2009

AN INVESTIGATION OF DECISION-MAKING AND THE TRADEOFFS INVOLVING COMPUTER SECURITY RISK

Li-Chiou Chen
Pace University - New York, lchen@pace.edu

Daniel Farkas
Pace University - New York, dfarkas@pace.edu

AN INVESTIGATION OF DECISION-MAKING AND THE TRADEOFFS INVOLVING COMPUTER SECURITY RISK

Li-Chiou Chen
Pace University
lchen@pace.edu

Daniel Farkas
Pace University
dfarkas@pace.edu

ABSTRACT

Individual decision making in computer security risk plays a critical role in successful information security management. This paper describes a study that investigated how individuals make tradeoffs regarding computer security risk. The study asked subjects to make decisions on two hypothetical scenarios in which subjects were asked to choose between avoiding computer security risk and accepting a reward. We found that individual computer security risk perception, culture and security skills have an impact on their decisions regarding trading off computer security with rewards.

Keywords

Computer security risk, risk perception, risk attitude, risk tradeoff, time discounting.

INTRODUCTION

Security policies and education are often adopted in organizations to manage computer security risk (Stoneburner, Goguen, and Feringa, 2002). However, the success of these efforts largely depends on the individuals involved. An individual decision might have a big impact on the information security of the entire organization. For example, an employee might write down the password of an important account and leave it close to the desk for convenience. Unknown malware downloaded from the Internet can also find its way into an organization's network via employees' laptops, emails, or portable data drives. Individual decision making involving computer security risk thus plays a critical role in successful information security management. Understanding how people make security related decisions will enable engineers to build better security systems and facilitate managers to design better security policies and educational programs. The paper focuses on studying how individuals make tradeoffs involving computer security risk.

We conducted an empirical study on the tradeoff between computer security risk and monetary reward. Our study was built upon theories from individual decision making and empirical evidence from previous e-commerce research. Although researchers have tried to design software with better security usability (Cranor and Garfinkel, 2005), computer security still often involves the tradeoff between security risk and convenience, functionality, or monetary reward. Our study presented the subjects with two hypothetical scenarios in which they had to choose between a monetary reward and avoiding an implicit computer security risk. We investigated the factors that may have an impact on their decision-making, such as individual differences, computer security knowledge and computer experience. Our results provide insight and implications for managing computer security risk.

The next section will provide a conceptual framework of computer security risk tradeoffs grounded by theories from individual decision making and evidence from other security risk related literature. Section 3 will describe our empirical study. Section 4 will analyze the results from the study. Section 5 discusses the results and their implications followed by conclusions.

A CONCEPTUAL FRAMEWORK OF COMPUTER SECURITY RISK TRADEOFFS

Previous research has provided some empirical evidence on how end users perceive online security risk (Bhatnagar, Misra, and Rao,2000; Miyazaki and Fernadez, 2001). However, little research has been done in providing a theoretical foundation or empirical evidence in how individuals make decisions involving computer security risk tradeoffs. To bridge this gap, we propose a conceptual framework of individual risk tradeoffs between rewards and computer security, as shown in Figure 1. The framework is grounded by theories and evidence from individual decision making. Using this framework, we studied three research problems in computer security risk tradeoffs. 1) How do individuals make decisions involving monetary rewards? 2) Does individual risk perception towards computer security have an impact on their decisions in the tradeoffs? 3) What is the impact of individual differences, computer security knowledge and computer experience on the tradeoffs? This

framework hypothesizes the factors that may have an impact on risk perception and attitude towards computer security risks (Chen and Farkas, 2009) and the factors that may have an impact on specific computer security risk tradeoffs, such as tradeoffs between the risk and monetary rewards. In our study , we empirically examined four sets of hypotheses (H1, H2, H3, and H4) that describe the relationships between the dependent variables - individual computer security risk tradeoffs, and the independent variables - risk perception and attitude, individual differences, computer security knowledge and computer experience.

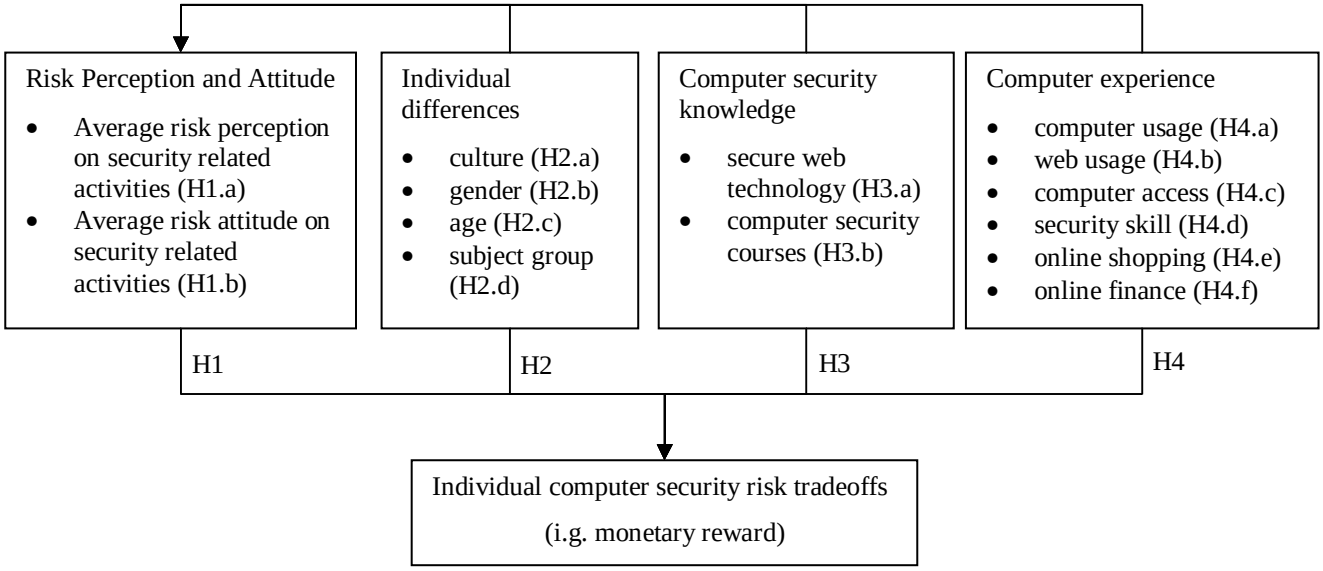

Figure 1. A conceptual framework of individual risk tradeoffs between rewards and computer security

Risk Perception, Risk Attitude, and Risk Tradeoffs

Hypothesis H1: Individuals who have a higher average risk perception of computer security related activities tend to reject rewards and avoid computer security risks (H1.a) and individuals who have a higher average risk attitude towards computer security related activities tend to accept rewards and therefore take computer security risks (H1.b).

Risk perception refers to an individual's judgment of how risky a certain event is. Understanding how humans perceive the exposure and the effects of risk is considered an important part of analyzing and managing technology-induced risk (Morgan, 1981). However, risk perception of computer security has yet to be fully studied although the general perception of risk has been found to greatly impact individual computer decisions (Hardee, West, and Mayhorn, 2006).

Risk attitude refers to an individual's decisions or preferences of risk-related choices. This topic has drawn abundant research in the field of individual decision making. Prospect theory (Kahneman and Tversky, 1979) has been the most cited theory in this field since it can explain the empirical evidence that violates assumptions in the classical expected utility theory (Friedman and Savage, 1948; Machina, 1990) in Economics where an individual's risk attitude is a function of risk preference, outcomes, and the probability of occurrence. Prospect theory explains that people tend to overweigh outcomes that are considered certain in comparison to outcomes that are merely probable (Tversky and Kahneman, 1981). Prospect theory has been proposed to explain how individuals make decisions when facing security tradeoffs (West, 2008) but no empirical studies have been done at this point. It is unclear if people behave the same way in computer security risk tradeoffs compared to economic tradeoffs. In the context of computer security, this theory implies that people will prefer smaller security gain over a chance of larger reward and will prefer a chance of larger security loss over a small loss. For example, users might choose to risk the possibility of virus infection rather than spend $200 on anti-virus software.

Other psychological heuristics and biases may also have impacted on individual decisions on security related tradeoffs. In particular, one of our scenarios investigated tradeoffs involving inter-temporal choices since many computer security decisions involving a time factor. For example, when a user downloads free software from the Internet, the tradeoff would be enjoying the immediate convenience or facing potential security risk in the future. Time discounting research (Loewenstein, 1992; Loewenstein and Prelec, 1992) has found that when the outcomes of a decision occur at different times, people tend to discount future outcomes. In addition, people prefer immediate gain to future gain and prefer future loss to immediate loss.

Individual Differences, Computer Security Knowledge and Computer Experience

Hypothesis H2: Both culture (H2.a) and gender (H2.b) have an impact on an individual's computer security risk decisions. Younger students are more likely to tradeoff computer security risk with rewards (H2.c) and so do undergraduate students (H2.d).

Hypothesis H3: Individuals who know more about secure web technology (H3.a) and who are more educated in computer security subjects (H3.b) are less likely to tradeoff computer security risk with rewards.

Hypothesis H4: Individuals who are more computer savvy are less likely to tradeoff computer security risk with reward. This includes individuals who use computers more frequently (H4.a), who browse the web more frequently (H4.b), who have computer access both at work and at home (H4.c), who have more security skills (H4.d), who have had online shopping experiences (H4.e) and who have conducted online financial transactions (H4.f).

Research in e-commerce has provided empirical evidence on how end users perceive online security risk. The technological risks of using the Internet are considered a factor when consumers make Internet shopping decisions (Bhatnagar, Misra, and Rao,2000). Greater Internet experience and the use of other remote purchasing methods have been found to be related to lower levels of perceived risk toward online shopping (Miyazaki and Fernadez, 2001). One study found that the lack of specific knowledge of web site authentication makes users vulnerable to attacks (Dhamija, Tygar, and Hearst, 2006). The mental model approach (Norman, 1983) has been used in risk communication to understand an individual's reasoning of specific risk in areas such as environmental (Morgon, Fischhoff, Bostrom, and Atman, 2001), data privacy (Diesner, Kumaraguru, and Carley, 2005) and computer security (Asgharpour, Liu, and Camp, 2007; Liu, Asgharpour, and Camp, 2007). Using a card sorting game, researchers have found that mental models of computer security risk strongly correlate to an individual's expertise in security (Asgharpour et al., 2007). Research has also shown that risk perception is different in different domains (Weber, Blais and Betz, 2002) and in different cultures (Weber and Hsee, 1998).

Studies have shown that the lack of correct information about privacy technology is one of the reasons people ignore online privacy (Acquisti and Grossklags, 2005). In addition, various empirical studies (Dhamija et al., 2006; Downs, Holbrook and Cranor, 2007) on phishing have shown that users lack the specific knowledge necessary to distinguish genuine web sites from fake ones. Incomplete information or lack of specific security knowledge could be the factors hindering judgment when making secure decisions. An individual's experience with technology and computer security may also play a role in providing one with the information used in making judgments on decisions regarding computer security risk.

AN EMPIRICAL STUDY

We conducted a web-based survey from May to June 2008. In the survey, we asked subjects to rate 7 computer security activities, listed in Appendix A, using a five-point Likert scale. For each activity, the subjects were asked to express how likely they were to engage in this activity to elicit risk attitude and how risky they perceived this activity to elicit risk perception. All 7 activities describe situations when subjects have to take some computer security risk in order to gain a certain benefit, such as reading news online, obtaining free software, etc.

Subjects were asked to make decisions on two hypothetical scenarios, listed in Appendix B. The scenarios were about shopping online for a digital camera. In the first scenario, we investigated tradeoffs regarding monetary rewards. The subjects were asked to choose between accepting reward and rejecting reward. Accepting a reward refers to paying less for a digital camera with some uncertain security risk by accepting an unknown web script. Rejecting a reward refers to paying more for the same digital camera with no security risk. We did not explicitly identify the security risk in the scenario. When the subjects decided to accept reward, they were asked to select a level of reward from $10 cheaper to $50 cheaper than the $200 original price for the camera. In the second scenario, we investigated risk tradeoffs regarding a time delay as reward. The subjects were asked to choose between a "delay" reward and an "immediate" reward. Immediate reward refers to paying less immediately with some uncertain security risk and delay reward refers to paying the same as the first choice only after redeeming a mail-in debate three months later with no security risk. In addition, subjects were asked for demographics, computer security knowledge, and computer experience.

RESULT ANALYSES

The participants were graduate and undergraduate students attending a university in the Northeast United States. Some of the students were online while others were taking a regular lecture based class. The survey was anonymous and the students did not receive any reward or course credit for participation. There were a total of 131 students and 112 of them completed the entire survey. We analyzed only the responses from subjects who completed all the survey questions. Among them, 65 (58%) are males and 47 (42%) are females. The subjects include four age groups, 31 (27.7%) are between 18 to 20, 59 (52.7%) are

between 20 to 29, 13 (11.6%) are between 30 to 39, and 9 (8%) are between 40 to 49. The responses are from 67 (60%) undergraduate students and 45 (40%) graduate students. The undergraduates were mostly freshmen, who were taking a university level computer introductory course. The graduate students were from three information technology related Master's programs, including Information Systems, Computer Science and Internet Technology. Most of the graduate students were working professionals. Among the graduate students, there was a cohort of India nationals, living and working in Bangalore, India taking the courses online.

Risk Tradeoffs

In the first scenario, 46 (41%) subjects chose to buy the digital camera from the online store with security risk and 59 (59%) chose not to buy it from the online store with security risk no matter how much cheaper the camera is. Table 1 shows the results in detail. Our subjects tended to accept the reward at two extremes: they would either accept it as long as there was a reward or they would only accept it at the highest price that they could get. This result implies that our subjects varied a lot in terms of their assessment of value for security risk. Research (Grossklags and Acquisti, 2007) has shown that subjects prefer to accept monetary reward over protecting data in two personal information protection scenarios. Further research is needed to investigate subjects' willingness to accept a reward for taking computer security risks.

Choices	Frequency	Percent
Will accept unknown web script for $10 cheaper	16	14%
Will accept unknown web script for $20 cheaper	4	3.6%
Will accept unknown web script for $30 cheaper	4	3.6%
Will accept unknown web script for $40 cheaper	4	3.6%
Will accept unknown web script for $50 cheaper	18	16%
Do not tradeoff security with a cheaper price	66	58%
Total	112	100%

Table 1. Results from the first scenario

In the second scenario, 78 (70%) subjects chose the delay reward and 34 (30%) chose the immediate reward. The percentage of subjects (30%) who decided to take the security risk is less than the percentage (41%) in the first scenario. Table 2 is a cross table of the two decisions. We observed three types of risk tradeoffs. The first group of subjects (77%) was consistent in both scenarios regarding their risk tradeoffs. Among them, 59 (53%) try to avoid the security risk in both scenarios by rejecting the monetary and immediate rewards. 27 (24%) accepted the security risk in both scenarios by accepting the monetary and immediate rewards. The second group of subjects (17%) chose to avoid the security risk as long as they obtained a reward. These subjects decided to take the security risk by accepting the monetary reward but avoided the security risk with the delay reward. The third group of subjects was inconsistent in their risk tradeoffs. 7 (6%) subjects decided to avoid the security risk by rejecting the monetary reward but they chose the immediate reward to accept the security risk. It is not clear what rationale was behind their choices. It is possible that the subjects made the choices randomly without understanding the scenarios.

		Scenario two (time delay reward)		
		delay reward	immediate reward	Total
Scenario one (monetary reward)	Rejecting reward	59 (53%)	7 (6%)	66 (59%)
	Accepting reward	19 (17%)	27 (24%)	46 (41%)
	Total	78 (70%)	34 (30%)	112

Table 2. Cross table of the responses from both scenarios

Individual Difference, Computer Security Knowledge and Computer Experience

We conducted a regression analysis to investigate hypotheses H1-H4 proposed in our conceptual framework. We analyzed the impact of independent variables on the choices in the two scenarios: the choice between accepting and rejecting a monetary reward and the choice between delay reward and immediate reward. Binary logistic regression was used since the dependent variables are binary.

Table 3 shows the independent variables that have significant impact at $p<0.05$. To study the impact of computer security risk perception on subjects' choices on the two scenarios, we calculated the average ratings of risk perception, denoted as average risk perception, and the average ratings of risk attitude, denoted as average risk attitude, towards the 7 computer security risk activities in Appendix A. We have five observations here.

1) Culture was a significant factor in the reward choice (supports hypothesis H2.a). The Indian students were more likely to accept a reward than non-Indian students (mostly US students) at $p=0.02$. We suspect that less Internet shopping experience might have an impact on the Indian students' decisions, but further study with a larger sample size is needed to verify this hypothesis.
2) Average risk perception was negatively correlated to both choices (supports hypothesis H1.a). This result implies that subjects who rejected the reward or chose the delay reward were more likely to be aware of the security risk than the subjects who accepted the monetary or immediate rewards.
3) Average risk attitude was positively correlated to both choices (supports hypothesis H1.b). This result implies that subjects who were more likely to engage in other types of computer security risk were also more likely to accept the monetary or immediate reward.
4) Security skill was negatively correlated to both choices (supports hypothesis H4.d). Subjects who had practiced more security skills, such as encrypting their emails or using software to detect spyware, were more likely to reject the monetary reward or to accept the delay reward. This result confirmed findings in (Asgharpour et al., 2007) in which computer security risk taking strongly correlated to an individual's level of expertise in security.
5) We did not find significant correlation to support other hypotheses (rejects H2.b, c, d; H3; and H4a, b, c, e, f at $p=0.05$) in the conceptual model. We did not find any significant correlation between the two choices and other computer experience, such as computer usage or online shopping experience, subjects' knowledge on web security technology and subjects' previous education in security courses.

Dependent variables	independent variables	Chi-square	B	S.E.	Wald	p	Exp(B)
Monetary reward (1: accepting reward/ 0: rejecting reward)	culture	6.70	-1.52	0.66	5.28	0.02	0.22
	average risk perception*	16.80	-1.21	0.33	13.58	<0.01	0.30
	average risk attitude*	2.44	0.49	24.76	1.00	<0.01	11.46
	security skill	8.28	-0.24	0.09	7.48	0.01	0.79
Time delay reward (1: immediate reward/ 0: delay reward)	average risk perception *	14.51	-1.22	0.36	11.67	<0.01	0.30
	average risk attitude*	0.92	0.32	8.01	1.00	<0.01	2.50
	security skill	6.51	-0.22	0.09	6.17	0.01	0.80

Table 3. Regression results for both monetary and time delay reward tradeoffs (* denotes $p<0.01$.)

DISCUSSION AND IMPLICATIONS

Prospect theory predicts that people tend to have inconsistent preferences when the same choice is framed differently (Tversky and Kahneman, 1981). Risk attitudes are different depending if the outcome is framed as a gain or a loss. People tend to be risk averse when the choice is framed as a gain but people tend to be risk seeking when the choice is framed as a loss. In the first scenario, we did not specifically frame our choices as gains or losses but different subjects might interpret the choices differently. Table 4 shows the possible interpretations of the choices in our scenarios. When the choices were

interpreted as gains, based on Prospect theory, our subjects should accept the reward. When the choices were interpreted as losses, our subjects should also accept the reward.

	Accepting reward	Rejecting reward
Choices framed as gains	Certain monetary reward	Uncertain computer security benefit
Choices framed as losses	Uncertain computer security loss	Certain monetary reward loss

Table 4. Framing the choices in the first scenario

However, the assumption behind the prediction is that the expected values of the two choices are equal. The expected value of computer security risk is hard to estimate since the probability of occurrence is hard to obtain. Individuals might have different perceived risk and have different valuation of computer security benefit as well. As we found in the previous section, subjects who perceived higher risk were more likely to reject the monetary reward. Their expected value of avoiding security risk was thus higher than the monetary reward presented in the choice. That is, their expected value of avoiding downloading the web script was more than $50 in the first scenario. For example, a technical savvy user might perceive a higher risk from the first scenario and therefore is less likely to accept the $50 reward but might accept a higher reward if it is expressed explicitly. We also observed similar results in the second scenario. If the subjects discounted a future reward, they should choose to take the immediate reward unless the expected value of the security benefit compensated the reward discounted by time.

Our results provide some insights into computer security risk management. First, the users have shown to be the weakest link in security from our observations. Although about 53% of our subjects chose to avoid security risk in both scenarios, 47% of subjects accepted the security risk in either one or both scenarios, which is a large percentage for computer security protection strategies to be effective. For example, an Internet worm could exploit the computers of these subjects and execute a denial of service attack to the servers managed by individuals who would choose to avoid the risk in the first place. Phishing attacks could be profitable even if they can only allure 47% of the users who have received phishing emails. Second, since average risk perception in security is a significant factor in computer security risk tradeoff, communicating computer security risk to the users might hold the key to reducing the risk, such as educating users about the likelihood of certain computer security incidents. Last but not least, educators can introduce users to more hands-on skills in computer security since our study found that individuals who have more security skills are less likely to tradeoff computer security risk with rewards.

CONCLUSIONS

We conducted an empirical study comparing tradeoffs on computer security risk and analyzed the variables that might have an impact on them. Our analyses showed that individuals who perceived higher computer security risk tend to reject monetary reward and avoid risk than individuals who had a lower risk perception. In addition, both culture and security skill have an impact on decision-making when avoiding computer security risk. Further research can be conducted to investigate the willingness to accept a reward for taking computer security risk and associated expected value on different types of computer security risk.

REFERENCES

1. Acquisti, A., and Grossklags, J. "Privacy and Rationality in Individual Decision Making," IEEE Security & Privacy (3:1), January/February 2005, pp 24-30.

2. Asgharpour, F., Liu, D., and Camp, L.J. "Mental Models of Computer Security Risks," in: Workshop on the Economics of Information Security, Pittsburgh, PA, 2007.

3. Aytes, K., and Connolly, T. "Computer Security and Risky Computing Practices: A Rational Choice Perspective," Journal of Organizational and End User Computing (16:3), Jul-Sep 2004, pp 22-40.

4. Bhatnagar, A., Misra, S., and Rao, H.R. "On Risk Convenience, and Internet Shopping Behavior," Communications of the ACM (43:11), November 2000, pp 98-105.

5. Bodin, L.D., Gordon, L.A., and Loeb, M.P. "Information Security and Risk Management," Communications of ACM (51:4), April 2008.

6. Chen, L.-C., and Farkas, D. "Individual Risk Perception and Attitude towards Computer Security Risks," International conferences on Internet Technologies and Applications, North Wales, UK, 2009.

7. Cranor, L.F., and Garfinkel, S. (eds.) Security and Usability. O'Reilly, Sebastopol, CA, 2005.

8. Dhamija, R., Tygar, J.D., and Hearst, M. "Why Phishing Works," in: ACM CHI, Montreal, Canada, 2006.

9. Diesner, J., Kumaraguru, P., and Carley, K.M. "Mental models of data privacy and security extracted from interviews with indians," 55th Annual Conference of the International Communication Association, New York, NY, 2005.

10. Downs, J.S., Holbrook, M., and Cranor, L.F. "Behavioral Response to Phishing Risk," in: APWG eCrime Researchers Summit, Pittsburgh, PA, 2007.

11. Friedman, M., and Savage, L.J. "The Utility Analysis of Choices Involving Risk," The Journal of Political Economy (56:4), August 1948, pp 279-304

12. Grossklags, J., Christin, N., and Chuang, J. "Predicted and Observed User Behavior in the Weakest-Link Security Game," in: Usability, Psychology, and Security San Francisco, CA, 2008.

13. Hardee, J.B., West, R., and Mayhorn, C.B. "To Download or Not to Download: An Examination of Computer Security Decision Making," ACM Interactions), May/June 2006, pp 32-27.

14. Jens Grossklags, A.A. "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information " Workshop on the Economics of Information Security, Pittsburgh, PA, 2007.

15. Kahneman, D., and Tversky, A. "Prospect Theory: An Analysis of Decision under Risk," Econometrica (47:2), March 1979, pp 263-291.

16. Liu, D., Asgharpour, F., and Camp, L.J. "Risk Communication in Computer Security Using Mental Models," Usable Security, Trinidad/Tobago, 2007.

17. Loewenstein, G. "The Fall and Rise of Psychological Explanations in the Economics of Intertemporal Choice," in: Choice over Time, G. Loewenstein and J. Elster (eds.), Russell Sage Foundation, New York, 1992.

18. Loewenstein, G., and Prelec, D. "Anomalies in Intertemporal Choice: Evidence and an Interpretation," The Quarterly Journal of Economics (107:2), May 1992, pp 573-597.

19. Machina, M.J. "Expected Utility Hypothesis," in: Utility and Probability: Utility and Probability, J. Eatwell, M. Milgate and P. Newman (eds.), W . W. Norton & Company, 1990.

20. Miyazaki, A.D., and Fernadez, A. "Consumer Perceptions of Privacy and Security Risks for Online Shopping," The Journal of Consumer Affairs (35:1) 2001, pp 27-44.

21. Morgan, M.G. "Probing the Question of Technology-Induced Risk," IEEE Spectrum (18:11), November 1981, pp 58-64.

22. Morgon, M.G., Fischhoff, B., Bostrom, A., and Atman, C.J. Risk Communication: A Mental Models Approach Cambridge University Press, Cambridge, UK, 2001.

23. Norman, D. "Some Observations on Mental Models," in: Mental Models, D. Gentner and A. Stevens (eds.), LEA, 1983.

24. Stoneburner, G., Goguen, A., and Feringa, A. "Risk Management Guide for Information Technology Systems," D.o.C. National Institute of Standards and Technology (ed.), 2002.

25. Tversky, A., and Kahneman, D. "The Framing of Decisions and the Psychology of Choice," Science (211:4481), Jan. 30 1981, pp 453-458.

26. Tversky, A., and Kahneman, D. " Advances in Prospect Theory: Cumulative Representation of Uncertainty," Journal of Risk and Uncertainty (5:4), October 1992, pp 297-323.

27. Weber, E.U., Blais, A.-R., and Betz, N.E. "A domain-specific risk-attitude scale: measuring risk perceptions and risk behaviors," Journal of Behavioral Decision Making (15:4), October 2002.

28. Weber, E.U., and Hsee, C. "Cross-Cultural Differences in Risk Perception, but Cross-Cultural Similarities in Attitudes towards Perceived Risk," Management Science (44:9), September 1998, pp 1205-1217.

29. West, R. "The Psychology of Security," Communications of ACM (51:4) 2008, pp 34-40.

APPENDIX A: RISK QUESTIONS IN COMPUTER SECURITY

1. Clicking on a unknown web link sent by a friend through emails
2. Accepting unknown web scripts in order to watch your favorite show online
3. Downloading free software from unknown sources on the Internet
4. Accepting web cookies to read online newspaper
5. Saving user names and passwords of web sites on your computer for future access
6. Purchasing a product from an online merchant that you have not heard of before
7. Accepting unknown web scripts in order to pay your bill online

APPENDIX B: RISK TRADEOFF SCENARIOS

Scenario 1: Assume that you decide to purchase a digital camera from an online store that offers the best price. The camera is $200 (USD). When making an order on this online store, the browser asks you if you would like to accept unknown web scripts from the store's web site. Which of the options would you choose?

A. Will accept unknown web scripts from the store if the camera is $10 (USD) cheaper than other stores.

B. Will accept unknown web scripts from the store if the camera is $20 (USD) cheaper than other stores.

C. Will accept unknown web scripts from the store if the camera is $30 (USD) cheaper than other stores.

D. Will accept unknown web scripts from the store if the camera is $40 (USD) cheaper than other stores.

E. Will accept unknown web scripts from the store if the camera is $50 (USD) cheaper than other stores.

F. Will not accept unknown web scripts no matter how much cheaper this store sells the camera compared to other stores. You will buy the camera from another store.

Scenario 2: Assume that you decide to choose from two online stores that both sell the same digital camera. Which of the following options would you choose?

Store A charges $200 (USD) for the camera but asks you to accept unknown web scripts while making the order.

Store B charges $250 (USD) for the same camera but offers a mail-in rebate through which you can reclaim $50 (USD) three months later.