security.
- H2b: Such self-serving bias increases as social/psychological distance with a comparison target increases.

Hypothesis 3: **Perceived Controllability and Optimistic Bias**

H3: There is a negative relationship between perceived controllability and risk perception.

Research Methodology

Instrument

The initial set of items was created based on Straub (1990), Goodhue and Straub (1991), Skinner (1995), Armitage et al. (1999), and Ajzen (2002). Since some of these constructs are new to MIS research, we executed a rigorous validation process to ensure that all scales would accurately measure the constructs.[1] Once the item pools were created, pretest interviews were conducted. A group of MIS faculty and graduate students, a total of 32 individuals, were solicited to further demonstrate content validity and clarify the wording for each item. Subjects were allowed to set aside statements that were ambiguous. Consistent placement of items into a particular category demonstrates convergent validity with the related construct, and discriminant validity with the other constructs. Items that consistently did not match the corresponding construct or were reported to be ambiguous were deleted from the item pool. A pilot test was conducted with a group of graduate students to ensure the initial reliability of the scales and the general mechanics of the questionnaire, such as instructions, completion time, and appropriate wording. Based on the responses received from this pilot test, the questionnaire was revised. This process resulted in four items for risk perception and another four items for perceived controllability constructs. (See the appendix.)

Participants

A total of 248 students enrolled in a master's program majoring in business with a part-time or full-time job participated in this study. The mean age of participants was 28.93, and their work experience averaged 12.97 years. The average period of

[1]The discussion on the rigorous scale development process we went through is not included in this paper because of the page limit. It is available upon request.

information system usage was 8.88 years. Sixty-three percent of the subjects were men. Their participation was voluntary and the survey instrument was distributed during classes. Anonymity was stressed.

Measures

Comparative likelihood can be measured either directly or indirectly. Direct comparison involves a single estimate of an individual for the likelihood of experiencing an event relative to a target's likelihood of the same event. Indirect comparison involves two estimates. One is self-likelihood of and the other is target's likelihood of an event occurring in the future. The direct method tends to produce greater bias than the indirect method and fewer choices on the scale results in greater bias than more choices on the scale (Klein and Helweg-Larsen 2002).

The underlying assumption of this comparative approach is that for a negative event, a significant tendency for the sample self-rating to be lower than the comparison group mean indicates an optimistic bias (Harris 1996). This is because it is unrealistic for most people to be better than their friends or average other person. Therefore, if enough people in a given group perceive that their likelihood of getting a negative event is significantly lower that those of others, we can claim that at least a proportion of the people in the group are unrealistically optimistic (Harris and Middleton 1994). Thus, it is important to note that optimistic bias is usually measured on a group basis, not on an individual level.

In this study, we used an indirect method. Since it tends to produce smaller bias (therefore, more conservative) than a direct method. In addition, it allows us to determine whether perception on controllability influences optimistic bias via self risk perception or target risk perception. Each participant received a booklet containing items that measure risk perception and perceived controllability pertaining to information security. The participants rate their perceptions on risk related to their information system and their controllability. The same sets of questions were repeated to measure the participants' perceptions related to their friends' and average other person's information systems. We specified "a friend" as someone who has some degree of electronic interaction such as sending and receiving e-mail and/or file sharing activity. An average other person refers to a person who falls in the same demographic classification as the subject but with no direct interaction with them. Questions to measure demographic variables are also included in the questionnaire. The responses to items for risk perception range from 1 (very low) to 7 (very high) and those for controllability range from 1 (strongly disagree) to 7 (strongly agree). The mean difference between the estimations for the comparison target and for oneself was taken as a measure of optimistic bias and illusion of control.

Analysis and Findings

Measurement Model

An exploratory factor analysis (EFA) was conducted to identify the factor structure of perceived controllability and risk perception items. The correlation matrix of the 24 items (see Table 1) was factor analyzed using the maximum likelihood method. An oblique rotation method (Quartimin with Kaiser normalization) was applied to determine the factor loadings since the factors are assumed to be correlated. Based on the scree test and interpretability of the rotated factor loading matrix, the six-factor model seems most reasonable.

As presented in Table 1, each of the six factors has high loadings on four items (range: 0.548 to 0.966) that are designed to measure the factor and low loadings on the other items (range: 0.001 to 0.242). These results suggest that the 24 items are reliable indicators of the 6 distinct constructs. Thus discriminant validity was observed. The internal consistency reliabilities (Cronbach alpha) for the six factors are between 0.899 and 0.963 (see Tables 2 and 3). The factor loading pattern and high reliabilities allowed convergent validity.

As shown in Table 4, the correlations among the three risk perception factors are high (0.509, 0.372, and 0.467) as well as those among the three controllability factors (0.393, 0.281, and 0.429). Correlations between the three risk perception factors and the three controllability factors are relatively low. This result suggests that the risk perception factors are discriminated from the controllability factors. However, the negative correlations between perception and controllability were also observed (–0.330 self; –0.355 friend's; –0.153 average other's). These negative correlations were predicted by Hypothesis 3, which will be analyzed more specifically by using structural equation modeling in the following section.

Table 1. Factor Loadings of 24 Items from Exploratory Factor Analysis (EFA)

	Risk–Self	Risk–Friend	Risk–Other	Control–Self	Control–Friend	Control–Other
V10	0.548	0.242	0.022	–0.093	0.003	0.057
V11	0.791	0.149	0.008	–0.069	0.111	–0.077
V12	0.966	–0.030	0.047	0.038	–0.030	–0.026
V13	0.953	–0.097	–0.019	0.022	–0.052	0.021
V14	0.008	–0.002	–0.031	0.868	–0.001	–0.065
V15	–0.021	0.060	–0.001	0.909	–0.071	0.036
V16	–0.012	–0.078	0.067	0.731	0.074	0.006
V17	0.013	0.049	–0.009	0.771	0.050	0.074
V18	0.038	0.829	0.076	–0.017	0.023	0.000
V19	0.003	0.924	0.048	0.009	–0.001	–0.014
V20	0.020	0.945	–0.003	0.030	–0.031	–0.020
V21	0.012	0.904	–0.008	0.018	–0.066	0.028
V22	–0.031	0.072	–0.069	0.080	0.853	–0.031
V23	–0.039	0.016	–0.004	–0.013	0.940	–0.017
V24	0.014	–0.045	0.010	0.012	0.801	0.018
V25	0.064	–0.137	0.073	–0.035	0.781	0.126
V26	0.045	–0.020	0.885	–0.004	–0.062	0.073
V27	–0.015	0.060	0.912	–0.040	0.010	–0.008
V28	–0.005	0.035	0.945	–0.002	0.034	–0.026
V29	–0.018	–0.012	0.907	0.060	0.013	–0.070
V30	0.007	–0.067	0.053	0.030	0.025	0.848
V31	0.009	0.034	–0.001	0.027	–0.002	0.897
V32	–0.036	0.016	–0.032	–0.026	0.037	0.898
V33	–0.004	0.023	–0.046	0.002	–0.018	0.939

Table 2. Factor Loadings of Risk Perception Factors and Reliability Coefficients (CFA)

Factor	Item	Loading
Risk – Self	10	0.796
(Cronbach alpha = 0.920)	11	0.890
	12	0.932
	13	0.875
Risk – Friend	18	0.899
(Cronbach alpha = 0.963)	19	0.947
	20	0.955
	21	0.935
Risk – Average Other Person	26	0.887
(Cronbach alpha = 0.957)	27	0.933
	28	0.963
	29	0.923

Table 3. Factor Loadings of Controllability Factors and Reliability Coefficients (CFA)

Factor	Item	Loading
My controllability	14	0.811
(Cronbach alpha = 0.899)	15	0.860
	16	0.802
	17	0.814
Friend's controllability	22	0.845
(Cronbach alpha = 0.923)	23	0.892
	24	0.859
	25	0.869
Average Other Person's controllability	30	0.897
(Cronbach alpha = 0.947)	31	0.893
	32	0.892
	33	0.880

Table 4. Correlations Among the Six Factors (EFA)

	Self–Perception	Friend–Perception	Other–Perception	Self–Control	Friend–Control	Other–Control
Self–Perception	1.000	0.509	0.372	–0.330	–0.073	–0.046
Friend–Perception		1.000	0.467	0.018	–0.355	–0.111
Other–Perception			1.000	0.117	0.011	–0.153
Self–Control				1.000	0.393	0.281
Friend–Control					1.000	0.429
Other–Control						1.000

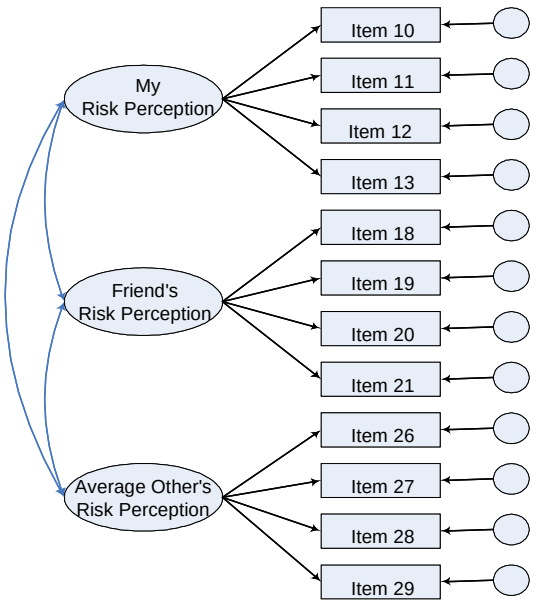

Figure 1. Confirmatory Factor Analysis Model for Risk Perception

Optimistic Bias in Risk Perception

Using AMOS 4.0 software, we first tested the existence of comparative optimism in risk perception in the domain of information security. The path diagram is presented in Figure 1, which is a confirmatory factor analysis (CFA) with mean structure. The fit indices suggest that the model fits the data well (χ^2 = 341.709, *df* = 60, *p* = 000; NFI = .969; NNFI = .966; CFI = 0.974; RMSEA = .138[2]). All of the factor loadings are very high (see Table 2), and correlations among the three factor scores are also high (see Table 5). The mean factor scores of risk perception for my system, for a friend's system, and an average other's system are 3.875, 4.270, and 4.849, respectively (see Figure 2). The mean factor score of risk perception of my system is significantly lower than that of risk perception of my friend's system ($\chi^2_{diff}(1) = 14.048$, $p = .000$) and that of risk perception of an average other's system ($\chi^2_{diff}(1) = 70.924$, $p = .000$). These results support Hypothesis 1a. The extent of the difference on risk perception between my system and the average other's system is significantly higher than that of my system and my friend's ($\chi^2_{diff}(1) = 39.802$, $p = .000$). Therefore, Hypothesis 1b is supported.

Table 5. Correlation Among the Three Risk Perception Factors (CFA)

	Self	Friend	Average
Self	1.000	0.561	0.435
Friend		1.000	0.513
Average			1.000

Table 6. Correlation Among Three Controllability Factors (CFA)

	Self	Friend	Average
Self	1.000	0.415	0.300
Friend		1.000	0.454
Average			1.000

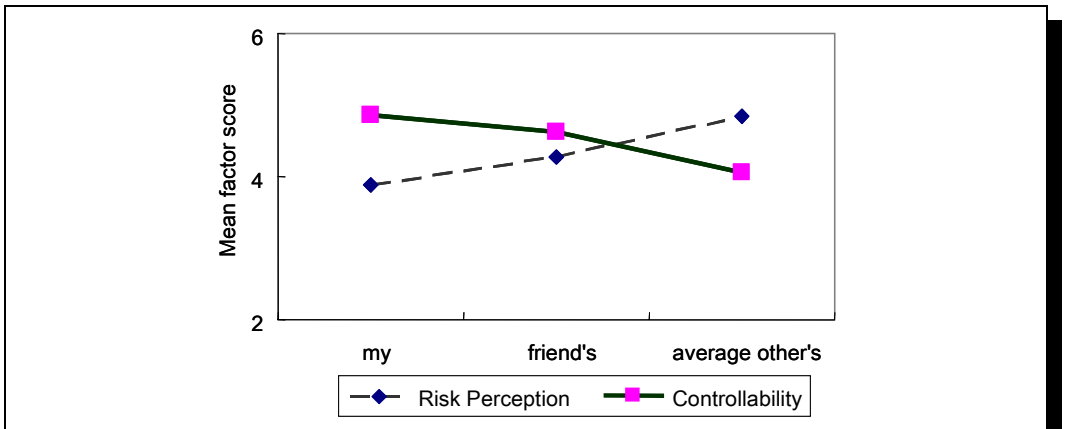

Figure 2. Factor Means of Risk and Controllability Perception

[2]RMSEA is higher than reasonable fit criterion (0.08). As Steiger (2002), who invented RMSEA, pointed out, as implied correlations are higher, RMSEA tends to be bigger. He also recommended that the cut-off value (such as 0.08) should not be treated too seriously. The data set used here contains high correlations and factor loadings are also very high. Based on Browne et al. (2002) and Steiger (2002), this study relies more on other fit indices.

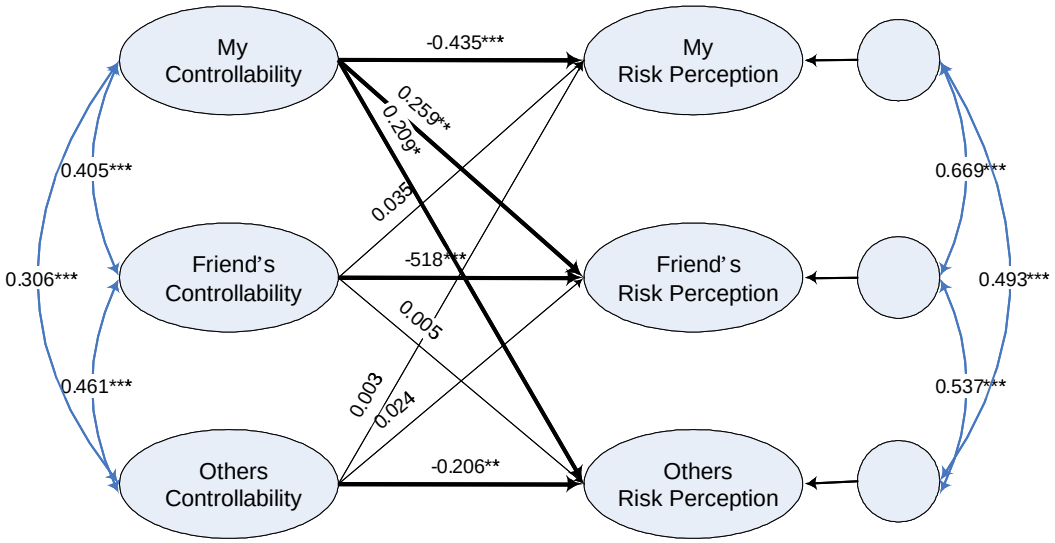

Figure 3. Path Diagram for Relationship Between Perceived Controllability and Risk Perception (The thick lines represent statistically significant coefficients)

Self-Serving Bias in Perceived Controllability

A confirmatory factor analysis with mean structure was conducted to test the existence of a self-serving bias in the perception of controllability. The same form of path diagram as in Figure 1 is applied. The fit indices of the model suggest that the model fits the data well (χ^2 = 362.373 *df* = 60, *p* = 000; NFI = .964; NNFI = .961; CFI = 0.970; RMSEA = .143). All factor loadings are very high (see Table 3), and correlations among the three factor scores are also high (see Table 6). The mean factor scores for controllability for self, friend's, and averages other's are 4.858, 4.624, and 4.066, respectively (see Figure 2). The mean factor score of my controllability is significantly higher than that of my friend's controllability ($\chi^2_{diff}(1) = 5.540,\ p = .019$) and average other's controllability ($\chi^2_{diff}(1) = 52.694,\ p = .000$). These results support Hypothesis 2a. The extent of the difference between my controllability and average other's controllability is significantly higher than that between my controllability and my friend's controllability ($\chi^2_{diff}(1) = 30.825,\ p = .000$). Thus, the result is consistent with Hypothesis 2b.

Relationship between Perceived Controllability and Optimistic Bias

To investigate the relationship between perceived controllability and optimistic bias, a structural equation model is constructed (see Figure 3).[3] The fit indices of the model suggest that the model fits the data well (χ^2 = 795.894 *df* = 255, *p* = 000; NFI = .959; NNFI = .967; CFI = 0.972; RMSEA = .098). The SEM analyses showed that all three controllability (self/friend's/average other's) had a negative influence on its risk perception (β = –0.435, *p* < .001; β = –0.518, *p* < .001; β = –0.206, *p* < .001). These results support Hypothesis 3. Interestingly, while my controllability perception had a negative influence on my risk perception, it had positive influences on risk perception for friend's system (β = 0.259, *p* < .001) and average other's system (βb = 0.209, *p* < .001). These results indicate that users with greater perceived controllability tend to perceive their own risk lower but other's risk higher.

[3]The high correlations among the three controllability factors and among the residuals of the three risk factors are because of the nature of measurement. Since the same sets of items were used to measure self, friend's, and other's controllability and risk, high correlations are predicted.

Discussions and Concluding Remarks

This research was motivated by a dissonance observed in the information security domain: understanding of information security threats but low regard in addressing the issue. We attempt to explain this gap by examining if users demonstrate optimistic bias in their risk perception on information security. For all of the four questions that we used to measure vulnerability perception, participants perceive that their risk is significantly lower than that of the two comparison targets, friend and average other person. This optimistic bias was more evident as social and psychological distance increases (i.e., more with average other person than with friend). Such a self-serving tendency of interpreting their situation is also observed in their controllability perception. For the questions that measure perceived controllability of information security, significant comparative optimism was observed. Similar to risk perception, the extent of a self-serving tendency was more severe with average other person than with friend.

These results show that relative to their friend and average other person, they feel less vulnerable to information security threats and that they have more control to protect their information system. It indicates that users' optimism in the domain of information security seems double-sided in nature: defensive as well as functional. Defensive optimism is related to a naïve optimism which indicates such misfortune will not happen to me. Functional optimism is related to personal resources and ability to exercise a course of action (Schwarzer 1994).

Our study has significant implications for practitioners. Perceptions, whether accurate and rational or not, are themselves important factors of managing the realities of risk (Baron et al. 2000). As evidenced in the numerous studies that tested the contention of strong attitude (belief) and subsequent behavior relations, a person's attitude (belief) toward an object influences the overall pattern of his responses to the object (Ajzen and Fishbein 1977). Thus we may argue that this unrealistic optimism observed in the domain of information security may lead people to ignore the measures and practices to offset information security threats.

The importance of ongoing security training and awareness programs has been raised in many information security studies (Dhillon and Backhouse 2001; Dutta and Roy 2003; Hone and Eloff 2002; Mitnick 2003; Nosworthy 2000). However, risk communication and management efforts are likely to fail unless they carefully devise ways of eliminating these biases. Since an optimistic bias is not so much that individuals believe that negative events will not happen but rather that these events are relatively unlikely to happen to them (McKenna 1993), people may consider that the risk communication and security practices are directed at other people who are more vulnerable than themselves. Considering the dependency of today's organizations on information systems, a call for increased awareness of information security issues is even more critical. Given that a human is the first and utmost defense line of information security, an awareness program based on understanding the unique characteristics of human perception would be far more effective.

References

Alicke, M. D., Klotz, M. L., Breitenbecher, D. L., Yurak, T. J., and Vredenburg, D. S. "Personal Contact, Individuation, and the Better-than-Average Effect," *Journal of Personality and Social Psychology* (68), 1995, pp. 804–825.

Ajzen, I. "Construction of a Standard Questionnaire for The Theory of Planned Behavior," 2002 (available online at **http://www-unix.oit.umass.edu/~aizen/**).

Ajzen, I. and Fishbein, M. "Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research," *Psychological Bulletin* (84), 1977, pp. 888–918.

AOL/NCSA. "AOL/NCSA Online Safety Study," Research Report, American Online and the National Cyber Security Alliance, October 2004 (available online at **http://www.staysafeonline.info/pdf/safety_study_v04.pdf**).

Armitage, C. J., Conner, M., Loach, J., and Willerts, D. "Different Perceptions of Control: Applying an Extended Theory of Planned Behavior to Legal and Illegal Drug Use," *Basic and Applied Social Psychology* (21), 1999, pp. 301-316.

Bandura, A., Reese, L., and Adams, N. E. "Microanalysis and Fear Arousal as a Function of Differential Levels of Perceived Self-Efficacy," *Journal of Personality and Social Psychology* (43), 1982, pp. 5-21.

Baron, J., Hershey, J. C., and Kunreuther, H. "Determinants of Priority for Risk Reduction: The Role of Worry," *Risk Analysis* (20), 2000, pp. 413-427.

Becker, M. H., and Rosenstock, I. M. "Comparing Social Learning Theory and the Health Belief Model," *Advances in Health Education and Promotion*, (2), 1987, pp. 245-249.

Brancheau, J. C., Janz, B. D., and Wetherbe, J. C. "Key Issues in Information Systems Management: 1994-95 SIM Delphi Results," *MIS Quarterly* (20:2), 1996, pp. 225-242.

Brewer, M. B. "The Social Self: On Being the Same and Different at The Same Time," *Personality and Social Psychology Bulletin* (17), 1991, pp. 475-482.
Brown, J. D. "Evaluations of Self and Others: Self Enhancement Biases in Social Judgments," *Social Cognition* (4), 1986, pp. 353-376.
Browne, M. W., MacCallum, R. C., Kim, C., Anderson, B. L., and Glaser, R. "When Fit Indices and Residuals are Incompatible," *Psychological Methods* (7), 2002, pp. 403-421.
Buehler, R., Griffin, D., and Ross, M. "Exploring the 'Planning Fallacy': Why People Underestimate Their Task Completion Time," *Journal of Personality and Social Psychology* (67), 1994, pp. 366-381.
Burger, J. M., and Burns, L. "The Illusion of Unique Invulnerability and the Use of Effective Contraception," *Personality and Social Psychological Bulletin* (14), 1988, pp. 264-270.
Cooper, A. C., Woo, C. Y., and Dunkelberg, W. C. "Entrepreneurs' Perceived Chances for Success," *Journal of Business Venturing* (3), 1988, pp. 97-108.
DeJoy, D. M. "The Optimistic Bias and Traffic Accident Perception," *Accident Analysis and Prevention* (21), 1989, pp. 333-340.
Dhillon, G., and Backhouse, J. "Current Directions in IS Security Research: Toward Socio-Organizational Perspectives," *Information Systems Journal* (11), 2001, pp. 127-153.
DTI. "Information Security Breaches Survey 2004," Technical Report, the British Department of Trade and Industry, 2004 (available online at **http://www.infosec.co.uk/files/DTI_Survey_Report.pdf**).
Dutta, A., and Roy, R. "The Dynamics of Organizational Information Security," in *Proceedings of the 24th International Conference on Information Systems*, S. T. March, A. Massey, and J. I. DeGross (Eds.), Seattle, WA, 2003, pp. 921-927.
Ernst & Young. "Global Information Security Survey," White Paper, Ernst & Young, 2004.
Festinger, L. "A Theory of Social Comparison Process," *Human Relations* (7), 1954, pp. 117-140.
GAO. "Information Security Management: Learning from Leading Organization," Report GAO/AIMD-98-68, United States General Accounting Office, Washington, DC, 1998 (available online at **http:www.gao.gov/special.pubs/ai9868.pdf**).
Goodhue, D. L., and Straub, D. W. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management* (20), 1991, pp. 13-27.
Harris, P. "Sufficient Grounds for Optimism? The Relationship between Perceived Controllability and Optimistic Bias," *Journal of Social and Clinical Psychology* (15), 1996, pp. 9-52.
Harris, P., and Middleton, W. "The Illusion of Control and Optimism about Health On Being Less at Risk but No More in Control than Others," *British Journal of Social Psychology* (33), 1994, pp. 319-386.
Helweg-Larsen, M., and Shepperd, J. A. "Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A Review of the Literature," *Personality and Social Psychology Review* (5), 2001, pp. 74-95.
Hone, K., and Eloff, J. H. P. "Information Security Policy: What do International Security Standards Say," *Computers and Security* (21), 2002, pp. 402-409.
Hoorens, V. "Self-Favoring Biases for Positive and Negative Characteristics: Independent Phenomena?," *Journal of Social and Clinical Psychology* (15), 1996, pp. 53-67.
Hoorens, V., and Buunk, B. P. "Social Comparison of Health Risks: Locus of Control, the Person-Positivity Bias, and Unrealistic Optimism," *Journal of Applied Social Psychology* (23), 1993, pp. 291-302.
Klein, C. T. F., and Helweg-Larsen, M. "Perceived Controllability and the Optimistic Bias: A Meta-Analytic Review," *Psychology and Health* (17), 2002, pp. 437-466.
Langer, E. J. "The Illusion of Control," *Journal of Personality and Social Psychology* (32), 1975, pp. 311-328.
Laplace, P. S. *A Philosophical Essay on Probabilities*, Dover, New York, 1951.
Larwood, L., and Whittaker, W. "Managerial Myopia: Self-serving Biases in Organizational Planning," *Journal of Applied Psychology* (62), 1977, pp. 194-198.
Levine, J. M., and Green, S. M. "Acquisition of Relative Performance Information: The Roles of Intrapersonal and Interpersonal Comparison," *Personality and Social Psychology Bulletin* (10), 1984, pp. 385-393.
Loch, K. D., Carr, H. H., and Warkentin, M. E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16), 1992, pp. 173-186.
March, J. G., and Shapira, Z. "Managerial Perspectives on Risk and Risk Taking," *Management Science* (33), 1987, pp. 1404-1418.
McKenna, F. P. "It Won't Happen to Me: Unrealistic Optimism or Illusion of Control?," *British Journal of Psychology* (84),1993, pp. 39-50.
Miller, D. T., and Ross, M. "Self-serving Biases in Attribution of Causality: Fact or Fiction?," *Psychological Bulletin* (82), 1975, pp. 213-225.
Mitnick, K. "Best Practice: Are You the Weak Link?," *Harvard Business Review* (81), 2003, pp. 18-20.
Niederman, F., Brancheau, J. C., Wetherbe, J. C. "Information Systems Management Issues for the 1990s," *MIS Quarterly* (15:4), 1991, pp. 475-500.

Nosworthy, J. D. "Implementing Information Security in the 21st Century: Do you have the Balancing Factors?," *Computers and Security* (19), 2000, pp. 337-347.

Ozer, E. M., and Bandura, A. "Mechanisms Governing Empowerment Effects: A Self-Efficacy Analysis," *Journal of Personality and Social Psychology* (58), 1990, pp. 472-486.

Patrick, B. C., Skinner, E. A., and Connell, J. P. "What Motivates Children's Behavior and Emotion? The Joint Effects of Perceived Control and Autonomy in the Academic Domain," *Journal of Personality and Social Psychology* (65), 1993, pp. 781-791.

Perloff, L. S., and Fetzer, B. K. "Self-Other Judgments and Perceived Vulnerability to Victimization," *Journal of Personality and Social Psychology* (50), 1986, pp. 502-510.

Rothman, A. J., Klein, W. M., and Weinstein, N. D. "Absolute and Relative Biases in Estimations of Personal Risk," *Journal of Applied Social Psychology*, (26), 1996, pp. 1213-1236.

Schwarzer, R. "Optimism, Vulnerability, and Self-Beliefs as Health-Related Cognitions: A Systematic Overview," *Psychology and Health*, (9), 1994, pp. 161-180.

Sheer, V. C., and Cline, R. J. "The Development and Validation of a Model Explaining Sexual Behavior among College Students: Implications for AIDS Communication Campaign," *Human Communication Research* (21), 1994, pp. 280-304.

Siponen, M. T. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management and Computer Security* (8), 2000, pp. 31-41.

Skinner, E. A. *Perceived Control, Motivation, and Coping*, Sage Publications, Thousand Oaks, CA, 1995.

Steiger, J. H. "Point Estimation, Hypothesis Testing, and Interval Estimation Using the RMSEA: Some Comments and a Reply to Hayduk and Glaser," *Structural Equation Modeling: A Multidisciplinary Journal* (7), 2002, pp. 149-162.

Straub, D. W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1), 1990, pp. 255-276.

Straub, D. W., and Welke, R. J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), 1998, pp. 441-469.

Svenson, O. "Are We All Less at Risk and More Skillful than Our Fellow Drivers?," *Acta Psychologica* (47), 1981, pp. 143-148.

Wayment, H. A., and Taylor, S. E. "Self Evaluation Processes: Motives, Information Use, and Self-Esteem," *Journal of Personality* (63), 1995, pp. 329-357.

Weinstein, N. D. "Effects of Personal Experience on Self-Protective Behavior," *Psychological Bulletin* (105), 1989, pp. 31-50.

Weinstein, N. D. "Unrealistic Optimism about Future Life Events," *Journal of Personality and Social Psychology* (39), 1980, pp. 806-820.

Weinstein, N. D. "Unrealistic Optimism about Susceptibility to Health Problems: Conclusions from a Community-Wide Sample," *Journal of Behavioral Medicine* (10), 1987, pp. 481-500.

Weinstein, N. D., and Klein, W. M. "Unrealistic Optimism: Present and Future," *Journal of Social and Clinical Psychology* (15), 1996, pp. 1-8.

Will, T. A. "Downward Comparison Principles in Social Psychology," *Psychological Bulletin* (90), 1981, pp. 245-271.

Wood, J. V. "Theory and Research Concerning Social Comparisons of Personal Attributes," *Psychological Bulletin* (106), 1989, pp. 231-248.

Zakay, D. "The Influence of a Perceived Event's Controllability on Its Subjective Occurrence Probability," *The Psychological Record* (34), 1984, pp. 233-240.

Appendix: Items Used to Measure Risk Perception and Controllability on Information Security

	Very Low	Low	Somewhat Low	Average	Somewhat High	High	Very High
The risk from information security threats to **my system** is	☐	☐	☐	☐	☐	☐	☐
The likelihood that **my system** is disrupted due to information security breaches in the next 12 months is	☐	☐	☐	☐	☐	☐	☐
The chance that **my system** will fall a victim to an information security breach is	☐	☐	☐	☐	☐	☐	☐
The vulnerability of **my system** to information security threats is	☐	☐	☐	☐	☐	☐	☐

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
I have the means to control information security threats.	☐	☐	☐	☐	☐	☐	☐
I have the ability to execute security practices to avoid information security threats.	☐	☐	☐	☐	☐	☐	☐
I have access to necessary resources (such as software, person to get help) to protect my information system.	☐	☐	☐	☐	☐	☐	☐
I can exercise a course of action to avoid an information security breach.	☐	☐	☐	☐	☐	☐	☐