

# Information Assurance in B2C Websites for Information Goods/Services

DAN J. KIM, NATARAJAN SIVASAILAM AND H. RAGHAV RAO



## INTRODUCTION

A study by Consumers Union (Tedeschi 2002) went on to expound that Internet users are fairly skeptical of websites that sell goods or give buying advice. Fraud on the Internet rose sharply in 2002, with the FBI reporting more than 48,000 complaints referred to prosecutors — triple the number of the year before. The total dollar loss of Internet fraud reported to the Internet Fraud Complaint Center in 2002 was \$54 million (IFCC/FBI 2003), compared with \$17 million the year before, but they still represent only a fraction of the crimes authorities believe are occurring (Associated Press 2003).

'The Internet's borderless nature presents new opportunities to scam artists whose reach would normally be limited and requires law enforcement agencies to work together to catch them,' US Attorney General John Ashcroft (Reuters 2003) said recently. He further added, 'These cyberswindles and dot-cons present new challenges to law enforcement.' Clearly, this represents the need for eradication of fraud and the associated apprehension on the part of online buyers, by various confidence-building measures that attest to the reliability and genuineness of online businesses. We consider information assurance to be one such powerful

measure, and this paper focuses on the extent of self-imposed efforts (rather than legally mandated) by firms toward assurance programs.

The weaknesses of information assurance in online commerce could have a considerable detrimental impact on e-commerce. Such unfavorable effects have been documented by a Yankelovich information assurance study carried out along with the American Institute of Certified Public Accountants (AICPA and Yankelovich Partners, 1997). Key findings of that study were that consumers were worried about online security; they were not sure if there was a genuine business behind the website they were interacting with; they didn't know 'if and when' they would receive the merchandise or services they ordered; they didn't like the traceability of transactions on the Internet (many want a high degree of privacy related to their personal information and transactions); and they were worried that they might become victims of electronic fraud.

There has been little research (to our knowledge) done in the area of information assurance as applied to business websites, given that websites are the keys to online transactions of consumers on the Internet. This research is an attempt to fill this gap. The main objective of this paper is to carry out exploratory/

## A b s t r a c t

Consumer fraud on the Internet is slowly mounting, resulting in appreciable monetary losses, and growing distrust of e-commerce websites. Information assurance has been proposed to be one solution to counter this, to which consumers have also been favorably receptive. We explore here the extent of adoption of such assurance among Business-to-Consumer (B2C) information goods/services websites. The main objective of the paper is to carry out exploratory/descriptive research to study the extent of assurance services in websites that provided information/digital goods or services to the consumer directly through their online presence. The paper investigates the connections between company characteristics (company type, size and reputation) and assurance service dimensions (security, privacy and business integrity) using a novel measure, the emphasis density index (EDI) of information assurance and presence of assurance service seals. This study provides some practical insights from the findings of the results.

**Keywords:** information assurance, B2C websites, information goods/services

## A u t h o r s

### Dan J. Kim

(dankim@msu.edu) is an Assistant Professor of Telecommunication, Information Studies, and Media at Michigan State University. Recently he has focused on trust in e-commerce, wireless and mobile commerce, and information security and assurance. His work has been published or is forthcoming in journals such as *Communications of ACM*, *Decision Support Systems* and *IEEE IT Professional*.

### Natarajan Sivasailam

(sivasailam\_n@yahoo.com) was formerly a graduate student at The State University of New York at Buffalo. He is now a private researcher.

### H. Raghav Rao

(mgmtrao@buffalo.edu) is a Professor of MIS at SUNY Buffalo. He is also an Adjunct Professor of Computer Science and Engineering and is co-Editor in Chief of *Information Systems Frontiers* and an Associate Editor of *ISR*, *IEEE SMC* and *DSS*.

descriptive research to study the extent of assurance services in websites that provide information/digital goods or services to the consumer directly through their online presence. There are two major research questions of the study. First, what dimensions can be identified in the information assurance in B2C websites for information goods/services? Second, are there any differences in emphasis (importance) in the assurance service dimensions in terms of company characteristics (company type, size and reputation)?

In order to answer these questions, in this study, we have developed six web assurance dimensions, which are clustered into three standard industry practice dimensions (Privacy of customer information, Security of information stored/transmitted, and Accountability or Business Integrity of the business/enterprise). In order to compare the emphasis of dimension, we developed an 'emphasis density index' of information assurance, a measure for assessing the extent of assurance implementation, in firms focusing on the information goods/services industry. Information goods include a wide range of traditionally paper-based products such as books, magazines, newspapers, journals, photographs, maps and other graphics. These are all transparent examples of products that exist as physical products but that can easily be digitized for the electronic market place (Shapiro and Varian 1998).

The study conducted in this paper has a two-fold contribution. We believe it is among the first: (a) to investigate the extent of implementation of visible assurance services in B2C e-commerce information goods/services company websites as perceived by consumers; and (b) to determine the presence of possible patterns in the extent of implementation of assurance services in such websites of selected Fortune 1000 Companies.

The paper is organized as follows. The next section discusses the background of information assurance and its dimensions. The research model and ensuing hypotheses are presented next, followed by a description of firm characteristics. The data collection, data analysis, and the results of the model are described. The study concludes with a discussion of findings and limitations.

## RATIONALE FOR ASSURANCE DIMENSIONS

The historic need for assurance has been well illustrated after the stock market crash of 1929, when the US Securities and Exchange Commission mandated that publicly traded companies have their financial statements certified by independent auditors; this was an important step forward to bring about trust among investors. There are though, however, no such assurance requirements mandated by law in the online arena for e-commerce companies, concerning privacy, security or business integrity. The sight of *privacy* violations, *security*

breaches exposing entire customer records, and poor *business integrity*, for example in terms of unfulfilled orders coupled with lax customer service only serve to compound the distrust that exists regarding this new business avenue.

Information assurance aims to improve the quality or state of being secure at situations where the consumer is not quite familiar with the background of a business (Colwill *et al.* 2001). The most widely used computer security model is the CIA (confidentiality, integrity and availability) triangle framework (Parker 1994) which addresses the fundamental concerns regarding the vulnerability of information security. Confidentiality of information deals with the intentional or unintentional unauthorized disclosure of information. Integrity of data is the quality or state of being whole, complete and uncorrupted. Availability ensures the reliable and timely access to information by the appropriate personnel (Whitman and Mattord 2004).

Although the CIA triangle is founded on three desirable dimensions of computer information security, the heralding of the e-commerce era and its present-day needs have made the CIA framework inadequate, because they are limited in scope and cannot encompass the constantly changing Internet environment. Therefore, based on the available literature, we have developed six web assurance dimensions: security, transaction integrity, authenticity, privacy compliance, business integrity and financial settlements.

According to the Yankelovich study (AICPA and Yankelovich Partners 1997), security of information stored/transmitted to and from the company' computer systems, privacy of customer information, and accountability or business integrity of the business/enterprise are important factors that influence a Business-to-Consumer (B2C) e-commerce purchase. In the Yankelovich study, three dimensions are considered as targets of assurance service by the AICPA standard WebTrust.

Based on standard industry practices and norms, security, transaction integrity and authenticity of parties have been clustered in to one group called 'Security'; Business integrity and financial settlements are grouped as 'Business integrity', and 'Privacy' is retained as such. Thus, this study will be mainly considering the three 'dimensions' of *Security*, *Privacy* and *Business Integrity*. These dimensions will form the basis of consumers' evaluation of e-commerce websites on information assurance.

Table 1 summarizes these dimensions, key issues addressed, potential remedies as well as sources.

## Security

Information security on the Internet pertains to the safeguarding of proprietary/personal data from unauthorized/inadvertent access/disclosure. Though

Table 1. Information assurance dimensions

<i>Area of assurance provided</i>	<i>Issues addressed</i>	<i>Potential remedy and assurance seal services</i>	<i>Sources</i>	
Security	Security	-Unauthorized access -Distributed denial of service attacks -Malicious programs/Malware (Viruses, worms, spyware) -Man-in-the-middle attack	-Proper password generation guidelines -Prompt application of software patches -Intrusion detection software -Firewalls (Proxy servers) -Traffic management software -Back-up servers & IP numbers -Anti virus/anti spyware -Seals like Verisign, Thawte, WebTrust, BBBOnline Reliability, etc.	(Miyazaki and Krishnamurthy 2002, Chellappa and Pavlou 2002, Foo <i>et al.</i> 1999, Ratnasingham 1998a, 1998b, Gritzalis and Gritzalis 2001)
	Transaction integrity	-Alteration of documents -Deletion of documents -Duplication of documents -Diversion/non-receipt of documents	-Software controls -Encryption -Electronic sender-receipts	(Colwill <i>et al.</i> 2001, Foo <i>et al.</i> 1999, Ratnasingham 1998a, 1998b, Gritzalis and Gritzalis 2001)
	Authenticity of parties to transaction	-Identity theft -Proof-of-origin -Authentication - Man-in-the-middle attack	-Digital signatures/certificates(e.g., Verisign, Thawte, KPMG, etc) -Identity Seals -Encryption -Key management -Virtual private networks -Intrusion detection system	(Colwill <i>et al.</i> 2001, Hawkins <i>et al.</i> 2000, Foo <i>et al.</i> 1999, Ratnasingham 1998b, Gritzalis and Gritzalis 2001)
Privacy	Privacy compliance	-Unauthorized access -Inappropriate usage	-Software/electronic controls -Physical controls -Managerial controls/restrictions to access data that could aid in profiling -Privacy seals like TRUSTe, BBBOnline, WebTrust	(Cranor 1999, Benassi 1999, Pugliese 2000, Chellappa and Pavlou 2002, Foo <i>et al.</i> 1999, Ratnasingham 1998a, 1998b, Gritzalis and Gritzalis 2001)
	Business integrity	-Grievance redressal -Returns and refunds -Prompt delivery of goods/services	-Comprehensive audit of business practices -Role of arbitrator/mediator -Seals like BBBOnline reliability, WebTrust	(Pugliese 2000, Miyazaki and Krishnamurthy 2002, Ratnasingham 1998b)
Integrity	Financial settlements	-Safe, private, trustworthy -Diversion of payments -'Breach of contract' -Unauthorized usage of financial/payment data -Non-repudiation of transactions/contracts	-Secure sockets layer -Macropayments (First virtual, CyberCash, BankNet echeque, Digicash, Mondex -Micropayments (e-coins, e-wallets) -Escrow services	(Miyazaki and Krishnamurthy 2002, Lansing and Hubbard 2002, Buck 1996, Dai and Grundy 2003)

there are various advancements in security technologies, the specter of websites being compromised because of lax security procedures is very common. Companies need to employ encryption during data transmission, and need consumer data to be stored in secure environments that are free from external/internal tampering. Statistics from

the federally funded Computer Emergency Response Team (CERT) at Carnegie Mellon University show that a total of 137,529 security incidents<sup>1</sup> were reported for the year 2003 (<http://www.cert.org/stats>). Examples of security exposures abound in the popular press. For example, hackers gained access to credit card data of

customers of CDUniverse.com and Creditcards.com, and even published that information on a public website in the former case.

Standard practices in the security arena include the disclosure of information about registration; identification through usernames/passwords; usage of industry-standard encryption to transmit sensitive data such as financial information, social security number, etc.; timely application and or adoption of software patches; deployment of firewalls or intrusion detection software, usage of Digital IDs or Certificates; methods to communicate to customers if their data had been compromised, and redressal of issues about security.

## Privacy

Privacy violations often occur. The Federal Trade Commission took to task Toysmart.com for having collected information from children, and selling customer private information in violation of privacy laws (COPPA — Children's Online Privacy and Protection Act) and its own privacy policy.

The *Oxford English Dictionary* defines 'privacy' to be 'a state or condition of being free from public attention as a matter of choice'. In the online arena, the core principles of privacy include: disclosure of information collection, and dissemination practices; providing the consumer with a choice with respect to how their information may be used; measures to protect the integrity of personal information and preclude their unauthorized disclosure, and protecting children — compliance with governmental laws such as Children's Online Privacy and Protection Act (COPPA).

Businesses are expected to disclose their information privacy practices prominently on their sites, including the specific types of data that are collected both actively and passively; how that information may be used; possible third-party dissemination; how individuals may restrict the usage of their information and correct any factual errors in the same; usage of cookies or other electronic technologies that could either identify them personally or otherwise; contact information to resolve questions/concerns about privacy policies; how grievances may be redressed, and possible third-party roles (Pugliese and Halse 2000; Ware 2002). Physical, electronic and managerial measures should be instituted to guard against inadvertent disclosures, and guard the integrity and confidentiality of consumer data.

## Business integrity

As mentioned before, consumers reported a total loss of \$54 million to the IFCC, which was essentially due to various kinds of fraud, with auction fraud involving cases of non-deliverable merchandise being the maximum.

Further, as part of 'Project Toolate.com', the FTC took action against e-retailers who did not ship products in a timely fashion, in violation of various laws. Again, accountability or business integrity of e-retailers needs to be reinforced because of such incidents.

The statistics furnished by the IFCC/FBI do not convey a pretty picture of the business integrity of some e-commerce firms. Unfortunately, this creates fear in the minds of the consumer about even honest, albeit unknown, firms. Assurance programs that attest the business integrity of firms should follow the below-mentioned guidelines as a minimum:

- truthful and accurate communications without deceptive marketing;
- upfront disclosure and forthrightness about various business policies, such as refunds, returns, exchanges, taxes, shipping charges, etc. and information about the business and its products and services;
- adoption of practices that aim to preserve the integrity of customer data, providing customers with choices of how their data may or may not be used, and preventing the data from falling in to the wrong hands by way of physical, electronic and managerial measures;
- customer satisfaction — the merchant should aim to be prompt in resolving queries; and
- redress grievances in a timely and responsible manner.

## RESEARCH MODEL AND HYPOTHESES

This study investigates the connections between company characteristics (company type, size and reputation) and assurance service dimensions (security, privacy and business integrity) by the emphasis density index of information assurance and presence of assurance service seals. Figure 1 presents the basic conceptual framework underlying the emphasis density index of information assurance and assurance seal services explaining the emphasis of assurance dimensions by firm characteristics (industry type, firm size and reputation) that form the basis of this study.

### Firm characteristics

*Industry type.* An earlier study (Sivasailam et al. 2002) focused on the extent of assurance in the B2C sector in such physical goods as books, DVDs, etc., and found that there were significant differences in the extent of implementation among various industries, and the various dimensions involved in assurance. The current study focuses on B2C companies that provide information goods/services over the web, as opposed to physical goods and we expect similar significant differences across industries.

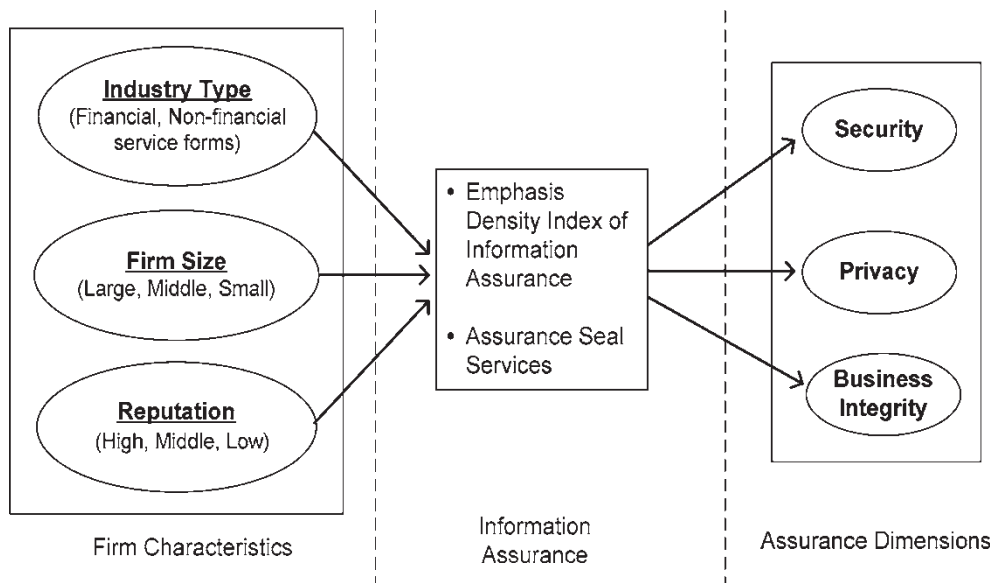


Figure 1. Research model

Within the group of industries that sell information goods, two types of industry domains are considered in this study: financial services and non-financial services. We define a financial services domain as consisting of those industries that are related to monetary transactions such as banks and insurance companies while a non-financial services domain consists of industries which are not directly related to monetary transactions but are strongly related to information assurance service such as computer software and data services, hospitality. To this effect, we chose four industries: Banks (account balances could be viewed, fund transfers effected, etc), Insurance companies (insurance quotes obtained, premiums paid, etc), Hospitality (hotel room reservations could be made, etc), and Computer software and data services (commercial software could be bought and downloaded, upgraded, etc.). Financial and non-financial services firms are likely to exhibit different assurance characteristics because the risk associated with each for the consumer is different. This leads to the following hypotheses.

H1a: Companies (e.g., banks and insurance) that deal with monetary transactions are more concerned about security than other companies (e.g., computer software and hospitality).

H1b: Companies that deal with monetary transactions are more concerned about privacy than other companies.

H1c: Companies that deal with monetary transactions are more concerned about business integrity than other companies.

**Firm size.** Fundamental and seemingly simple things as choosing easily guessable passwords could result in very far-reaching consequences that compromise entire customer databases. For example, Greg Shipley, Director of Consulting of Neophasis, a Chicago-based security company says, 'Just about every company that we have

gone in to, even large multinationals, has a high percentage of accounts with easily (cracked) passwords.' He adds, 'We have yet to see a company whose employees don't pick bad passwords' (Lemos 2002). As such, it is conceivable that firm size is irrelevant as far as information assurance implementations go. This is in contrast to earlier research in information systems, for example, that firm size effects stock market reactions to IT investments or that consumers' trust is positively influenced by size of a company (Jarvenpaa *et al.* 2000). However we articulate the following hypotheses following prior research:

H2a: Bigger companies are more concerned about security than smaller ones.

H2b: Bigger companies are more concerned about privacy than smaller ones.

H2c: Bigger companies are more concerned about business integrity than smaller ones.

**Reputation.** Assurance services are aimed at situations where the consumer is not quite familiar with the background of a business, and may have to look for elements that 'certify' the trustworthiness of the business to provide assurance. In the physical world, we feel comfortable walking in to a Wal-Mart, or surfing to WalMart.com, and buying things there. On the other hand, one may not be so sure about classicguitars.com. Here, we see that Wal-Mart is a long standing firm of high reputation, that has stood the test of time of honoring its policies and can be counted upon, if things went wrong or if we were not satisfied or for some reason simply wanted to return the product. Wal-Mart has several information assurance mechanisms in place that are available for the public to peruse. On the other hand, we do not know how the guitar site may respond under

similar circumstances, because of the simple fact that not many people may be familiar with this company that has an unknown reputation, and hence the public may be reluctant to trust this company (Jarvenpaa *et al.* 2000; Mayer *et al.* 1995). Further, elements of information assurance might be missing in the case of the guitar company. This leads to the following hypotheses.

H3a: More reputable companies are more concerned about security than less reputable ones.

H3b: More reputable companies are more concerned about privacy than less reputable ones.

H3c: More reputable companies are more concerned about business integrity than less reputable ones.

### Construct operationalization

*Industry classification.* All the companies chosen in this study belong to the B2C industry (Sivasailam *et al.* 2002), are involved with information goods/services, and have an online presence available for consumer transactions. More specifically, we focus on banks, and insurance industries in the financial services domain and computer software and data services and hospitality in the non-financial services domain. We selected the list of banks and insurance companies, computer software and data services, and hospitality using the industry index of *Fortune* magazine ([www.fortune.com](http://www.fortune.com)).

*Fortune rankings as a proxy for size.* Fortune rankings are assigned based on a company's revenues. This measure has been chosen for our study in line with previous research that studied size in the context of trust (Jarvenpaa *et al.* 2000). Fortune rankings adequately capture the size factor. Size was further classified into three types in the following manner: The top 1–250 firms in the Fortune list were the large firms (approx annual revenue >\$7.5 billion), the next 251–1000 firms were the medium firms (annual revenue >\$1.0 billion and <\$7.5 billion) and the rest of the firms that did not appear in the fortune 1000 list were the small firms (less than \$1.0 billion).

*Google importance rankings as a proxy for reputation.* Reputation rankings provided by the search engine Google.com for each of the companies that had an online e-commerce presence were collected. Reputation was also further classified into three types based on the Google rankings: high level (8–9), mid level (7) and low-level reputation (1–6) based on Google rankings (Jarvenpaa *et al.* 2000). This system of rankings was chosen because we found that the median ranking was seven, and to ensure proper group distribution, we categorized the rankings in to three categories as described above.

### Assurance seal services

Assurance seal services are based on the idea of making the vulnerable entity (the consumer) more comfortable with the transaction and ensuring that the other (the company) follows through on its promises. The purpose of assurance seals is to provide assurance to consumers that a website discloses and follows through with its operating practices, that it handles payments in a secure and reliable way, that it has certain return policies, or that it complies with a privacy policy that says what it can and cannot do with the collected personal data (Koreto 1997; Castelfranchi and Tan 2001).

Assurance seal service was first started by the Better Business Bureau (BBB) system, which was founded in 1912 and is today supported by 250,000 local business members in the US. The stated mission of the BBB system is 'to foster fair and honest relationships between businesses and consumers, instill consumer confidence and contribute to an ethical business environment'. BBB Members are subject to standards set by the Bureau, and have to adhere to them to be continuously certified as a Member. These standards pertain to customer service, policy adherence (e.g., returns, exchanges), and dispute resolution among a plethora of other requirements.

The best known assurance seal services nowadays are WebTrust, TRUSTe, Verisign, Thawte and BBBOnline. Services vary widely in what they offer. Nonprofit assurance services like BBB and TRUSTe merely evaluate their client's privacy policy to make sure that it conforms to the set of assurance requirements established by the service. They do not provide advice or consulting. WebTrust uses licensed public accountants who complete special training as to how a WebTrust seal is issued. Verisign provides digital ID services, which certify the electronic merchant's authenticity. Thawte offers highly authenticated SSL (Secure Sockets Layer) and code signing certificates to secure all online data transmissions. Other service like BizRate.com and Gomez.com rely on the ratings of consumers who have bought products or services at that site. The Online Privacy Alliance is a group of corporations and associations that have come together to uphold self-established privacy standards.

To summarize, Verisign, Thawte, WebTrust and BBBOnline Reliability offer security assurance services. TRUSTe, BBB, and WebTrust provide privacy assurance services (Gray and Debrecey 1998). The Better Business Bureau focuses more on privacy and business integrity than security, while Verisign provides digital ID services only. There is only one comprehensive assurance program — WebTrust — that addresses consumer concerns in the security, privacy and business practices in a comprehensive fashion.

Based on a detailed literature study of the topic of assurance dimensions, the survey instrument was developed to enable operationalization of the critical

features of (a) security, (b) privacy and (c) business integrity. In order to measure the strength of each assurance service dimension and to use the emphasis-density index that we had developed for this study, individual website features were the targets of our scrutiny/research. Queries regarding critical features were codified in the form of questions and measured using dichotomous scales (see Table 2). For purposes of instrument validity and reliability, a panel of experts reviewed and revised the instruments and a pilot test was conducted with a small number of sites prior to the collection of data for the field test.

## DATA COLLECTION, ANALYSIS AND RESULTS

The majority of data have been collected from websites of Fortune 1000 Companies in four industries: banks, insurance companies, computer software and data services, and airline/hospitality. Among Fortune 1000 companies, there were only 81 companies that met certain conditions for this study; i.e., they sold information goods/services as opposed to physical goods through their websites, were required to be among the four sectors (i.e., banking, insurance, computer software and data services, and airlines/hospitality) and must have had an online commerce website. The Appendix contains a list of the firms sampled. The data for a total of 81 websites were collected in the form of responses to questions that were posed to a group of graduate level e-commerce students with regard to transaction websites (please see Appendix). Each website was evaluated by two students. Further, to check the validity of the data collected, following Hu (2001), the authors randomly chose 25% of the responses to verify the accuracy of the student responses (Hu *et al.* 2001).

For coder reliability, we calculate Cohen's Kappa,<sup>2</sup> (Riffe *et al.* 1998) which is used for nominal-level measures and all disagreements are assumed to be equivalent (Cohen 1960). The total number of items for coding is 18, which are as follows — 6 items for security, 7 items for privacy, and 5 items for business integrity. Since a total of 81 websites from four sectors were evaluated, a total of 1,458 independent coding decisions were made by coders. Out of the 1,458 coding decisions, coders disagreed in 159 instances. So, the simple percentage of agreement — the percentage of agreement among two or more coders — is 89%. The acceptable level of necessary agreement is dependent on the type of research conducted, but a minimum level of 80% is usually an acceptable standard (Riffe *et al.* 1998). The calculated Cohen's Kappa is 85.46%, which can be interpreted as the agreement that has been achieved as a result of the category definitions and their diligent application by coders, after a measure of the amount of chance agreement being removed.

## Emphasis density index for assurance services

To measure the strength of each assurance service dimension, we developed a novel 'emphasis-density index' of websites for security, privacy and business integrity dimensions. The emphasis-density index refers to the ratio of the number of features a website possesses, to the total number of features in each dimension. This density represents the extent to which the website emphasizes the specific assurance service dimension. For example, based on the survey items for assurance service as shown in Table 3, if a website has 5 features out of 7 security survey items, the emphasis-density index of security dimension would be  $5/7$ , which is 0.714. The density 0.714 is the percentage of features that the website possesses.

Table 3 shows densities of each dimension by company type, size and reputation. According to the summarized mean density in Table 3, banks, insurance industries, computer software and data services, and hospitality have 0.693, 0.608, 0.556, and 0.532 security densities respectively. The mean densities of firms in the financial services domain (i.e., banks and insurance industries) and in the non-financial services domain (i.e., computer software and data services and hospitality) are 0.651 and 0.544 respectively. It can be interpreted that banks, insurance industries, computer software and data services, hospitality, financial, and non-financial domain firms emphasize security according to the density. Figure 2 plots the means of densities of the three dimensions for each company characteristic (company type, size, and reputation).

## Comparison of assurance dimensions

In order to test the mean differences among the web service assurance dimensions within each company characteristic (company type, size and reputation), one-way ANOVA (analysis of variance) and mean comparison tests were conducted using SPSS ver.10. Table 4 and the first part of Table 5 represent F-ratios of ANOVA and t-test results for each dimension, respectively. The results show there is evidence that the mean density differs significantly among company types (financial vs. non-financial firms) for the business integrity dimension, and among companies of different reputations for security, privacy, and business integrity dimensions. Further, F-test results regarding company size and the three assurance dimensions are not significant. This implies that companies of different sizes emphasize the various dimensions more or less equitably.

In addition to determining that differences exist among the means, we wish to know which of these means differ. In other words, even if the overall tests of business integrity with company types and all three dimensions with company reputation are significant, we do not know

Table 2. Information assurance features

**Security:** List any security assurance service(s) that the website utilizes. Example – Verisign, Thawte, WebTrust, BBBOnline Reliability, etc.

1.1 Does the website have a security policy, and, are links to the policy provided on most web pages?	Any e-commerce site that collects personally identifiable information should have a robust security infrastructure. When the salient features of this are explained in the form of a 'security policy', and displayed on the website, this is expected to encourage confidence on the part of the user, and make the website more 'trustable'.
1.2 Does the website disclaim it's security measures i.e., provide a disclaimer?	Security policies tend to increase trust. For example, Amazon.com says that, 'We guarantee that every transaction you make at Amazon.com will be safe.' On the other hand, a disclaimer that a website may not be liable for any breaches of security does not prove helpful in making a user part with sensitive information.
1.3 Does the website employ encryption or use SSL technology to handle sensitive information?	The usage of encryption, firewalls, etc protects the security of personal information, as opposed to not using them would be tantamount to inviting disaster.
1.4 Does the website have a safe shopping guarantee?	A safe shopping guarantee, like the one provided by Barnes & Noble protects customers from any unauthorized charges arising out of a customer's usage of the credit card on it's website. This reassures customers that they could safely trust the website with their credit card information, and that they need not endure the hassle of fraudulent charges.
1.5 Does the website use Physical, Electronic and Managerial measures to safeguard your information?	The usage of Physical, Electronic, and Managerial measures may be reasonably expected to increase the security and integrity of data, and protect it from inadvertent or unauthorized disclosures. (Example – Apple.com 'How we protect your personal information')

**Privacy:** List any privacy assurance service that the website utilizes. Example – TRUSTe, BBBOnline Privacy, WebTrust, Online Privacy Alliance, etc.

2.1 Does the website have a privacy policy, and, are links to the policy provided on most web pages?	A privacy policy clearly outlines the information collection practices of a website. It spells out what is collected, what is not, how that information is used, what sort of choices the consumer has over the usage of that information, the ability to maintain the accuracy of that data, etc. By stating this clearly upfront, one will be less apprehensive of his/her privacy being violated and be more confident about the site's usage of personal information
2.2 Does the website collect details such as IP number, browser, operating system, time and date of visit, or such seemingly unidentifiable information?	Various websites log such things as IP numbers, browsers used, operating system of the querying computer, time/date of visit, encoding language of the browser, or such apparently personally unidentifiable information. However, with some serious efforts, a person can be identified, and can be profiled by his/her surfing habits.
2.3 Are you able to correct inaccuracies, and control the usage of personal information by the website?	The ability to correct inaccuracies, and control the usage of information is central to maintaining the integrity of customer data. A sound privacy policy should have provisions for them.
2.4 Does the website use cookies? If so, are they temporary or persistent?	Cookies are a product of the dot.com revolution. While temporary cookies may be harmless, persistent ones could prove powerful in profiling web surfers, with their surfing habits being closely monitored, and privacy being violated. The case of DoubleClick illustrates the abuse of cookies.
2.5 Is the website P3P compliant? (Refer to the website of World Wide Web Consortium - <a href="http://www.w3.org/P3P">http://www.w3.org/P3P</a> )	The World Wide Web Consortium (W3C) has recently developed specifications for the Privacy for Platform Preferences Project (P3P), by which a Consumer wields greater control over the information collected by a website – they may specify the sites whose cookies they wish to be blocked, and based upon the privacy policies of websites, allow them to set cookies/collect information, among other things.
2.6 Does the website share your information? If so, is it in a personally identifiable manner or anonymous fashion?	Consumer privacy laws, till date, follow the 'opt-out' philosophy, by which users have to take the initiative of letting companies know that they wish for their personal information not be shared with other entities; thus, the onus is placed on the consumer, rather than the company that collects/possesses such information. An 'opt-in' policy would be more privacy-friendly in the way that only those who desire to have their information shared would find so.
2.7 Does the website store any personally identifiable information other than your username? (Example – credit card details, address, phone number, etc)	The storage of personally identifiable sensitive information such as credit cards leaves the possibility that there may be an inadvertent disclosure of such data, and thus, resulting in potential misuse. To circumvent this, certain companies do not store such information, and only retain the bare minimum to facilitate login, and such activities.

Table 2. Continued

**Business Integrity:** List any business integrity assurance service that the website utilizes. Example – BBBOnline, Reliability, WebTrust, etc.

3.1 Does the website have a Frequently Asked Questions (FAQ) section, outlining information about the usage of the website?	A clear and comprehensive FAQ section dispels various doubts that a potential customer may have about a websites policies, makes these policies transparent, and hence increases the possibility of a sale
3.2 Does the website provide an order number or confirmation number so as to uniquely identify and track your transaction?	In a POS (Point of Sale) transaction, the buyer gets a receipt that details the transaction. On the other hand, in an online sale, the only proof of payment could be realized in the form of a unique order/confirmation number for a transaction, by which transactions could be traced and/ audited. This is essential to track the progress of a transaction, amend any preferences directly related to the transaction, and prevent repudiation
3.3 Does the website provide information regarding resolving customer queries/complaints?	Providing a comprehensive mechanism to resolve customer complaints/grievances greatly reduces the dissatisfaction and the resulting mistrust if for some reason, a customer is not satisfied with a product/ service, and wishes to rectify the same.
3.4 Does the website provide information in the form of email address, Phone/FAX, Mailing address to contact the company?	The Consumers Union study highlighted that consumers were highly skeptical of websites, and that they wished to see the physical address at which a company was located; this would give the buyer peace of mind, because this conveys the impression that the business behind a website is a legitimate company, and that it is not a phony one/ fly-by-night operation.
3.5 Does the website outline a 'refunds policy'?	As highlighted before, various policies such as privacy, security, when clearly disclosed on websites tend to promote confidence. Similar is the case with such things as warranty, returns, refunds, etc. This piece of information may prove to be decisive in winning/losing a customer

Table 3. Mean density of assurance service dimensions

	<i>Company types from Fortune industry classifications</i>						<i>Company size (Fortune ranking)</i>			<i>Reputation (Google ranking)**</i>		
	<i>BK</i>	<i>IN</i>	<i>CD</i>	<i>HO</i>	<i>FIN</i>	<i>NFIN</i>	<i>Large (1–250)</i>	<i>Mid (251–1000)</i>	<i>Small (beyond 1000)</i>	<i>High (8–9)</i>	<i>Mid (7)</i>	<i>Low (5–6)*</i>
no. of firms	20	20	20	21	40	41	26	28	27	18	35	26
Security	0.693	0.608	0.556	0.532	0.651	0.544	0.558	0.583	0.642	0.435	0.667	0.654
Privacy	0.414	0.414	0.367	0.422	0.414	0.395	0.401	0.388	0.423	0.389	0.449	0.363
Business Integrity	0.653	0.610	0.686	0.838	0.631	0.762	0.669	0.700	0.726	0.622	0.663	0.846

Note: BK- Bank, IN-Insurance, CD- Computer software & Data services, HO-Hospitality, FIN (BK+IN), NFIN (CD+HO).

\* No firm had a Google ranking below 5, \*\* Google did not rank two companies.

which specific groups differ from each other. Thus, to find out which specific groups of company types, size and reputation are different, we conducted planned (a priori) contrast tests with the assumption of unequal variances (Tabachnick and Fidell 1996). A planned comparison test for means allow us to reject the null hypothesis that, within the assurance service dimension, the various company characteristics (industry, size and reputation) are independent of each other. Table 5 presents the results.

The contrast test results show that there are statistically significant differences regarding business integrity assurance dimension between the various sectors of banks and hospitality, computer software and data service and insurance, and hospitality and insurance firms. There are differences in security concerns between low-, mid- and

top-level reputation firms; along with privacy concerns between mid-level and top-level reputation firms. In business integrity assurance, there are significant differences between the highest reputation firms and the mid- and lower- level reputation firms.

Table 6 summarizes all hypotheses test with conclusions (accept or reject).

In addition to the above hypotheses, we conducted an analysis based on the number of assurance service seals. The results are presented in Tables 7 and 8.

Based on the Chi-Square tests, we note that only Privacy-Company type is statistically significant. This result can be interpreted as follows: there are significant differences regarding the number of seals related to privacy concerns between company types (financial and non-financial service firms).

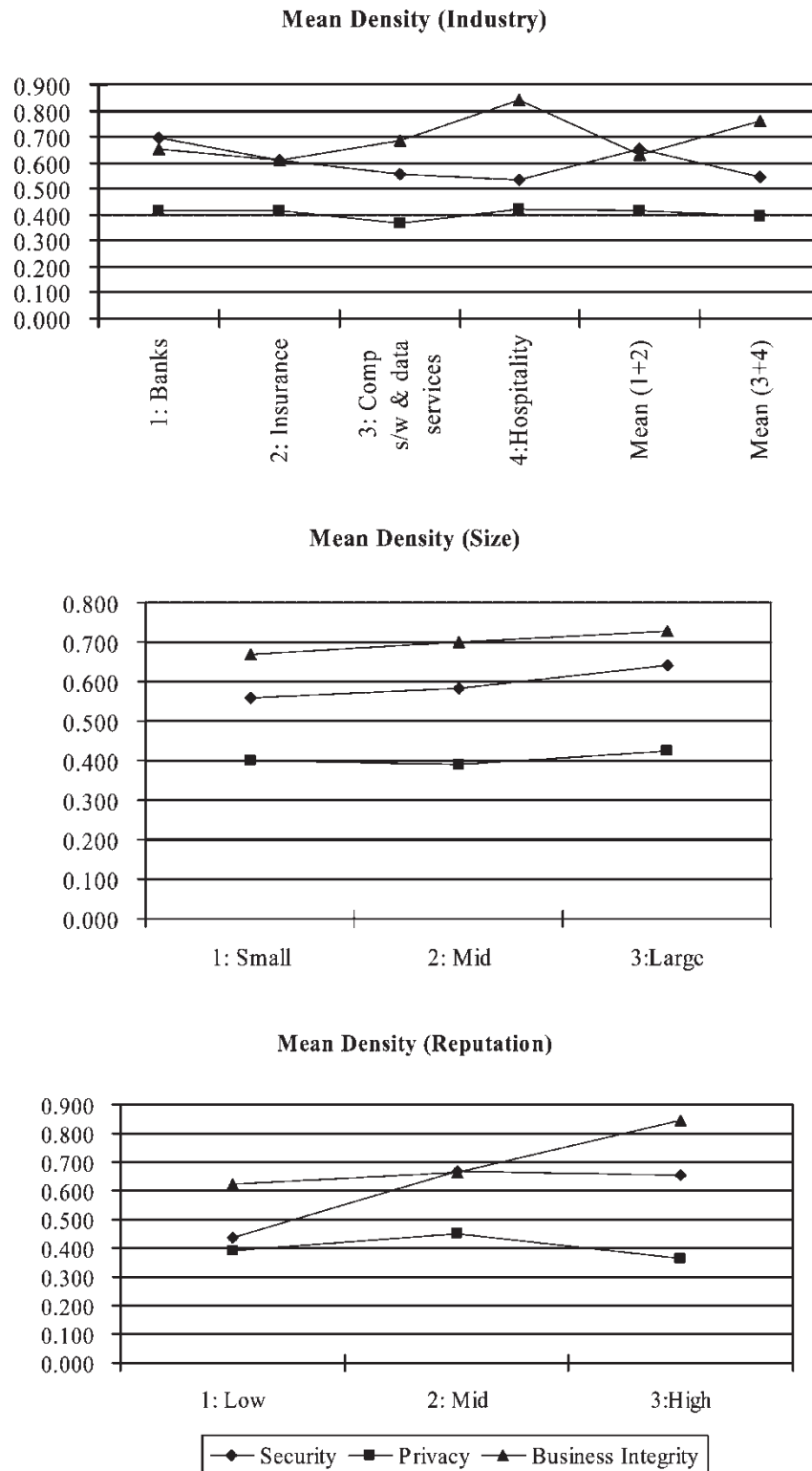


Figure 2. Mean densities of three dimensions for company characteristics

**DISCUSSION AND CONCLUSION**

Everyday, we keep hearing of bad experiences of the common consumer on the Internet. An earlier study on efforts of B2C sites selling physical goods showed that efforts toward seeking assurance were very much

wanting (Sivasailam *et al.* 2002). Various other studies have shown that consumers are otherwise also skeptical of privacy, security and the lack of ethics/accountability on the web, and would favorably be receptive to assurance provided by third parties. The results of the study indicate that firms need to do more to seek assurance

Table 4. Summary F-ratios of ANOVA analysis

	<i>Company types (FIN vs. NFIN)</i>	<i>Company size</i>	<i>Reputation</i>
Security	1.393 (0.242) <sup>1</sup>	0.577 (0.564)	5.022***(0.009)
Privacy	0.000 (0.987)	0.341 (0.712)	2.617* (0.080)
Business integrity	11.854*** (0.001)	0.395 (0.675)	9.471*** (0.000)

Notes: <sup>1</sup> F-Ratio (significance).

\* significant at the 0.1, \*\*\* significant at the 0.01 level.

Table 5. Summary t-statistics contrast tests

<i>Contrast</i>	<i>Mean difference</i>	<i>Standard error</i>	<i>t-stat</i>	<i>Significant (2-tailed)</i>
Mean comparison test (Financial vs. Non-Financial firms)				
Security	0.076	0.065	1.180	0.242
Privacy	-0.000	0.036	-0.017	0.987
Business integrity	-0.165	0.048	-3.443***	0.001
Company types * Business integrity				
Bank-Insurance	0.01000	0.06387	0.157	0.876
Bank-Computer	-0.10000	0.07298	-1.370	0.179
Bank-Hospitality	-0.21810	0.07155	-3.048***	0.004
Computer-Hospitality	-0.11810	0.07081	-1.668	0.103
Computer-Insurance	0.11000	0.06304	1.745*	0.090
Hospitality-Insurance	0.22810	0.06137	3.716***	0.001
Reputation * Security				
Low-Mid	-0.23143	0.09536	-2.427**	0.023
Low-Top	-0.21860	0.09844	-2.221**	0.035
Mid-Top	0.01283	0.05907	0.217	0.829
Reputation * Privacy				
Low-Mid	-0.06006	0.05094	-1.179	0.247
Low-Top	0.02608	0.04720	0.552	0.586
Mid-Top	0.08613	0.03388	2.542**	0.014
Reputation * Business integrity				
Low-Mid	-0.04063	0.05707	-0.712	0.481
Low-Top	-0.22393	0.0566	-3.954***	0.000
Mid-Top	-0.18330	0.04838	-3.789***	0.000

Note: \* significant at the 0.1, \*\* significant at the 0.05, \*\*\* significant at the 0.01 level.

Table 6. Summary of hypotheses test

<i>Hypothesis</i>	<i>F-ratio</i>	<i>Significant</i>	<i>Conclusion<sup>1</sup></i>
H1a: Security*Company type	1.393	0.242	Reject
H1b: Privacy*Company type	0.000	0.987	Reject
H1c: Business integrity*Company type	11.854**	0.001	Accept
H2a: Security*Size	0.577	0.564	Reject
H2b: Privacy*Size	0.341	0.712	Reject
H2c: Business integrity*Company size	0.395	0.675	Reject
H3a: Security*Reputation	5.022***	0.009	Accept
H3b: Privacy *Reputation	2.617*	0.080	Accept
H3c: Business integrity*Reputation	9.471***	0.000	Accept

Note: Accept or Reject null hypothesis with 0.1 significance level.

\* significant at the 0.1, \*\* significant at the 0.05, \*\*\* significant at the 0.01 level.

Table 7. Number of assurance service seals

	Company types from Fortune industry classifications						Company Size (Fortune ranking)			Reputation (Google ranking)		
	BK	IN	CD	HO	FIN	NFIN	Large (1–250)	Mid (251–1000)	Small (beyond 1000)	High (9–10)	Mid (7)	Low (5–6)
no of companies	20	20	20	21	40	41	26	28	27	18	35	26
Security	2	2	4	5	4	9	4	5	4	4	8	1
Privacy	0	4	9	4	4	13	5	4	8	8	8	1
Business integrity	0	0	1	1	0	2	0	0	2	2	0	0

Note: BK- Bank, IN-Insurance, CD- Computer software & Data services, HO-Hospitality, FIN (BK + IN), NFIN (CD + HO).

Table 8. Result of Pearson chi-square tests

	Company types (FIN vs. NFIN)	Company size (Fortune ranking)	Reputation (Google ranking)
Security	2.146 (0.146) <sup>1</sup>	0.107 (0.948)	2.621 (0.270)
Privacy	5.508907 (0.064*)	3.163 (0.531)	4.241 (0.374)
Business integrity	2.001 (0.157)	4.338 (0.114)	4.183 (0.124)

Note: <sup>1</sup> Chi-Square Value (p-value).

\* significant at the 0.05 level, \*\* significant at the 0.01 level.

for their websites. Statistically, we found significant differences in implementations of various assurance dimensions involving various classifications. This leads us to observe some interesting patterns:

- Privacy assurance was significantly more pronounced in mid-level firms than high reputation firms, which is different from the earlier study (Sivasailam *et al.* 2002) in which large companies were found to have placed more emphasis on privacy seals than mid-size or small firms. Here, we believe that the mid-level ones are more pronounced in privacy efforts because the top-level firms may be banking on their longevity to demonstrate their commitment to uphold consumer interests.
- Mid-level and high reputation companies were found to attach more importance to security efforts than those at the lower level. This is predictable, because a security breach to a top/mid tier company could cause more damage through unfavorable publicity than a company that is relatively lower in the ladder.
- We note that the emphasis on business integrity is markedly high in the hospitality industry, and is significantly more when compared to the banks and insurance companies. This observation seems to be puzzling, considering the fact that banks and insurance companies should have a higher emphasis on this element, because a consumer's financial stakes are involved here rather than a simple one-off reservation in a hotel or a holiday resort company. Nevertheless, this presents the case for more efforts on the part of

financial companies to take more steps in providing assurance along these lines. In addition, we found that top-level firms were more interested in business integrity than low/mid level companies. This though, is different from the earlier study in which we found no differences involving business integrity assurance efforts across a wide variety of companies irrespective of industry type or company size or reputation.

From the above statistical findings, we have concluded that while there are some random patterns of assurance in each of the dimensions that are the object of our study, there is no strong suggestion of uniformity of application of assurance measures (with respect to the three assurance dimensions) or a deliberate policy of implementing/seeking assurance, both within individual websites, and also those within particular industry types/domains. For example, while some websites have felt the need for procuring digital IDs, they have not felt the necessity of seeking assurance in privacy or business integrity. Even where websites have not felt the need for external assurance certifications (such as TRUSTe, BBBOnline), the extent of self-imposed assurance mechanisms have widely varied within websites and industries. For example, BancWest Corporation and Comerica are both banks that are part of the study; their individual emphasis-density indexes (EDIs) stand in stark contrast against each other — in the security dimension, while the EDI of the former is zero, the EDI of the latter is one; which means that while BancWest Corp's website was totally devoid of any assurance measures, Comerica's

website had all of the assurance measures that we had surveyed, in spite of the fact that both did not carry any external assurance certifications. We should emphasize that these statistics were obtained during the period of Jan 2002 to Mar 2002, and their status may have well changed subsequently. Under such circumstances, we believe that a limitation of this analysis of web seals is that there are not enough firms adopting assurance service seals. There are at least two interpretations for this: the current awareness of assurance practices and those of web seals is still at an early stage in the market and companies in the service area dealing with information goods do not think they need assurance and seal services. More research needs to be done in this area.

So, what should consumers be looking for in a website? While trying to answer this question, one should look at it from the perspective of a person who would shop at a well-established, long existing brick-and-mortar business that has clearly defined, well furnished and prominently visible policies on its property. With that as a reliable background, at a basic level, the website must carry a security policy, privacy policy and policies relating to returns, warranty and information to contact customer service. Table 2 provides a comprehensive list of the features/information assurance mechanisms that are to be assessed in an e-commerce website.

Although the findings of this study provide interesting insights for information assurance in B2C websites for information goods/services, this study has several limitations. First, this study considered two types of domains (financial and non-financial service). Since there is no clear-cut definition of financial and non-financial service domain, we had developed our own definition and classified the firms based on that. Second, the data for this study included only a limited group of companies and sectors. All the information that was collected was only from what was provided on the websites, and did not involve any one-on-one contact with the website (i.e., telephone calls, email, web chat or postal mail). This may create the impression of a strong sampling bias. However, this is important because an important implied objective of the study was to investigate the assurance measures provided ONLY by the (e-commerce medium) website, and not by any other transactional medium; no regular web shopper could take the time to contact a company (either by phone or by email). Some companies do not have phone support at all (e.g., amazingly, for a company the size and prominence of Amazon.com, it does not offer telephone support — their *only* mode of support is email!). Most companies take at least a day's time to respond to emails; web chat is still a novelty in most sites to ask in detail about their various policies. Unless the shopper has had prior experience with their brick-and-mortar counterpart (and hence have their trust), the shopper would likely move to another firm which is transparent in its policy, and is hence more appealing to the customer. Besides, a truly electronic

transaction is devoid of human-to-human interaction, thereby depriving the accompanying element of intelligent and deliberate conversation (of a rational entity like a cogent human being) and hence, the underlying trust involved. It is under such conditions that we have striven to determine the elements of a website that inspire trust in a consumer.

Further, in the case of security assurance, we see that while most of the sites had received Verisign assurance, most of the subjects of the study (students who were asked to answer a questionnaire) were unable to identify this, and simply concluded that they were not independently checked by Verisign, in spite of a visible pictorial mechanism (normally, the padlock or an unbroken key in a browser) to verify this compliance. This was so because of the absence of a Verisign seal. A plausible theory that we can think of to explain this is the following: Those websites that seek digital IDs from Verisign are not mandated by Verisign to display their seal. Verisign merely provides the seal to the website that seeks their service. It is up to the website to take the initiative to display the seal. The best reasons that the authors could think of are that webmasters are either too lethargic to display the seal or do not realize the significance of displaying the seal.

It should be noted here that even though all the sites that employed SSL (Secure Sockets Layer) protocol in this study were provided digital certificates by Verisign for transmitting confidential information via the Internet, it is also possible that no assurance provider is needed to enable the invoking of SSL. The scrambling/enciphering of data can be achieved without the intervention of a third party. The role of the digital certificate provider is solely to attest that any exchange of decipherable sensitive information is visible only to the buyer and the seller and that it cannot be intercepted by any third party.

However, this is in marked contrast with other services like TRUSTe, BBBOnline, etc. Those websites that seek their assurance from them find that it is not only in their best interest to display the assurance seal, but also mandatory to display the seal. Why this different philosophy here? We need to look at this from the perspective of both the parties involved here (the seeker of the assurance service and the assurance provider: (1) the seeker benefits by displaying the assurance seal to signify a sign of approval of the site's policies — that they meet or exceed the provider's standards, and also from the goodwill associated with the provider; (2) the assurance provider mandates that the seeker display the seal so as to inform the general public that the website must meet the standards set by the provider, and that the seeker cannot violate its own policies; and also that, if the seeker violates its own policies, to let the public at large know that a grievance redressal mechanism is available, in which the provider will take an active role.

We see this difference mainly because of the narrow area of assurance provided by Verisign *vis-à-vis* the

other providers. Getting Verisign assurance entails no elaborate procedural/active practices as that involved with TRUSTe (e.g., administering privacy policies) or BBBOnline (e.g., Being prompt in refunds, etc.).

Since the motivation of our study was to assess the visible assurance elements on transactional websites as perceived by consumers, we decided not to correct this in the statistical analysis. With regard to privacy, we found that sites utilized cookies to various extents. Some of them used session/transient types, while others used permanent ones. While cookies may be used for fairly innocuous purposes such as for facilitating easy login purposes, a potential for abusing them also arises, which may involve monitoring the user's web surfing habits by stealth (on a long-term basis). Hence both session and permanent cookies were not discriminated in this study. In spite of these, we believe that these limitations do not negate the results of the study.

For purposes of further/future research, it may be worthwhile to conduct a comparative research on the emphasis differences of assurance dimensions among B2C, B2B and C2C websites using the emphasis density index of information assurance which has been developed and validated in this study.

A more comprehensive and bolder study may involve contacting individual websites including a survey of CIOs and trying to compare and contrast the true extent of assurance measures that have been adopted, which involve those behind the scenes, but whose cognizance the average surfer may not be able to decipher from the public content on the website.

## ACKNOWLEDGEMENTS

The research of the third author was supported in part by the National Science Foundation under grants numbers 9907325, 0420448 and 0417095.

## Notes

1. Incident is defined as 'the act of violating an explicit or implied security policy' by CERT ([http://www.cert.org/tech\\_tips/incident\\_reporting.html](http://www.cert.org/tech_tips/incident_reporting.html)).
2.  $Kappa = \frac{P_o - P_e}{1 - P_e}$  in which:  $P_o$  = observed agreement,  $P_e$  = expected agreement.

## References

- AICPA and Yankelovich Partners (1997) 'Electronic Commerce Assurance: Attitudes Toward CPA WebTrust', [<http://www.aicpa.org/webtrust/yankel.htm>].
- Associated Press (2003) 'Internet Fraud Spikes Sharply', *Wired.com*, 9 April, [<http://www.wired.com/news/print/0,1294,58409,00.html>].
- Benassi, P. (1999) 'TRUSTe: An Online Privacy Seal Program', *Communications of the ACM* 42: 56–9.
- Buck, S. P. (1996) 'Electronic Commerce — Would, Could and Should You Use Current Internet Payment Mechanisms?' *Internet Research: Electronic Networking Applications and Policy* 6: 5–18.
- Castelfranchi, C. and Tan, Y.-H. (2001) *Trust and Deception in Virtual Societies*, Kluwer Academic Publishers.
- Chellappa, R. K. and Pavlou, P. A. (2002) 'Perceived Information Security, Financial Liability, and Consumer Trust in Electronic Commerce Transactions', *Journal of Logistics Information Management* 15: 358–68.
- Cohen, J. A. (1960) 'Coefficient of Agreement for Nominal Scales', *Educational and Psychological Measurement* 20: 37–46.
- Colwill, C. M., Todd, M. C., Fielder, G. P. and Natanson, C. (2001) 'Information Assurance', *BT Technology Journal* 19: 107–14.
- Cranor, L. F. (1999) 'Internet Privacy', *Communications of the ACM* 42: 28–31.
- Dai, X. and Grundy, J. (2003) 'Customer Perceptions of a Thin-client Micro-payment System: Issues and Experiences', *Journal of End User Computing* 15: 62.
- Foo, S., Leong, P. C., Hui, S. C. and Liu, S. (1999) 'Security Considerations in the Delivery of Web-based Applications: A Case Study', *Information Management & Computer Security* 7: 40–50.
- Gray, G. and Debrecey, R., (1998) 'New Assurance Services: The Electronic Frontier', *Journal of Accountancy* 185(May): 32–8.
- Gritzalis, S. and Gritzalis, D. (2001) 'A Digital Seal Solution for Deploying Trust on Commercial Transactions', *Information Management & Computer Security* 9: 71–9.
- Hawkins, S., Yen, D. C. and Chou, D. C. (2000) 'Awareness and Challenges of Internet Security', *Information Management & Computer Security* 8: 131–43.
- Hu, X., Lin, Z. and Zhang, H. (2001), 'Myth or Reality: Effect of Trust-Promoting Seals in Electronic Markets', *Proceedings of the Eleventh Annual Workshop on Information Technologies & Systems, New Orleans, Louisiana*, Dec. 15–16.
- Internet Fraud Complaint Center/Federal Bureau of Investigation (2002) 'IFCC 2001 Internet Fraud Report', [[http://www1.ifccfbi.gov/strategy/IFCC\\_2001\\_AnnualReport.pdf](http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf)].
- Internet Fraud Complaint Center/Federal Bureau of Investigation (2003) 'IFCC 2002 Internet Fraud Report', [[http://www.ifccfbi.gov/strategy/2002\\_IFCCReport.pdf](http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf)].
- Jarvenpaa, S. L., Tractinsky, N. and Vitale, M. (2000) 'Consumer Trust in an Internet Store', *Information Technology and Management* 1: 45–71.
- Koreto, R. (1997) 'In CPAs We Trust', *Journal of Accountancy* December: 62–4.
- Lansing, P. and Hubbard, J. (2002) 'Online auctions: The Need for Alternative Dispute Resolution', *American Business Review* 20: 108–16.

- Lemos, R. (2002) 'Hackers Can Crack Most in Less Than a Minute', CNET News, [<http://news.com.com/2009-1001-916719.html>].
- Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995) 'An Integrative Model of Organizational Trust', *Academy of Management Review* 20(3): 709–34.
- Miyazaki, A. D. and Krishnamurthy, S. (2002) 'Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions', *The Journal of Consumer Affairs* 36: 28–49.
- Parker, D. B. (1994) 'Demonstrating the Elements of Information Security With Threats', *17th National Computer Security Conference*: 421–30.
- Pugliese, A. J. and Halse, R., (2000), 'SysTrust and WebTrust: Technology Assurance Opportunities', *The CPA Journal* 70(11): 28–33.
- Ratnasingham, P. (1998a) 'Internet Based EDI Trust and Security', *Information Management & Computer Security* 6(1): 33–9.
- Ratnasingham, P. (1998b) 'Trust in Web-based Electronic Commerce Security', *Information Management & Computer Security* 6(4): 162–6.
- Reuters (2003) 'US charges 135 with net crimes', *Wired.com*, 16 May, [<http://www.wired.com/news/print/0,1294,58875,00.html>].
- Riffe, D., Lacy, S. and Fico, F. G. (1998) *Analyzing Media Messages — Using Quantitative Content Analysis in Research*, Mahwah, NJ: Lawrence Erlbaum Associates.
- Shapiro, C. and Varian, H. (1998) *Information Rules: A Strategic Guide to the Network Economy*, Boston, MA: Harvard Business School Press.
- Tabachnick, B. G. and Fidell, L. S. (1996) *Using Multivariate Statistics*, New York: HarperCollins.
- Tedeschi, B. (2002) 'Consumers Union to Put Ratings Systems of Web Sites on the Web', *NYTimes*, 15 April, [<http://www.nytimes.com/2002/04/15/technology/ebusiness/15ECOM.html>].
- Sivasailam, N., Kim, D. J. and Rao, H. R. (2002) 'What Companies Are(n't) Doing about Web Site Assurance', *IT Pro* 4: 33–40.
- Ware, L. C. (2002) 'Invest in Privacy Policies and Keep Your Customers', *CIO*, 1 February, [[http://www.cio.com/archive/020102/tl\\_numbers.html](http://www.cio.com/archive/020102/tl_numbers.html)].
- Whitman, M. E. and Mattord, H. J. (2004) *Management of Information Security*, Thomson Course Technology.

**Appendix: List of firms**

<i>Banks</i>	<i>Insurance</i>	<i>Computer software &amp; data services</i>	<i>Hospitality</i>
BancWest Corporation	Chubb	America Online	Airtran Airways
Bank of America	Safeco	IMS Health	Alaska Air
BB & T Corp	Progressive Insurance	Amazon.com	American Airlines
Citibank	MetLife	Barnes & Noble	Continental Airlines
Comerica	Allmerica Financial	Equifax	Delta Airlines
Commerce Bank	Erie Insurance Group	The New York Times	Northwest Airlines
Fifth Third Bank	Ohio Casualty Group	Symantec	Pan American Airways
Firststar Corp	Mercury General	McAfee	Southwest Airlines
First Union	State Farm	Intuit	United Airlines
Fleet Bank	Liberty Mutual	F-Secure	US Airways
HSBC Bank USA	Allstate	OnTimeAuditor	Marriott International
JP Morgan	Amer. Family Insurance	PayMyBills	Park Place Entertainment
KeyBank	Conseco	ConsumerReports	Starwood Hotels & Resorts
MarketPlace Bank	Amer. Insurance Group	Elance Enterprise	Harrah's Entertainment
MBNA America Bank	Hartford Fin. Services	Paytrust	Hilton Hotels & Resorts
Mellon Bank	John Hancock Fin. Services	eLibrary	Mandalay Resort Group
M & T Bank	Nationwide Insurance Enterprise	Britannica	Wyndham International
PNC Bank	Loews	The Wall Street Journal	Meristar Hotels & Resorts
Safeway Select Bank	St.Paul Companies	Salon	Priceline
Sun Trust Bank	USAA	eMarketer	Expedia
			Hotwire

Copyright of Electronic Markets is the property of Routledge, Ltd. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.