2000

Consumer Perceptions of Online Transaction Security - A Cognitive Explanation of the Origins of Perception

Easwar A. Nyshadham
Embry-Riddle Aeronautical University, nyshadhe@cts.db.erau.edu

Consumer Perceptions of Online Transaction Security - A Cognitive Explanation of the Origins of Perception

Easwar A. Nyshadham, Department of Aviation Business Administration, Embry-Riddle Aeronautical University, nyshadhe@cts.db.erau.edu

"Many consumers visit the Travelocity site, but it takes as many as five visits to generate a single booking, and many people look but never book at all. Why? The primary reason given for this hesitancy is the fear of credit card theft or fraud. Even among those persons who made a reservation, a study showed that some three out of five agreed with the statement that sending a credit card over the Internet was "just plain stupid." The fact is that the chances of fraud or theft with respect to credit card transactions on the Internet are far less than for transactions using cash registers, fax machines, the mails, and the telephone. ***Yet, nagging doubt persists, and consumer perceptions are of course reality(*****emphasis ours*****)****. We will continue to work with Mastercard and other leaders to develop standards for secure electronic transactions that will alleviate these fears. In the meantime, the government can help by letting the public know that electronic transactions are safe."*

by CEO of Travelocity, April 1998, Testimony before House Committee

"While many consumers are visiting online retailers, few are buying. ***The study argues that online retailers need to improve convenience and value for consumers and assist them in overcoming their fears around security. Retailers must also provide reluctant consumers with compelling reasons for accepting the Internet as a new way to shop(*****emphasis ours*****)****. Some of these reasons might include the use of consumer assurance brands and enhanced levels of convenience, customization, selection, service and pricing."*

From the Executive Summary of a study conducted by Boston Consulting Group, for Shop.Org, March 1999

Abstract

An important impediment to the success of business to consumer ecommerce is the consumer perception regarding the riskiness of the online channel. A widely held perception among consumers is that financial transactions on the Internet are inherently more risky and not secure. Interestingly enough, most security experts would view Internet transaction as, in fact, more secure than traditional transactions. The persistence of this misperception is therefore, quite surprising.

In this research, we focus on consumers' perceptions of online risks. We suggest that the consumer risk perceptions also arise from some well-known cognitive biases that decision-makers (consumers) are typically subject to. Taking an information processing view of customer decision making, we provide a subset of cognitive biases, which affect consumer judgments in information acquisition, alternative valuation and learning from evidence. Theoretical and limited experimental evidence is provided.

Keywords: Electronic Commerce, Internet, security, privacy, B2C commerce, online risks, heuristics, cognitive biases

Section 1: Risks in B2C Online Ecommerce and Research Questions

There is a widely held perception among consumers that informational flows associated with online transactions are much less secure than the flows in traditional transactions. Three issues of managerial importance emerge from such a perception. The first quote summarizes the first issue: consumers subject to such a perception may either not transact online at all or may only partially consummate the transaction on the Internet i.e., consumers may "look" but not "book" online. The second issue arises from the second quote: to the extent that such a perception exists, do consumers have to be provided additional compensation or "compelling reasons" for engaging in online transactions? The third issue follows from the above two – if the security concerns are merely a perceptual issue and not based on objective evidence, then why can't the industry merely communicate to the consumers that their exaggerated perceptions are incorrect?

In this research, we examine a descriptive theory of decision making (e.g., Prospect Theory) and identify heuristics/biases which can explain the questions raised above. The three research questions are stated as follows:

R1: Do cognitive biases affect consumer perception of online transaction risk?
R2: Do cognitive biases affect the "compensation" demanded by consumers for transacting online?
R3: Do cognitive biases affect how consumers process objective risk information?

Section 2: Security Perceptions

Numerous surveys (Anonymous 1997a, 1997b, 1998a, 1998b, 1998c, 1998d, 1999a, 1999b) have been conducted to understand consumer perceptions of online transactions. Two primary "sources of friction" for online transactions that emerge from a summary of the studies are i) security concerns and ii) privacy concerns. Rose et. al., (1999) conducted a comprehensive review of technological impediments to business to consumer electronic commerce and suggest that security is the most important issue facing business to consumer ecommerce. In this research, we view security as the primary determinant of consumer trust and hence focus on this issue.

The consumer perception that Internet transactions are insecure is quite surprising. Numerous technology experts refute the claim that transacting on the Internet by sending credit card information or other important personal information is any less secure than transacting otherwise (See, for example, the quote by the CEO of Travelocity). It is likely that encrypted information flows are the least significant source of security risks. Second, the most significant risks for security may arise from the internal security policies and procedures adopted by firms (Cohen, 1996). Segev et. al. (1998) suggest that the most sever security threat may in fact be the "emancipated corporate computer user".

To summarize, numerous independent surveys have found that, consumer concerns about security and privacy far outweigh their other concerns such as usability of the web site, download delays, search problems, interface limitations etc. From a consumer perspective, it is likely that security is primarily a perceptual issue – i.e., consumers systematically misjudge the risks in online transactions. Consumer perceptions that online transactions are insecure, we submit, arise from cognitive heuristics they employ in understanding and evaluating risks. The heuristics or "rules of thumb" employed by consumers lead to systematic misperceptions or cognitive biases.

Section 3: Security perceptions and Cognitive Biases

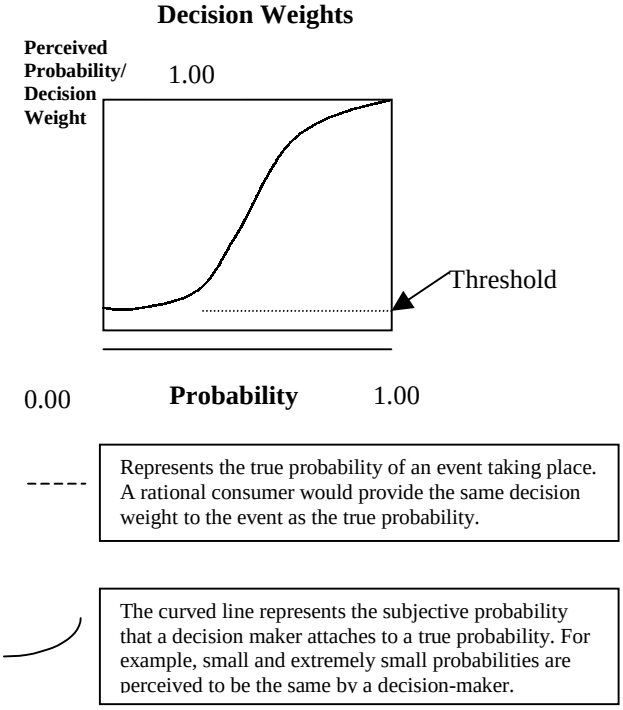
Normative theories of decision making, such as the Subjective Expected Utility Theory (SEU theory) describe how a decision makers ought to behave. In contrast, descriptive theories, such as the Prospect Theory (Tversky and Kahneman, 1992), focus on how consumers behave rather than how they ought to behave. This stream of literature (Kahneman & Tversky 1983, Slovic & Lichtenstein 1982) argues that humans are subject to biases, which are perceptual in origin. When faced with a decision problem, humans employ heuristics to simplify processing of information. However, to the extent that heuristics are "rules of thumb", they are not always accurate. Application of heuristics, therefore, can lead to *systematic* errors in judgment.

The research questions and the relevant biases organized by stage of human information processing are summarized in Table 1.

a) Information Acquisition Stage:

When making decisions under uncertainty, people "code" objective probabilities of events presented to them into subjective probabilities or "decision weights" prior to decision making. The function used to convert true probabilities to decision weights is S-shaped and flat at lower end, as shown in Figure1. (Tversky and Kahneman 1992, Camerer and Ho 1994, Tversky and Fox 1995, Wu and Gonzalez 1996, Gonzalez and Wu 1999). The implication of a consumer using such a function is that, individuals attach the same subjective probability to all events below a certain probability threshold.

Figure 1: Normative probabilities versus



An Illustration of Coding Bias: Assume that a consumer initially views an unencrypted web site as having a small risk p=.001(say) of being hacked. Assume the vendor upgrades security through an appropriate mechanism and lowers the risk to one in a quadrillion (i.e., $p=1/10^{15}$). If the threshold of probability for the consumer is (say) .001, then she consumer would perceive the same risk for even after the security upgrade.

Table 1. Summary of Cognitive Origins of security concerns

Research Questions/ Support	Stage of Information processing	Phenomenon / Source of Bias	Implication for Consumer Decision Making
R1: Do cognitive biases affect consumer perception of online transaction risk? **Support: Literature**	**Information Acquisition:** Understanding of probabilities of risky events	Consumers fail to distinguish between very low probabilities and low probabilities and behave as if they are nearly the same./ Decision weights used in place of true probabilities	Probability of online security risk is overestimated.
	Information Acquisition: Understanding of probabilities of risky events	Concrete and vivid examples of past risky events, rather than frequency, are used to judge the probability of occurrence of events in the future/ Availability and Concreteness heuristics	Probability of online security risk is overestimated**.**
R2: Do cognitive biases affect the "compensation" demanded by consumers for transacting online? **Support: Literature**	**Evaluation of Alternatives:** Valuing a gamble	In comparing online versus traditional offerings, if consumers view the online channel as riskier, the perceived value of the online offering will be much lower to the consumer than the rational theory would suggest/ Loss Aversion Phenomenon.	The value of a good sold online is underestimated**.**
R3: Do cognitive biases affect how consumers process objective risk information? **Support: Literature and an Experiment**	**Attribution of Causes and Effects:** Formation of a mental model of risks and causal attributions	Statistical data and expert judgments will not be used to correct misperceptions./ Neglect of consensus information in attribution and the base rate neglect biases.	Online transactions will continue to be perceived as risky, regardless of how sound and statistically valid evidence to the contrary is.

Kahneman and Tversky (1983) describe a second cognitive bias, which also serves to exaggerate risk perception in consumers. They state that when people assess the probability of an event, the ease with which salient instances or occurrences, which are readily "available" for recall determine the value assessed. The judgmental heuristic used here is called availability. However, availability in memory is affected by how vividly prior instances of the event were described to a subject. Slovic et.al., (1983) argue that concrete illustrations of a phenomenon make them more available, so that they are easily recalled from memory by human decision-makers and used as proxies for estimation of likelihood of an event..

Illustration of Availability and Concreteness: In the past, media has focused a lot of attention on hackers (Slatalla and Quittner 1995, Stoll 1989.) Further, the breaking of the 40-key encryption code used by Netscape browser in earlier versions, as well as the 56-bit DES encryption code are also public knowledge and are discussed in textbooks dealing with electronic commerce (Kalakota and Whinston 1996). To the extent that a customer can recall the security incidents vividly, she will overstate the probability of hacking or a general security incident.

To summarize, the two cognitive phenomena described above explain why the probability of a risky event, such as hacking, may be exaggerated by most consumers. The first bias suggests that consumers do not distinguish between low and extremely low probability events and perceive them as if they were nearly the same. The second bias (availability) suggests that concrete illustrations of phenomenon, rather than frequency of the phenomenon, influence probability judgment. The overall impact of these biases is that, a human decision maker would systematically overestimate the security risks in online transactions. Hence, consumers would perceive the Internet as more risky than it actually is.

b) Valuing Alternatives

According to Kahneman and Tversky (1983), "losses loom larger than gains". It may be argued that people use the traditional, offline transaction channels as a frame of reference when evaluating online transactions. To the extent that online channels are considered to be riskier, consumers may perceive a potential loss in transacting online. Using traditional utility theory, one would assume that a consumer should be offered a "risk premium" to make her indifferent between using the traditional channel versus the online channel. Under prospect theory, however, the disutility of an online transaction, being a perceived loss, is higher than rational theory would suggest. Ceteris paribus, the risk premium or the "compensation" demanded by a consumer under Prospect Theory will be larger than the risk premium computed under rational theories.

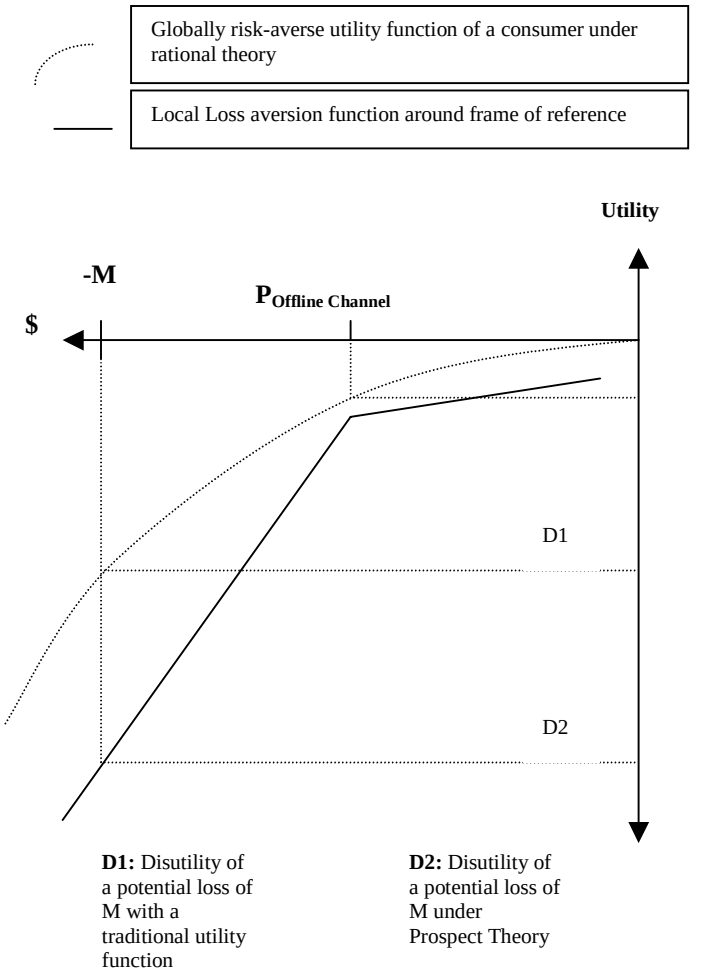
Assume that a consumer perceives the offline channel as risk free. However, on the online channel, a consumer may perceive that a small probability p exists of a loss of

$M, say due to credit card fraud. This creates an added disutility to the consumer. Therefore, to make a consumer indifferent between buying online versus offline, a "compensation" or risk premium has to be offered to the consumer. Given a utility function for the consumer and specific values for probability p and potential loss $M, a risk premium can be computed.

The magnitude of risk premium would be higher under Prospect Theory. Prospect theory would suggest that consumers would now use a local utility function, centered on the frame of reference, which has a much steeper slope for perceived losses than perceived gains. Correspondingly, the disutility of buying online is higher and therefore, to compensate for this higher disutility, a larger "compensation" or risk premium needs to be offered.

This argument is presented in Figure 2. Consumer utility is plotted on the y-axis and the dollar amounts corresponding to a loss of $M (hence -$M) is plotted on x-axis. The $P_{Offline\ Channel}$ represents the frame of reference. The consumer is assumed to have a globally concave,

Figure 2. Disutility under Loss Aversion



risk-averse utility function which is standard in utility theory. A potential loss of $M has a disutility corresponding to the intercept on y-axis of D1. The prospect theory utility function is centered around the current frame (price in an offline channel) and is much steeper for losses than gains. The corresponding disutility is D2 which is higher than D1, the disutility under standard theory. The corresponding expected disutility under prospect theory will also be higher (probability of loss, p, is not shown in the figure.).

Illustration of Loss Aversion: To make this argument concrete, assume that a widget is being sold offline for $P_{offline\ channel}$ of $10. When the same widget is sold online, due to the added risk, assume that a standard "compensation" of E(-$M,p)=$-1 has to be offered to make a consumer indifferent to buying the product online versus offline. Under prospect theory, the expected disutility has to be larger than $1, say $2. The price of widget, under loss aversion is, therefore, $8. The impact of loss aversion is that goods sold online will be undervalued, ceteris paribus.

c) Attribution Biases and Consumer Learning

To the extent that industry experts believe that online transactions are not as insecure, it would seem that communicating the lower risks is a solution to the problem. If consumers are provided with objective information on risks, will they discard their original perceptions and use the objective information in their decision making?

In an experiment designed to answer this question, 50 undergraduate subjects enrolled in a business school were informed that in a typical Internet transaction, five parties are usually involved and each one contributes to the riskiness of the transaction. The parties are: buyer, seller, the insecure channel, a financial intermediary such as a credit card company and the Internet Service Provider (ISP). Subjects were initially asked to provide a subjective estimate of risks arising out of each party involved in an online transaction, using a constant sum 100 point scale. Following this, they were provided with hypothetical base rates i.e., seemingly objective probabilities of how likely each party would have been responsible for a security incident.

Next, a vignette was provided to the students in which, a hypothetical consumer makes an online purchase and finds out three months later, that there was suspicious activity on his credit card. The vignette was carefully structured to be completely uninformative. Subjects were then asked to provide a third set of risk estimates to

indicate the probability that each party was responsible. A copy of the instrument is available from the author.

The mean perceived risks for each party, aggregated across subjects, are plotted on the y-axis in Figure.4. The first set of columns refers to the subjective mean risks provided by subjects at the beginning of the experiment. The second set of columns displays the researcher-provided base rates i.e., seemingly objective probabilities based on a fictitious study. Subjects participating in the experiment did not know this during the study, but were debriefed later on. The third set of columns refer to the probabilities assigned to various parties by students, after they are exposed to the base rates and the vignette.

Since the vignette itself is uninformative, subjects will have to make judgments of risks based on prior information. If subjects persisted with their original perceptions, then the distribution of risks across parties in perceived and judged cases should be nearly the same. The hypothesis is stated formally as follows:

H1: Judged probabilities (third set of columns) come from the same distribution as the perceived probabilities (first set of columns)

A Kolmogorov-Smirnoff test for equality of two sample distributions was rejected at 0.05 level (D*=2.6), suggesting that original perceptions were modified during the experiment. A second K-S Test was conducted to test if the treatment had an effect, i.e., judged probabilities had the same distribution as the base rates. The hypothesis is stated as follows:

H2: Judged probabilities (third set of columns) come from the same distribution as the base rates (second set of columns).

A Kolomogorov-Smirnoff test for equality of perceived and base rate distributions led to a rejection of the null that the two distributions were equivalent at 0.05 level (D*=1.94). This would suggest that subjects, in judging fault based on the uninformative vignette, did not use the base rate information.

The results from the experiment may be summarized as follows: subjects judgments indicate that neither their original perceptions, nor the base rates are being used. Communicating seemingly objective base rates to the subjects did not result in subjects using the base rates. Difficulty in communicating risks, therefore, is a significant issue for online security perceptions.

Section 5: Summary

Current research on electronic commerce security is focused on the technical aspects such as vulnerabilities, risks, mechanisms and security frameworks etc. Increasing evidence suggests that consumers perceive the online channel as more risky than traditional channels. Such perceptions may be best explained as arising out of well known cognitive biases that consumers are subject to.

Cognitive biases literature provides a theoretical basis for suggesting that i) security risks will be exaggerated by consumers, ii) the "compensation" sought by consumers may be more than what traditional theory would suggest, ceteris paribus, and iii) such perceptions may be difficult to change. The implied hypotheses may be tested in an empirical and/or experimental setting. In this research, we provide experimental evidence to answer the third research question which suggests that consumers are likely to ignore seemingly objective evidence and therefore, it would be difficult to communicate online transaction risks.

Future research may focus on further clarifying and extending the role of cognitive biases in security perceptions. In this research, theoretical support was provided for the first two research questions and experimental evidence was provided for the third research question. Experimental tests of the first two research questions will also be an important step in understanding the role of the biases.

References:

Anonymous (1997a) "CDT Survey" http://www.cdt.org/privacy/survey/findings/cdtbody.html

Anonymous (1997b) "April 1997: Commerce, Communication, and Privacy Online" http://idt.net/~pab/comp%20surv.html

Anonymous(1998a) "June 1998: E-Commerce and Privacy: What Net Users Want" June 1998: E-Commerce and Privacy: What Net Users Want http://idt.net/~pab/E-Commerce%20Exec.%20Summary.html

Anonymous (1998b) "FamilyPC User Internet Study '98" http://www.cdt.org/privacy/survey/findings/familypc.html

Anonymous (1998c) "GVU's 10th WWW User Survey" http://www.gvu.gatech.edu/user_surveys/survey-1998-10/ (December 1998)

Anonymous (1998d) "Window-Shopping the Web" http://www.idg.net/idg_frames/english/content.cgi?vc=docid_9-117089.html

Anonymous (1999a) "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy" http://www.cdt.org/privacy/survey/findings/attbody.html

Anonymous(1999b) "Executive Summary" section in The State of Online Retailing 2.0 by Boston Consulting Group http://www.shop.org/research/summary.htm

Camerer C.F. and Ho Teck-Hu. (1994) "Violations of the Betweenness Axiom and Nonlinearity in Probability". Journal of Risk and Uncertainty 8, 167-196

Cohen,F. (1996) "Your Firewall won't save you". Forbes ASAP Supplement, June 3

Gonzalez R and Wu G. (1999) "On the Shape of the Probability Weighting Function" Cognitive Psychology (forthcoming)

Kahneman, D., and Tversky, A. (1992) "Prospect Theory: An Analysis of Decision Making under Risk"; Econometrica; 47,263-291

Kahneman, D., Slovic, P ., Tversky, A. (1982) *Judgment under Uncertainty: Heuristics and Biases*; Cambridge University Press

Kalakota R., and Whinston B. A. (1996) "Electronic Commerce : A Manager's Guide". Addison-Wesley Publishing Co.

Pecaut D.(1999) "Boston Consulting's E-Commerce Practice", Interview transcripts available at http://news.lycos.com/stories/Technology/Internet/19990719RTNET-RETAIL-ONLINE.asp, Monday, July 19

RSA (1998). "RSA Laboratories' Frequently Asked Questions About Today's Cryptography". Available at: http://www.rsa.com/rsalabs/faq/html/questions.html

Rose, Gregory; Khoo Huoy; Straub W. Detmar. (1999)"Technological Impediments to Business to Consumer Electronic Commerce", Communications of the Associations for Information Systems, Volume 1, Article 16, June

Segev Arie., Porra J and Roldan M. (1998) "Internet Security and the case of Bank America", Communications of the ACM, Vol.41, No.10, pp. 81-87

Slatalla, M. & J. Quittner (1995). Masters of Deception: The Gang that Ruled Cyberspace. HarperCollins (New York).

Slovic, P., Fischoff, B., and Lichtenstein, S. (1982) "Facts versus Fears: Understanding Perceived Risk" in *Judgment under Uncertainty: Heuristics and Biases*

Kahneman, D., Slovic, P ., Tversky, A.,(Eds.), Cambridge University Press; pp. 463-489

Stoll, C. (1989). The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Pocket Books (Simon & Schuster, New York).

Tversky A. and Fox C.R. (1995) "Weighting Risk and Uncertainty". Psychological Review, 102, 269-283

Tversky A. and Kahneman D. (1983) Availability: A heuristic for judging frequency and probability; *Cognitive Psychology*; 5, 207-232

Wu G., and Gonzalez R.G. (1996) "Curvature of the Probability Weighting Function". Management Science, 42, 1676-1690