E-COMMERCE SAFETY AND SECURITY: A STATISTICAL ANALYSIS OF CONSUMERS' ATTITUDES

Dr. Tyler T. Yu, Mercer University, yu_tl@mercer.edu
Dr. Miranda M. Zhang, Mercer University, zhang_mm@mercer.edu
Dr. Lloyd Southern, Mercer University, southern_l@mercer.edu
Dr. Carl Joiner, Mercer University, joiner_wc@mercer.edu

ABSTRACT

This article examines the issue of E-commerce - Internet security. A review of the literature is provided first. Then marginal and joint probability analysis is conducted to demonstrate the relationship between consumers' attitudes toward Internet security and a set of selected socioeconomic and demographic variables. Then, hypothesis tests are performed to determine the statistical significance of the relationship. Empirical results show that consumers' thoughts and attitudes toward Internet/E-commerce safety and security are largely affected by various demographic and socioeconomic factors such as age, gender, race/ethnicity, employment status, computer skills, income levels, career differentiation and educational background.

Keywords: E-commerce, Internet security, consumer attitude, test of independence

INTRODUCTION

On October 27, 2000, hackers broke into Microsoft's computer network and tapped some of the software giant's secrets. The attack revealed one of the boldest industrial spy capers of the computer age and marked the rise of a new style of hacking that used a stealthy program called a worm to slip past computer defenses (8). The break-in was a deplorable act of corporate espionage aiming at Microsoft's flagship products Windows and Office. Cyber-blitzes like those briefly knocked out major Web sites in February 2000 – including Yahoo's and Inc.'s Internet gateway, e-Bay Inc.'s auction service and Amazon.com Inc.'s retail site – could easily be copied on a larger scale, pointed out by Richard Clarke, a staff member of the White House National Security Council of the Clinton Administration. Due to the nature of e-commerce, consumer confidence levels regarding privacy of personal information play a role in the growth rate of on-line business. Although industry initiatives and government regulations are necessary for tackling the security of e-business, we ultimately have zero privacy regardless of interventions (5). Currently, the U.S. government's privacy policy relies on industry self regulation rather than legal rights. Those currently in place are often vague, dubious, and subject to interpretation. It is argued that in the United States, substance abusers have greater privacy than Web users (7).

Despite the potential rewards for conducting business on the Internet, major corporations have been slow to embrace this technology (2). The number one rated concern for both businesses and consumers in establishing and participating in e-commerce is the potential for loss of assets and privacy due to breaches in the security of commercial transactions and corporate computer systems. A single publicized security breach can erode confidence in the business and not only damage the reputation of the firm, but also hurt the e-commerce industry as a whole.

PURPOSE AND OBJECTIVES

The purpose of this paper is to examine the potential consumers' attitudes toward Internet security issue. Specifically, a descriptive statistical analysis will be conducted, based on the survey information, to look at some of the probabilistic measures of consumers' opinions and attitudes toward Internet safety. Hypotheses tests will be performed to determine the statistical significance of their opinion and attitudes in relation to some of the demographic and economic factors, such as gender, income and educational background. Finally, conclusions will be drawn.

LITERATURE REVIEW

McGuire and Roser addressed the Internet security issue from business perspective (6). The authors suggest that recent attacks against websites and virus outbreaks should serve as a warning sign for companies doing business on the Internet. While opening new doors for companies worldwide for more business, it also makes companies more vulnerable in terms of security problems. They propose that the goal of Internet security should be to make an attack on the company computer system as difficult as possible. Specifically, the authors suggest that a company should define the way it uses the Internet. Then, it needs to identify possible threats, ranging from data destruction to unauthorized disclosure. Finally, it should match those threats with means and ways suitable and desirable to the company, or the company business operation.

Risk management has long been one of the primary concerns of most companies. Recently, risk management has had an added component: the attendant risk. Jorgensen (3) discusses the shifting paradigm of risk management from captive processing to the distributed access as the Internet has evolved into a global infrastructure that facilitates communication, control and computing. As such, risk managers must apply a systematic approach to examining their organizations' cyberspace activities and address risk identification, assessment, mitigation, financing and monitoring. The authors examined various aspects of risk management of corporate cyberspace including risk management process, using Internet as a business tool, how to protecting information, cyber-risk mitigation, and risk financing solutions.

Stevens discussed security issues relating to accountants as well as accounting firms, including virus threats, security issues, online data exchange, website security and physical security worries (10). As pointed out by the author, the riskiest area in the cyberspace management probably is in the establishment of the website by the accounting firm. Among all the threats to cyberspace, the virus is the most serious problem. Also, while the hackers' attacks to cyberspace draw most public attention, employees represent about 75% of the problem. It is suggested that employees should be screened and given limited access to the confidential information.

Some recent surveys suggest that this security problem is small but growing. The 1999 CSI survey of 521 organizations, including corporations, financial institutions, universities and government agencies, found system penetration by outsiders increasing for the third year in a row, with 30% of respondents reporting intrusions. The 163 institutions able to quantify the damage reported $124 million in total losses. The most serious threat was deemed to be "theft of property information," accounting for about $42.5 million in losses to 23 businesses and

organizations. "Financial fraud" ranked second in dollar amount that was lost, although it was slightly more common, with 27 respondents reporting $39.7 million in damage (11) .

A number of research articles addressed the concerns of the consumers on Internet safety (9, 12). Consumers tend to distinguish four types of privacy and security concerns for E-commerce: 1) Small-p privacy, as in freedom from junk mail, is a nuisance, but not a threat. 2) Privacy (large-P) of sensitive financial information is a significant concern. Privacy concerns are closely intertwined with security concerns. According to Tyler, consumers are also concerned about the security issues of giving their credit card details over the Internet. One of the problems is the authentication of the shoppers by vendors. 3) Security risk is based on the belief that either through malice of negligence, sensitive information or funds could be misrouted. And 4) Errors are closely related to perceived security of on-line transactions.

Abbot made a comparative study of the protocols used for online transactions (1). Secure Sockets Layer (SSL) and Secure Electronic Transactions (SET) are the two widely used communication protocols for making payments over the Internet. Abbot argues that there are four main benefits that SET offers over SSL. First, SET provides merchants with assurance that transactions will not be fraudulently charged back. This feature will lower the merchants' costs. Second, SET affords greater privacy and makes it easier to buy online. It assures the customer that the merchant is legitimate and the credit card is safe. Third, SET allows banks and companies extend their brands to cyberspace, while still maintaining their strong position as payment systems. The lower rates of fraud when using SET make credit cards more competitive than other means of payments. Fourth, SET defines inter-functionality between all parts of the card-payment process.

DESCRIPTIVE STATISTICAL ANALYSIS

The following constitutes the analysis of 156 observations in a survey concerning the safety issue on the Internet. In the survey, the 10 variables were taken into consideration to examine consumers' attitudes toward Internet safety: computer/e-commerce skills, e-commerce experience, age, gender, race or ethnicity, martial status, employment status, income level, career level, and educational background. The following tables demonstrate the joint and marginal probability analysis of the variables selected for this study.

The marginal and joint probabilities from Table 1 and Table 2 show the relationships between consumers' attitudes toward Internet/E-commerce safety and their computer/Internet skills and E-commerce experience. For example, the probability for a person to have some E-commerce

Table 1. Computer/Internet Skills

	UNSAFE	SAFE	VERY SAFE	TOTAL
NONE	2.56%	3.84%	0.00%	6.41%
SOME	8.97%	48.71%	10.89%	68.58%
A LOT	2.56%	15.38%	7.05%	25.00%
TOTAL:	**14.10%**	**67.95%**	**17.95%**	**1**

Table 2. E-commerce Experience

	UNSAFE	SAFE	VERY SAFE	TOTAL
YES	7.05%	48.07%	16.02%	71.15%
NO	7.69%	19.23%	1.92%	28.84%
TOTAL:	**14.74%**	**67.31%**	**17.95%**	**1**

skills and to consider it to be safe is 48.71 percent. Given that a person has some or a lot of computer/Internet skills, the probability for that person to consider E-commerce safe is 71.01 percent (the conditional probability). The probability that a person considers E-commerce to be safe and has experience is 48.07 percent. Given that the person has E-commerce experience, the probability for that person to consider the e-commerce to be very safe is 22.52 percent.

Tables 3, 4, and 5 show the probabilities derived for age, gender, and race/ethnicity. The probability for a person to be between 22 and 32 *and* consider E-commerce to be safe is 48.07%. Given that the person is between 33 and 42, the probability for that person to consider E-commerce to be safe is 85.71 percent. The probability for a person to consider E-commerce to be safe and to be female is 35.25%. The probability for a person to be male *and* to consider E-commerce to be very safe is 12.82%. Given that the person is a male, the probability for that person to consider E-commerce to be very safe is 25.32 percent. Given that the person is a female, the probability for that person to consider E-commerce to be safe is 71.43 percent. The probability for a person to be white *and* to consider E-commerce to be safe is 39.74 percent. The probability for a person to be black *and* to consider E-commerce to be safe is 16.66 percent.

Table 3 Age

	NOT SAFE	SAFE	VERY SAFE	TOTAL
22-32	12.18%	48.08%	13.46%	73.71%
33-42	1.92%	15.38%	0.64%	17.95%
43-52	0.00%	4.49%	3.21%	7.69%
OVER 52	0.64%	0.00%	0.00%	0.64%
TOTAL:	**0.15**	**0.68**	**0.17**	**1.00**

Table 4 Gender

	NOT SAFE	SAFE	VERY SAFE	TOTAL
MALE	5.13%	32.69%	12.82%	50.64%
FEMALE	8.97%	35.26%	5.13%	49.35%
TOTAL:	**14.10%**	**67.95%**	**17.95%**	**1**

Table 5. Race/Ethnicity

	NOT SAFE	SAFE	VERY SAFE	TOTALS
BLACK	3.21%	16.67%	0.00%	19.87%
WHITE	4.49%	39.74%	13.46%	57.69%
HISPANIC	0.00%	1.92%	1.28%	3.21%
ASIAN	6.41%	9.62%	2.56%	18.59%
NATIVE AMERICAN	0.00%	0.64%	0.00%	0.64%
TOTAL:	**14.10%**	**68.59%**	**17.31%**	**1**

Using the marginal and joint probabilities Table 6 and Table 7, some relationships between factors of employment status and income levels and consumers' attitudes toward Internet safety can be shown. For example, the probabilities for a person to be full time employed or not employed *and* to consider E-commerce to be safe are 55.12%, and 5.12%, respectively. The probabilities of full-time employed people considering the E-commerce to be very safe, safe, or not safe are 18.17%, 71.07%, or 10.74%, respectively. In terms of income, the probability for a person to have an income between *and* to consider E-commerce to be safe is 19.23 percent. The probability for a person to have an income between $50,000 and $74,999 *and* to consider E-commerce to be very safe is 3.84 percent. Given that a person has an income between $35,000

and $49,999, the probabilities that such a person considers E-commerce to be safe or very safe are 73.17%, or 14.64%, respectively.

Table 6. Employment Status

	UN SAFE	SAFE	VERY SAFE	TOTAL
FULL TIME	8.33%	55.13%	14.10%	77.56%
PART TIME	2.56%	5.13%	0.00%	7.69%
NOT EMPLOYED	1.92%	8.33%	3.21%	13.46%
UNEMPLOYED	1.28%	0.00%	0.00%	1.28%
TOTAL:	**14.10%**	**68.59%**	**17.31%**	**1**

Table 7. Income

	UN SAFE	SAFE	VERY SAFE	TOTAL
UNDER 24K	4.48%	12.82%	1.92%	19.23%
25K - 34K	4.49%	8.97%	1.92%	15.38%
35K - 49K	3.21%	19.23%	3.85%	26.28%
50K - 74K	1.28%	16.01%	3.85%	21.15%
75K - 99K	0.00%	7.05%	2.56%	9.62%
OVER 100K	0.64%	4.49%	3.21%	8.33%
TOTAL:	**22**	**107**	**27**	**156**

Tables 8 and 9 show the impact of career levels and educational background on consumers' attitudes toward Internet/ E-commerce safety. For instance, the probability for a person to work in a middle level position *and* to consider E-commerce to be safe is 41.02 percent. The probability for a person to work in an entry position *and* to consider E-commerce to be safe is 14.74 percent Given that a person works in an upper level position, the probability for that person to consider E-commerce to be very safe is 30.43 percent. The probability for a person to have business education *and* to consider E-commerce to be safe is 41.66 percent. The probability for a person to have an Arts & Science degree and to consider E-commerce to be safe is 18.58 percent. Given that a person having undergraduate education in business, the probability for that person to consider E-commerce to be safe is 73.86 percent. Given that a person has an Arts & Science background, the probability for that person to consider E-commerce to be safe is 59.18 percent. Given that a person has an engineering background, the probability for that person to consider E-commerce to be safe is 66.67 percent.

Table 8. Career Level

	UNSAFE	SAFE	VERY SAFE	TOTAL
ENTRY	6.41%	14.74%	3.21%	24.36%
MIDDLE	8.97%	41.03%	10.90%	60.90%
UPPER	0.00%	10.26%	4.49%	14.74%
TOTAL:	**15.38%**	**66.03%**	**18.59%**	**1**

Table 9. Educational Background

	NOT SAFE	SAFE	VERY SAFE	TOTAL
ARTS & SCI	6.41%	18.59%	6.41%	31.41%
ENGINEER	0.64%	7.69%	3.21%	11.54%
BUSINESS	7.05%	41.67%	7.69%	56.41%
EDUCATION	0.00%	0.64%	0.00%	0.64%
TOTAL:	**14.10%**	**68.59%**	**17.31%**	**1**

HYPOTHESIS TEST

Theoretical Framework

A test of independence will be used to determine if the consumer attitudes toward Internet and /or e-commerce safety are significantly related to the selected variables. For example, we want to know if the consumer attitude toward the safety issue is strongly influenced by gender

difference. Whether the difference between male and female on their attitudes toward Internet/E-commerce safety are "large" or "small" is a question answered with the aid of the χ^2 test. The null and alternative hypotheses will be as follows:

Ho: the column variable (male or female) is independent of the row variable (consumer attitude toward safety, i.e., Not Safe, Safe, or Very Safe)
Ha: the column variable (male or female) is not independent of the row variable (consumer attitude toward safety, i.e., Not Safe, Safe, or Very Safe)

The test statistic for independence is the χ^2 test, which is stated as

$$\chi^2 = \sum \sum (f_{ij} - e_{ij})^2 / e_{ij}, \text{ where}$$

f_{ij} is observed frequency for contingency table category in row i and column j
e_{ij} is expected frequency for contingency table category in row i and column j based on the assumption of independence.

The null hypothesis will be rejected if the $\chi^2_{\text{calculated}} > \chi^2_{\text{table}}$.

Data and Model

Data were collected using a survey conducted by the authors. As a result of the survey, a sample of 156 observations was used to formulate and test the hypotheses in the study. Specifically, the impact of the following elements on Internet safety and security was examined: age, gender, race/ethnicity, employment status, income level, career level, and educational background. The study first looked at consumers' computer/Internet skills and the past experience of using E-commerce. For example, one of the tests was to determine if the experience of using E-commerce has any influence on their attitudes toward Internet and E-commerce safety.

Empirical Results

The test of independence was performed on each of the elements listed above. The χ^2 statistic was used to test the significance of independence. At the 95% level of confidence, the test results reveal that consumers' attitudes toward Internet/e-commerce safety are strongly related to some of the demographic and socioeconomic factors such as computer/Internet skills, E-commerce experience, age, gender, race/ethnicity, and employment status. Meanwhile, the attitudes toward Internet/e-commerce safety issue are independent to other factors, namely, income, career level, and educational background. Table 10 shows the summary of the test results.

CONCLUSIONS

Based on the analysis conducted in this study, it seems that consumers' attitudes toward Internet/E-commerce safety and security were affected by age, gender, race/ethnicity, employment status, income, career levels, and educational background. According to the results of the ten tests of independence, at a 95% confidence level, some of the elements chosen for this study had significant impact on the attitudes toward the Internet/E-commerce safety.

It will be the challenge of future study to uncover the specific reasons as to why consumers' attitudes are strongly affected by some factors and not so strongly affected by other factors. It is hoped that this paper can stimulate further research in the area of consumer demand studies that might generate unique insights in the consumers' attitudes toward Internet/E-commerce safety.

Table 10. Summary of the Test Results of Independence

ELEMENTS	χ^2 calculated	χ^2 table	DECISION ON Ho	IMPACT ON ATTITUDE
Skills	16.4623	9.48773	reject	Significant
Experience	10.5867	5.99147	reject	Significant
Age	16.9237	12.5916	reject	Significant
Gender	6.9056	5.9914	reject	Significant
Race	23.6085	15.5073	reject	Significant
Employment	19.1925	12.5916	reject	Significant
Income	16.5561	18.3070	fail to reject	Insignificant
Career	9.1232	9.48773	fail to reject	Insignificant
Ed. Background	6.0283	12.5916	fail to reject	Insignificant

REFERENCES

1. Abbot, Shawn. (1999). The Debate For Secure E-Commerce, Performance Computing, pp. 37- 42.
2. Desloge, Rick. (1998). Security and Privacy Are top E-commerce Issues, St. Louis Business Journal, Vol. 19, No. 4.
3. Jordensen, Lori (1998). Connection to Risk? Managing Exposures to cyberspace, Risk Management, Vol. 45, No. 2, pp. 14-19.
4. Judge, Paul C. (1998). How Safe Is the Net? Business Week, N3583, p148.
5. Koster, Erika (1999). Zero Privacy: Personal Data on the Internet, the Computer Lawyer, 14 (4), pp 7 - 23.
6. McGuire, Brian L., and sherry N. Roser (2000). What Business Should Know about Internet Security, Strategic Finance, Vol. 82, No. 5, pp 50 -54.
7. Reidenburg, J.(1999). Restoring America's Privacy in Electronic Commerce, Berkley Technology Law Journal, 14 (2), pp. 771-792.
8. Reuters (2000). Hackers Break into Microsoft's Network, http://dailynews.yahoo.com.
9. Roboff, Gary and Cheryl Charles (1998). Privacy of Financial Information in Cyberspace: Banks Addressing What Consumers Want, Journal of Retail Banking Services, Volume XX, No. 3, pp 51- 56.
10. Stevens, Michael G.(1998). How Secure Is Your computer System? The Practical Accountant, Vol. 31, No. 1, pp. 24-32.
11. Sweeney, Paul (1999). Cyber-crime's Looming Threat, Banking Strategies, V75n4., 54-59.
12. Tyler, Geoff (1999). The Internet Marketplace Or Just a Shop Window, Management Accounting, Vol. 77, No. 1, pp59-60.