

People's Trust and Confidence in Using Information Technology Solutions, Pertaining to Security, Privacy and Credibility

Client: CPIT (Christchurch Polytechnic Institute of Technology)
Contact: [CPIT Staff Member]
Email: [CPIT Staff Member]@cpit.ac.nz
Project: Research Report
Type: Informative
Author: Simon Henshall

Abstract

Information management is a prevalent issue in the current state of technology. As a person involved directly with the management of information, the author feels as though more could be done to ensure that data integrity is maintained. Just who is attempting to access data, how are they attempting to do it, and why? In this report, the author researched twenty previously published journal articles, news reports and relevant web pages to further his individual knowledge about the situation at hand.

The author found that while there are indeed technical reasons for loss of data, surprisingly, the human element is the cause for far more concern. While the findings are unlikely to change the way in which IT professionals approach data management and security, the author hopes it will provide some insight into possible solutions to the problem at hand for businesses wishing to explore those avenues.

Introduction

With information technology systems becoming more widespread, both small, independent companies and large, corporate organisations are shifting towards an e-Commerce basis. However, transactions conducted via this platform have a certain degree of risk associated with them due to the lack of face-to-face communication.

Customers only have a limited number of verifiable means of identification for a company, and most of these aspects are forgeable through identity theft. While websites typically offer some means of verification and assurance of security, the question is posed: Just how much trust are the consumers willing to put into the e-Commerce method, and what does their lack of trust mean for the organisations?

As there is no defined simplistic method of ensuring trust over the Internet, customers typically fall back on traditional methods of confidence, such as trust in the individual, trust in the system, confidence in the seller, perceived credibility and previous experience. If an individual has heard about the company through a friend or the media, this is also likely to sway their perception.

The perceived trust of an organisation is very important over the Internet, as scammers are quickly shifting their focus to target the platform. This not only applies to monetary transactions such as e-Commerce, where the obvious motive for the scammer is the money, but also information presented as though it were legitimate. Trust in falsified information can lead a company to make a decision that they may not have opted for previously, and the way in which Web 2.0 is structured makes this much easier, as it effectively gives the scammers their own readily-available platform to reside on, and even promote themselves.

A plethora of information can be falsified over the Internet that would not be possible with traditional means, including company name, address, telephone number, website Uniform Resource Locator (URL), testimonials and most dangerously, identity itself. In real life, a potential scam victim would be able to detect visibly if the scammer wasn't legitimate. Over the Internet, however, this

task becomes much more difficult, so a degree of trust must be formed before committing to anything.

This paper looks at the issues of trust, credibility, privacy, security and confidence, as well as the impact of gender, age and ethnicity, with regard to the use of Information Technology Solutions, and attempts to suggest possible avenues to increase awareness of both the possible risks and advantages of using them.

Trust

Most business transactions are dependent on some level of trust between the two parties. In business transactions that do not occur on the web, trust is typically based contracts, guarantees and personal relationships between the two parties. That may not be the case for web transactions.

Online trust has been defined as “the Internet user’s psychological state of risk acceptance based on the positive expectations of the intentions or behaviours of an online service provider” (Rousseau et al., 1998) and customer trust as “the extent to which a customer believes that the supplier is honest, benevolent and competent” (Ryssel, Ritter, & Gemunden, 2004). It has been found that lack of trust of online businesses is one of the main reasons for customers not engaging in commercial transactions on the web. (Roca, García, & Vega, 2009)

Trust itself can be broken down into three different aspects: Individual Trust (The Approach of Personality Theorists), Societal Trust (The Approach of Sociologists and Economists) and Relationship Trust (The Approach of Social Psychologists). These three aspects pertain to the amount of trust someone has in the individual, the amount of trust someone has regarding society as a whole and the perceived trust between two parties, respectively. (Kini A. , 1998)

According to Rousseau *et al.* (1998), three different phases of trust can be distinguished: the phase of trust building, where trust is formed; the phase of stabilizing trust, where trust already exists; and the phase of dissolution, where trust declines. (Grabner-Krautter, 2009)

When the Internet was first conceived, it operated on a single domain of trust, while provisions were made to allow remote users' access to critical information on machines. As the Internet grew, more companies decided to opt for e-Commerce as a primary means for delivery of goods to customers. However, e-Commerce cannot achieve full potential without securing customer trust and addressing security management issues. Classic work in anthropology by Malinowski in 1922 revealed long ago the inextricable connection between cooperative social and economic relations. (Baba, Fall 1999)

E-Commerce is one of the fastest-growing economic activities worldwide. In the United States e-Commerce accounted for over US\$1,500 billion in manufacturing shipments (or about 31.2% of all shipments) in the year of 2008. (U.S. Census Bureau, 2008) In the United Kingdom a number of online banking companies have chosen to opt for no physical presence whatsoever, including Firstdirect, Ingdirect and Smile.

According to (Kini A. , 1998), the four factors that affect trust in electronic commerce are the individual, the system, the task, and the ‘information environment’. The information environment is a theory about the complexity of information management within an organisation. A massive change to the afore-mentioned information environment was brought about with the introduction of Web

2.0. Web 2.0 is the popular term for advanced Internet technology and applications, including blogs, wikis, podcasting, RSS, and social networks (Lai and Turban, 2008; Scholz, 2008). The essential difference between Web 2.0 and the traditional Web is that content is user-generated, and there is considerably more collaboration amongst Internet users. (Grabner-Krautter, 2009)

The primary reason for data loss within Web 2.0 is that most Web 2.0 users are 'time-poor' and tend to place a large amount of trust in their antiviral software to report any suspicious activity on their computer such as keyloggers. However, the vast majority of hackers and identity thieves residing on Web 2.0 obtain their information through social engineering, a process that is incredibly difficult for software to prevent. (Grabner-Krautter, 2009)

One of the most popular venues introduced with Web 2.0 is Online Social Networks (OSNs). These OSNs make it easier to provide false or misleading information, and it is more difficult to verify information provided by others, especially regarding their true identity and motives. In such situations of uncertainty, trust can serve as an important mechanism to reduce the uncertainty and complexity of exchanges and relationships. (Grabner-Krautter, 2009)

A major disadvantage of the Internet is the ability for incorrect or misleading information to be published with relative ease. "In some corporate contexts, if a work group sends out completely accurate and thorough information, its strategic position *vis-à-vis* other groups may be compromised. Knowing this, work groups may deliberately misrepresent the information they send." (Baba, Fall 1999)

Several factors can contribute to the lack of trust in electronic commerce, specifically issues of risk, security, privacy, dependability, and competence. Risk is an important component of trust, because an individual's decision to trust is primarily important when there is some risk of negative outcomes. Trust in a system is defined as "an individual's belief in the competence, dependability, and security of the system under conditions of risk":

Dimensions of Trust	Components	Item No.
Security	Theft	I1
	Privacy	I5
	Impersonation	I12
	Modification	I8
Dependability	Reliable	I3
	Error Free	I10
	Available	I6
	Consistent	I9
Competence	Expertise	I2
	Knowledge	I4
	Skill	I10
	Capability	I7

(Kini & Choobineh, 2001)

Researchers have studied how online customers develop their trust toward companies without any face-to-face interaction. For example, Venkatesh *et al.* (2003) found that perceived ease of use was significant only in the initial stages of learning to use various applications, and that aspects such as reliability are more important in the long run.

It turns out that customer perception of online banking security is significantly affected by the usage of the system itself, and the trust of the system and system operator. Non-users of Internet banking perceived the system to be insecure (over 50%), whereas users perceived the system to be secure (over 60%). This perception of security was increased through both trust in the system and trust in the provider. Though experts provide assurance of security, thereby increasing customer trust, this is offset by successful execution of botnets such as Zeus and Mariposa. (Twum, 2012)

In 2009, Roca *et al.* conducted a study of 180 students at a University in Spain to test intention to use online trading systems against the traditional Technology Acceptance Model (TAM). A key factor in TAM is the Perceived Ease-of-Use (PEOU), which developer Fred Davis defines as "the degree to which a person believes that using a particular system would be free from effort." TAM predicts user acceptance of any technology to be determined by two factors: perceived usefulness and perceived ease of use. The study allowed participants to effectively become e-Investors, with the following hypotheses:

- H1. Perceived usefulness has a positive effect on intention to use online trading services.
- H2. Perceived ease of use has a positive effect on perceived usefulness in the online trading services.
- H3. Perceived ease of use has a positive effect on intention to use online trading services.
- H4. Perceived trust has a positive effect on intention to use online trading services.
- H5. Perceived usefulness has a positive effect on perceived trust.
- H6. Perceived ease of use has a positive effect on perceived trust.
- H7. Perceived security has a positive effect on perceived trust.
- H8. Perceived privacy has a positive effect on perceived trust.

The results showed that perceived usefulness was a more important determinant of perceived trust than ease of use, suggesting that a more useful web site can encourage e-investors to trust in it, and if the site is easy to navigate will also increase willingness to trust. Roca *et al.* also draw on work from Koufaris and Hampton-Sosa (2004), who demonstrated that perceived security control of the site strongly influenced initial trust in the company. The most important antecedent of behavioural intentions is trust. Trusting perceptions directly influence the decision to use e-services, which is consistent with prior studies (Bhattacharjee, 2002; Kim *et al.*, 2008). Surprisingly, perceived privacy was not a determinant of perceived trust. (Roca, García, & Vega, 2009)

In 2001, Kini & Choobineh conducted research into the direct correlation between the 'Tendency to Trust' (TTT) a service provider and the risk involved (RI) in doing so over the World Wide Web (WWW), with the following hypotheses:

- H1: Trust in WWW commerce systems is lower than trust in conventional commerce systems.
- H2: Trust in the system will be higher for high information provision subjects than for low information provision subjects.

- H3: Trust in the WWW banking system will be lower for high-risk tasks than for low risk tasks.
- H4: Individuals with high TTT will have more trust in the system as compared to individuals with low TTT.
- H5: Trust in the system due to information provision will be higher for individuals with low TTT than for ones with high TTT.
- H6: Trust in the system for a high risk task is lower for individuals with low TTT than for ones with high TTT.
- H7: Trust in the system due to information provision will be higher for the high-risk task than for the low risk task.
- H8: Individual's with higher trust in the system

Only half of the hypotheses were validated:

Table 2 Summary of the Results

Hypothesis No.	Premise	Validated?
H1	Trust Between Systems	Yes
H2	Affect of Information	Yes
H3	Affect of Information	Yes
H4	Affect of Tendency to Trust	No
H5	Interaction of Information and TTT	No
H6	Interaction of Risk and TTT	No
H7	Interaction of Risk and Information	No
H8	Affect of Trust on Adoption	Yes

(Kini & Choobineh, 2001)

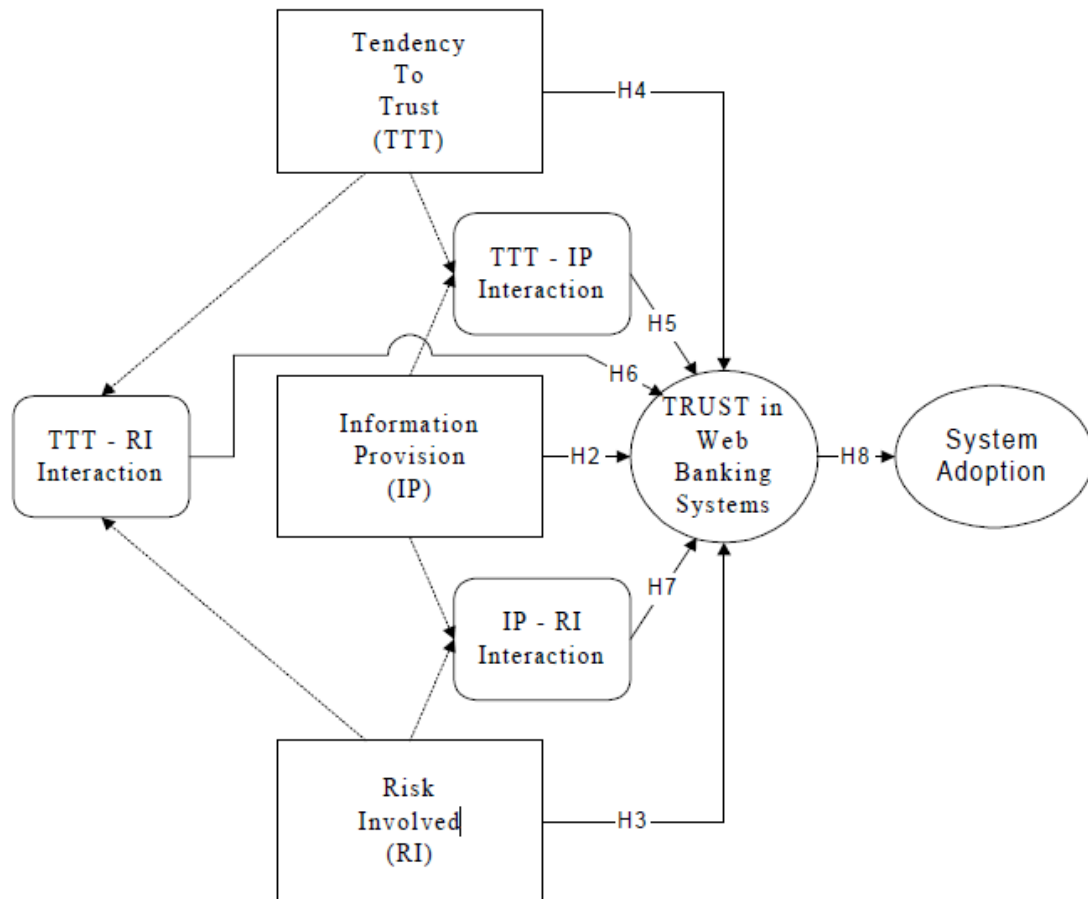


Figure 1: Research Model for Studying Trust in WWW Commerce

(Kini & Choobineh, 2001)

The results of the study showed that the subjects did not trust the WWW banking system as much as a conventional system. For successful interaction with an e-Commerce system there needs to be a high level of customer commitment.

Customer commitment is defined by Ryssel *et al.* (2004) as being drawn along four dimensions:

- Loyalty
- Willingness to make short-term sacrifices
- Long-term orientation
- Willingness to invest in the relationship

Ryssel *et al.* conducted a study to gain an initial and general understanding of the impact of IT on inter-firm relationships. Over 2000 companies were asked to participate in the study, although only 61 companies replied and proceeded. The following hypotheses were made:

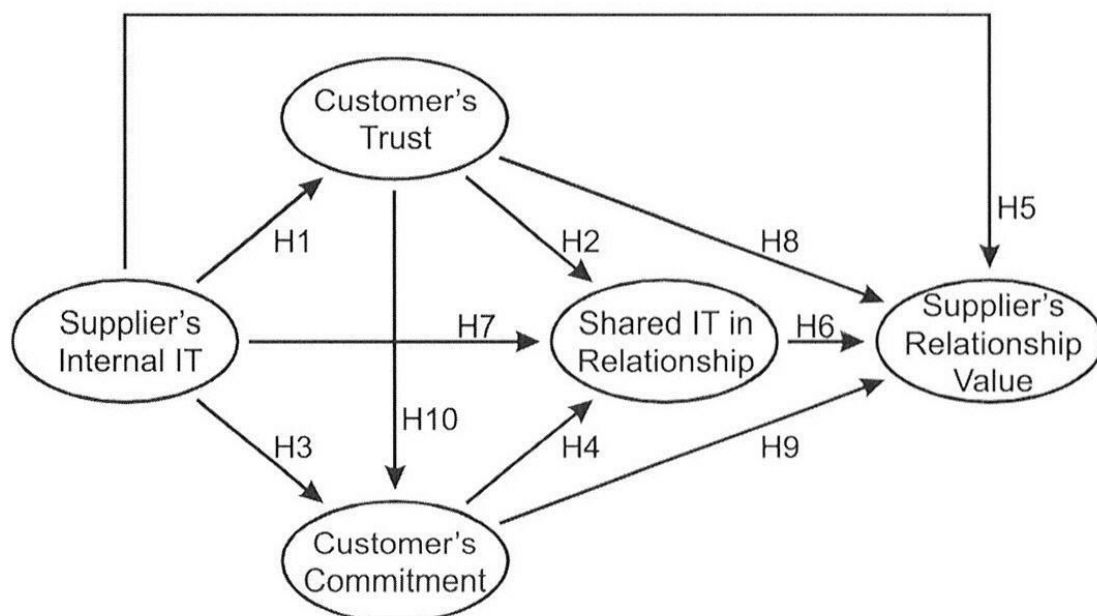
- H1. Higher employment of internal IT on the supplier-side leads to higher customer trust.
- H2. Higher customer trust leads to higher employment of shared IT.

- H3. Higher employment of internal IT on the supplier-side leads to higher customer commitment.
- H4. Higher customer commitment leads to higher employment of shared IT.
- H5. Higher employment of internal IT on the supplier-side leads to higher value creation in the relationship
- H6. Higher employment of shared IT leads to higher value creation in the relationship.
- H7. Higher employment of internal IT on the supplier-side leads to higher employment of shared IT.
- H8. Higher customer trust leads to higher value creation in the relationship
- H9. Higher customer commitment leads to higher value creation in the relationship.
- H10. Higher supplier trust leads to greater supplier commitment.

The results showed that the two important factors for a successful relationship are trust and commitment. Only if the customer trusts the supplier and is committed to him, is the customer willing to allow more 'value creation' for the supplier. Value creation is defined as "the performance of actions that increase the worth of goods, services or a business" and in the study, was found to be a component of the relationship atmosphere and not of the technology employed. However, the implementation of IT into a relationship is determined more by the technology within the company than the relationship atmosphere.

Commitment has a significant impact on shared communication and process IT, which gives support to the argument made in the paper that a long-term view is needed to justify investments in IT.

Figure 3 Conceptual model of this study



According to the findings, shared IT use is not a function of trust. Internal and shared IT have no significant impact on either direct or indirect value creation, except for in the case of shared process IT in relation to indirect value creation, which has a significant negative impact.

One implication of the study conducted by (Walton, 2013) is to avoid emphasizing product over process, particularly in development contexts involving distributed work (limited co-located, face-to-face collaboration across stakeholder groups). Even if ICTs convey relevant, timely information (product), intended beneficiaries will not act on that information if trust has not been built to mitigate the risks associated with participating (process).

The stakeholders involved in a single Information and Communication Technologies for Development (ICTD) project typically vary widely in socioeconomic status, technology use, language, ways of knowing, areas of expertise, and literacy levels. Thus, it can be challenging to develop the trust necessary to sustain a project and to understand and balance stakeholder interest.

While the success of information technology typically is not predicated upon bonds of trust, its failure often is the result of another phenomenon that has received less attention in the literature—distrust: “The presence of distrust between firms, functions, and hierarchical levels in a corporation results from an expectation of harm that is based, in part, on the memory of past negative exchanges (actual or perceived) between particular groups (Luhmann 1988). Such expectations, warranted or not, may inhibit the sharing of information across group boundaries, which is a prerequisite for effective use of information technology (Sproull and Keisler 1993)”. (Baba, Fall 1999)

In the context of e-business, several researchers have suggested that the technology itself – serving as a transmission medium for conducting economic transactions and including security services and technical solutions embedded in e-commerce technologies – has to be considered as an object of trust (Corritore et al., 2003; Grabner-Krautter and Faullant, 2008; Pennington et al., 2003/2004; Ratnasingam, 2005; Rotchanakitumnuai and Speece, 2003; Shankar et al., 2002). (Grabner-Krautter, 2009)

Thus, trust can be seen as a powerful alternative to formal governance mechanisms that allow exchange relationships to be formed and that attempt to control opportunism (Puranam and Vanneste, 2009). Where there are high levels of trust, people are more willing to provide support and take risk in information exchanges (Nahapiet and Ghoshal, 1998). However, “choosing to take a risk in a situation in which, if the trust is misplaced, the outcome could be worse than not having trusted at all” Deutsch (1958).

In a WWW commerce relationship, risk involves the probability of the individual engaging in WWW commerce facing negative outcomes like abuse of personal information or loss of financial resources from the untrustworthy behaviour of the WWW commerce system.

Having learned that cotton farmers in Andhra Pradesh had committed suicide over failed crops and their resulting inability to pay debts, a researcher at an Indian university led a project to use Information and Communication Technologies (ICTs) to extend the reach of agricultural experts. One of these projects was initiated to deliver farming advice at a customized, individual level. This customized focus alone was insufficient to create enough trust for farmers to risk their livelihoods by following the advice. (Walton, 2013)

The problem impeding the goal of improving farmers’ well-being was not a technology problem or a problem with the content or timing of information. It was insufficient trust for beneficiaries to take the risk of acting on information. Because they had insufficient pre-existing relationships with the

agricultural experts, farmers did not judge the risk of following their advice to be worth the potential harm: the possibility of losing crops comprising their livelihoods. “Credibility is important. So if I know that an expert is answering the question I have, then I believe in the answers.” – A farmer partaking in the project (Walton, 2013).

Credibility

Tseng and Fogg (1999) identify four source types of credibility: Presumed credibility (a user’s preconceived assumptions about the seller, based on stereotypes), reputed credibility (such as source labels), surface credibility (a user’s opinion based on simple overviews) and experienced credibility (a user’s first-hand experience over time). Links from one website to others act as referrals and may imply third-party endorsement, which increases reputed credibility.

Messages from both high and low credibility sources are learned equally well according to Hovland and colleagues (1949). Interestingly, it was discovered that the primary influence of credibility factors is at the point of ‘first contact’. That is to say, the means by which the message is made persuasive becomes unimportant, only that the message was indeed persuasive in the first place.

Olaisen (1990) discusses how “cognitive authority” is derived directly from the influence of the service on offer, and that the influence is derived directly from credibility. Combining cognitive factors such as influence, trustworthiness, competence and reliability with technical factors such as form, accessibility and flexibility creates an “institutional quality” (Olaisen, 1990). The greater the institutional quality is, the more credible the information. Interestingly, high price and limited timeframes are found to directly increase institutional quality.

As one might expect, more credibility is perceived in websites ending in .edu, .org and .gov than .com, along with websites that list author credentials. Websites that have been previously recommended by a friend or colleague are also given more credibility.

This raises concerns regarding the valuation of the degree of professionalism of website developers. A small, legitimate company may be composed of members who have immersive technical skill, though little website development skill, and the insufficiency of funds to pay for development of a more appealing website. Conversely, scammers with website development skills will have a massive influence on victims, as the website is often the point of ‘first contact’.

For example, one common method that scammers use to increase their credibility on the web is to fake positive feedback in the form of images. This can come either in the form of official Certificates of Authority (CoAs), pretending to be from well-trusted companies such as Microsoft, PayPal, SoftPedia or antiviral product sellers. Often these CoAs are accompanied by entirely falsified ‘user stories’ or testimonials to further help increase the perceived credibility of the website owner. (Wathen & Burkell, 2002)

People naturally trust others who are similar to them, and distrust those who are not. Trust and credibility is most commonly built on consistent, appropriate behaviour, over prolonged interaction. “If people are trusted to begin with, poor technical performance will not necessarily destroy trust. Trust will survive when a breach of promise or a technical failure is viewed as an isolated incident... Distrust occurs when people are perceived as having beliefs and values that are incompatible with

the organization's... If IT specialists are distrusted, they will not be credible, no matter how good their expertise and their technical performance." (Bashein, B. J., & Markus, M. L. 1997)

IT specialists tend to be perceived as having a low level of credibility by both businesspeople and themselves. IT specialists believe that ignorance on the part of businesspeople leads to negative stereotyping of IT specialists.

An interesting aspect is that different members of society have different 'rankings' regarding other's contributions and failures: "A man thinks he scores high with a woman when he does something very big for her, like buying her a new car... He assumes he scores less when he does something small, like opening the car door, buying her a flower, or giving her a hug. Based on this kind of score keeping, he believes he will fulfill her best by focusing his time, energy, and attention into doing something large for her... When a woman keeps score, no matter how big or small a gift of love is, it scores one point; each gift has equal value. Its size doesn't matter; it gets a point" (Gray, 1992).

This shows that "credibility is the result of the credit others give us, regardless of the credit we take". It is up to the individual to determine how credibility is perceived by the masses in order to succeed. (Bashein, B. J., & Markus, M. L. 1997)

To help attain credibility, IT specialists should attempt to use business jargon rather than IT jargon, become more involved with the customers, raise concerns gradually to avoid panic, and maintain detailed problem logs and publish summaries. It is also important to be enthusiastic, even if projects seem risky or misguided, and conduct demonstrations to educate clients about how IT works. IT specialists may face many technical difficulties, but taking care of customers should be their top priority. (Bashein & Markus, 1997)

Privacy

According to Claire Gauzente of the University of Angers, there are six main 'views' of privacy:

1. The right to be left alone
2. Limited access to the self
3. Secrecy
4. Control over personal information
5. Form of personhood protection
6. Intimacy

It has been said that "...privacy risk is a consumer's subjective evaluative assessment of potential losses to the privacy of confidential personally identifying information, including the assessment of potential misuse of that information that may result in identity theft." (Featherman, Miyazaki, & Sprott, 2010)

A poll conducted in early 2012 reports that 58% of all Internet users have at least one social networking profile. The average user's profile contains information about their home address, their pet's name, where they went to school, their mother's maiden name and other family details – just the kind of information used for security or 'lost password' questions for online banking and other

confidential services. The irony in this is that 'hackers' (as they are often incorrectly dubbed) do not need to worry about stealing information at all – victims often give it publicly.

While the majority of the general public seems happy to share private information freely, it is of importance to note that in a study prior to 1998 on where users place their trust, USA Today reported that only 5% of people surveyed trusted the Internet to send credit card information. A more recent study conducted by the Boston Consulting group found that more than 70% of the people surveyed were concerned about sending private information over the Internet (Kini A. , 1998). Interestingly, this suggests that the general public is actually unaware of what information should be kept private.

This is backed up by an investigation conducted by antiviral company Sophos. Sophos conducted a study in England in 2007 by creating a fraudulent Facebook account named 'Freddi Staur', a deliberate pun on the word 'fraudster'. The intention was to discover exactly how much information random citizens were willing to give away over Facebook, to see how susceptible the average Facebook user is to identity theft.

This study involved sending friend requests to 200 individuals chosen completely at random, and revealed some disturbing information:

- 87 of the 200 Facebook users contacted responded to Freddi, with 82 leaking personal information (41% of those approached)
- 72% of respondents divulged one or more email address
- 84% of respondents listed their full date of birth
- 87% of respondents provided details about their education or workplace
- 78% of respondents listed their current address or location
- 23% of respondents listed their current phone number
- 26% of respondents provided their instant messaging screen name

(Sophos, 2009)

A secondary study was conducted by the Australian division of Sophos in December 2009 to see how much had changed since the first investigation, and gauge if users had learned how to better protect their privacy. Two new fake profiles were created, 'Daisy Feletin', who had a picture of a cat, and 'Dinette Stonily', who had a picture of a rubber duck. The results were actually worse than the findings from the first study:

Information	Daisy Feletin	Dinette Stonily
Friends accepting	46%	41%
Total friends gained	46	49
Full d.o.b. (D/M/Y)	89%	57%
Partial d.o.b. (D/M)	9%	35%
Email address	100%	88%
College or workplace	74%	22%
Town or suburb	50%	43%
Full address	4%	6%
Phone number	7%	23%
IM screen name	13%	18%
Family and friend data	46%	31%
Average no. of friends	220	932

(Sophos, 2009)

In 2001, Pavlou and Chellappa conducted one of the first empirical studies that links perceived privacy and trust. Their study focused on perceived privacy and perceived security of web sites and their contribution to trust. The results indicated that although perceived privacy is a significant contributor to trust, perceived security is more important in the eyes of the consumer. (Gauzente, 2004)

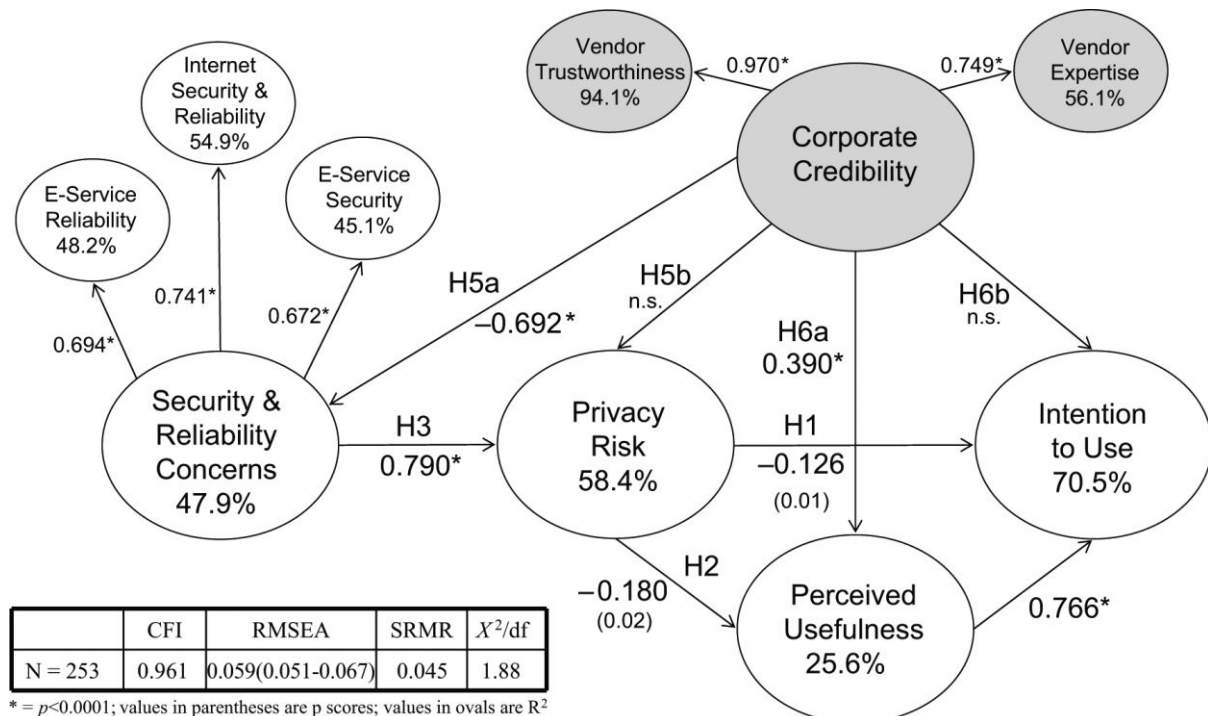
The Culnan and Milne report of 2001 indicates that 82% of consumers have already refused to give personal information because it was deemed too personal or unnecessary. In this study, 81% of consumers indicate that they want to protect themselves against privacy risks. However, 50% of consumers also acknowledge that they do not read web privacy notices from web sites. The two main reasons for this are that consumers trust well-known companies, but also believe that privacy notices are difficult to understand. In a paper referenced by (Gauzente, 2004), Han and Maclaurin (2002) insist that privacy policies must be unquestionably clear so that consumer fears are alleviated. (Gauzente, 2004)

A more recent research report was conducted by Featherman *et al.* in 2010, which looked into reducing the privacy risk in e-services. This report also provided direct links between corporate credibility and consumer privacy and security concerns. Their hypotheses were:

- H1. Privacy risk decreases consumer intent to use an e-service.
- H2. Privacy risk decreases the perceived usefulness of an e-service.
- H3. Consumers' security and reliability concerns increase assessments of privacy risk.
- H4. Ease of use reduces (a) the assessed privacy risk and (b) the security and reliability concerns of using an e-service.
- H5. Corporate credibility reduces (a) consumer security and reliability concerns and (b) consumer assessments of privacy risk.

- H6. Corporate credibility increases (a) the perceived usefulness of an e-service and (b) consumer intention to use the e-service.
- H7. Corporate credibility reduces the effect of privacy risk on consumer intention to use the e-service.

Both studies conducted by Featherman *et al.* found that security and reliability concerns influenced privacy risk, which in turn, influenced the perceived usefulness of the e-service and the intentions to use it. The following diagram illustrates the direct correlations in relation to each of their hypotheses:



(Featherman, Miyazaki, & Sprott, 2010)

“A related line of research suggests that a well-explained and easy to understand web site (i.e., one likely to be given a high rating of PEOU) increases consumer trust in an e-commerce vendor (Gefen et al., 2003). Because subsequent research indicates that trust and risk (as well as trust and security/reliability concerns) are inversely related (Pavlou, 2003; Pavlou and Gefen, 2004), this line of research suggests that, in addition to increasing consumer trust levels, PEOU also acts to reduce consumer perceived risk levels, as well as security and reliability concerns.” (Featherman, Miyazaki, & Sprott, 2010)

While privacy statements help to convince customers that the company is legitimate, security statements are expected to be perceived as more reassuring than privacy statements. Additionally, privacy statements pertaining to information control are expected to be perceived as more reassuring than other privacy statements.

Security

Although privacy is deemed an important aspect, the primary concern regarding e-Commerce is the security of the data, particularly if a monetary transaction is involved. When registering for a website, customers are prompted for a catalogue of personally-identifying information. This typically includes their full name, location and credit card information, though may also include some other personal information such as their pets or favourite colours (for account recovery purposes).

Internet security can be defined as “the protection of data from theft, loss or unauthorized access, use or modification.” (Jenkins, 2010) The issue of Internet security is so important that many large firms employ full-time security experts or analysts to maintain network security. However, few, if any, home and small business owners can afford that luxury.

In 2001, Miyazaki and Fernandez (2001) found that internet users’ top three concerns regarding online shopping were privacy, system security breaches from third parties (due to faulty technological security), and security breaches in the form of fraudulent online retailer behaviour. A more recent report by Litan in 2005 showed that 42% of respondents stated that concerns about online attacks to their confidential information have a negative impact on their shopping behaviour. (Featherman, Miyazaki, & Sprott, 2010)

There is also the possibility of the e-Commerce services themselves coming under attack. Criminal ‘hacktivists’ have started emerging, such as Anonymous -- notorious for crippling MasterCard and PayPal, as well as providing Internet access to countries such as Tunisia and Egypt when access was cut off. Having emerged from 4chan and initially formed in protest of the Church of Scientology, they now target organisations’ websites in order to take a stand for freedom of speech.

The term hacker was originally used to refer to a self-taught, highly-skilled computer expert. The mass media refer to hackers as people who break into computer systems, regardless of motivation. However, in the media, the term hacker is nearly always used for people who hack illegally for criminal purposes. Many Internet security professionals strongly disagree with the way in which the media use the term. (Jenkins, 2010)

Internet activist and journalist Quinn Norton, who was the keynote speaker at NetHui in Wellington likens the group Anonymous to slime mould – there is no central brain, or as Norton put it, “there is no-one driving this crazy bus.” It is interesting that Norton sees the rise of these ‘feral’ networks as one of the greatest influences on changes in society – so great, that he compares it to the introduction of the printing press. These groups are also (according to Norton), threatening our notions of law, order, nationhood and democracy. (Griffin, 2013)

It should be pointed out that Quinn’s view may be somewhat influenced by the fact that her ex-boyfriend Aaron Swartz, who co-founded Reddit, was indicted in 2011 after he hacked into the JStor academic article database of MIT. He believed research should be made freely-available on the Internet. However, as a result of his activities, numerous Universities and other agencies around the world are already making academic research freely-available online. (Griffin, 2013)

These hacktivists typically hack in order to obtain information that would not be readily-available through other means, pertaining to a specific organisation. However, personally-identifiable

information is nearly always found in concurrence, due to the configuration of most organisation servers. This information could give the attacker (or whomever they choose to on-sell the information to) a competitive advantage. (Griffin, 2013)

To prevent such instances occurring, organisations often employ specific IT teams (that require training and maintenance). The introduction of these IT teams often results in a complete reorganisation of the hierarchy of a company. Conversely, if a company were to provide a solution to hacking, such as prevention systems, they may in fact benefit from the growth of the amount of hacking.

While theft of confidential information is the main concern regarding hacktivists, a far more damaging byproduct is the possibility of viruses injected through backdoors left by hackers. While virus injection is not a certainty of successful hacks, once a hack is successful, there are no defences other than the mere choice of the hacker not to infect the system. In 2003, viruses introduced to companies as a result of security breaches were found to cost an estimated US\$55 billion. A study in 2011 showed that hacking was found to cost between US\$600,000 and US\$7 million in expenses each day, depending on the size of the organisation affected. On top of that, there are many additional costs to take into account such as the number of hours it costs employees to recover from the breach (which proved markedly detrimental). (Gish, 2013)

Security, which involves the use of technical advancements like cryptography, digital signatures and certificates aimed at protecting users from the risk of fraud, hacking or "phishing", has a positive influence on the intention to purchase online.

According to (Teixeira, 2007), small business owners often have the mentality that it "won't happen to my business", as there is nothing to gain from breaching security on such a small business. However, hackers are increasingly targeting small businesses because these usually do not have the resources or know-how that large corporations do.

In response to the need for greater speed and higher carrying capacity, most small or home businesses users rely on high bandwidth connections to the Internet such as a Digital Subscriber Line (DSL) or a cable modem. While these both provide high-speed access to the Internet, there are two fundamental vulnerability issues due to the fact that the connection is always open:

Because they are always on, they are always available for potential attackers to access. An unprotected connection to the Internet is an open two-way channel; information goes in and out of the system unimpeded. As long as an unprotected connection is maintained, it serves as a point of entry for potential intruders to enter or attack the system. (Jenkins, 2010)

Another concern is that always-on connections have static IP addresses. With classic Internet connection methods, such as dial-up modems, the connection made is temporary. Each time the connection is re-established, the computer gets a new IP address. This makes the computer harder for attackers to find, because the target address is always changing. Because high-speed connections remain connected, even when the computer is not in use, the IP address never changes. Once a potential hacker gains knowledge of the IP address, they will be able to return to it, placing it at greater risk of malicious intrusion. (Jenkins, 2010)

Once an attacker gains control of the user's computer, they gain access to all the files that are stored on the computer, including personal or company financial information, credit card numbers, and client or customer data or lists. This compromising of data could do serious damage to any business. If the data is altered or stolen, a company may risk losing the trust and credibility of their customers.

It was found that 82% of data that was either lost or stolen in the studies of Teixeira could have been avoided if the business had followed a simple cyber security plan, such as the 'five solutions' to the 'five common problems' outlined by Teixeira:

- **1:** To protect against **malicious code** (which results in an average loss of US\$69,125 for companies affected) you should install and maintain an antivirus, antispyware and firewall.
- **2: Stolen/lost laptops and mobile devices** cost companies an average loss of US\$30,570, and to protect against this you should keep backups of all important information, and encrypt data in case of a theft.
- **3:** The best way to combat **spear phishing** is to maintain a healthy degree of scepticism (especially with important information providers) and also raise awareness within the company. Teixeira believes that this is the most important aspect to consider, as it directly relates to the issue of trust and credibility.
- **4:** To prevent **unsecured wireless Internet networks** companies should change default passwords and make sure to encrypt all networks with Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) keys.
- **5:** There is always the possibility of an **insider/disgruntled employee threat**. Divide critical components amongst employees (minimising data loss if a breach occurs), change passwords often and institute background checks on employees to ensure employee integrity.

In a research paper by Daniel M. Downs, Ilir Ademaj and Amie M. Schuck where Chicago residents' knowledge about Internet security was studied, about one-third of the respondents stated that they understood spyware and firewalls very well, whereas just 23% of respondents were familiar with phishing. Only 23% of the respondents strongly agreed that they could fix their computer if it got infected. (Downs, Ademaj, & Schuck, 2009)

In 2005 businesses spent about US\$67 billion dealing with spyware, viruses, data theft and other computer-related crimes (U.S. Federal Bureau of Investigation, 2005), and in 2007 consumers lost about US\$239 million (or about US\$2,529.90 per victim) to Internet-related fraud and identity theft (Internet Crime Complaint Center, 2008). (Downs, Ademaj, & Schuck, 2009)

A study conducted jointly by AOL and the National Cyber Security Alliance (NCSA) in 2004 revealed that 81% of the respondents reported having some type of anti-virus software on their computer, however, only 68% reported updating the program at least weekly. (Downs, Ademaj, & Schuck, 2009)

In a more recent study conducted by McAfee and the NCSA (2007), researchers found that 87% of respondents reported they had an anti-virus program, but only about 52% had updated their program in the last week. Further, 44% of respondents did not understand how a firewall worked, and one in four had not heard of the term phishing. (Downs, Ademaj, & Schuck, 2009) In general, the

research suggests that about half of consumers do not know how to protect themselves from cyber criminals. (McAfee–NCSA Online Safety Study, 2007)

As more and more security breaches have occurred due to malicious or innocent attacks, the public opinion on security and trustworthiness of using the Internet for commerce has veered towards an attitude of distrust. In order to prevent serious loss, companies must take great measures to ensure data integrity, often at the expense of either monetary gain or the time spent by employees implementing the security. (Gish, 2013)

Confidence

Confidence is of paramount importance in the relatively-new medium of online auctions due to the fact that it is not simply a case of a consumer interacting with a company which has already established a base of trust and reliability, but with other private individuals.

“The purchase of online e-services is fundamentally different from the online purchase of goods or traditional services since e-services typically create a type of long-term relationship between the customer and online retailer that involves ongoing transmission and remote storage of the consumer’s confidential information.” (Featherman, Miyazaki, & Sprott, 2010)

In consumer online auctions the main risks are that the winner of the auction may not deliver payment, the seller may not deliver the goods, or the goods delivered may not be as the seller described. Scott and Walsham (2005) define reputation risk as “the potential that actions or events negatively associate an organization with consequences that affect aspects of what humans value.” According to eBay, the auction contract between a seller and the winning buyer is binding. eBay, however, does not enforce individual contracts, although it will suspend sellers who exhibit chronic non-performance.

Daniel Houser of the University of Arizona conducted a study in 2000 to discover the correlation between seller reputation on eBay and the amount buyers were willing to spend on items. In the 94 auctions in the data set, the number of positive, neutral, and negative comments left for sellers was 23, zero, and four respectively. The number of positive, neutral, and negatives comments left for buyers was 24, one, and one, respectively. (Houser, 2000)

Unsurprisingly, sellers with better reputations are more likely to attract more bidders in an online auction, as the bidders have confidence that the seller will indeed provide the goods in the condition and price stated. Sellers with good reputations are also often able to provide lower prices, and cut ‘deals’ as they can be trusted when buying in bulk; “Trust has important functions in all societies, including... reduction in the costs of exchange and other transactions” (Schmidt and Posner 1982).

A seller who provides good service can look forward to positive feedback from the buyer and this enhances his reputation. To add incentive to consistent good behaviour, eBay implemented a feedback system which provides not only the ability for others to help to provide insight on the integrity of a seller, but also provides incentives for good performance by sellers. The same also applies to buyers: a buyer who routinely delivers payment in the auction he wins will develop a good reputation and will not risk finding his bids cancelled due to a low feedback score.

Houser goes on to say that the “model of high-bid auctions predicts that the second highest bid should not depend upon the buyer’s own reputation” (Houser, 2000). The main finding of Houser’s study was that seller reputation (but not buyer reputation) is a statistically and economically significant determinant of auction prices.

While word of mouth is a key factor regarding credibility, due to the ability for anyone to post information anonymously, information published by those not knowledgeable in the relevant areas is often considered fact, despite it typically just being rumours. Some companies have even been destroyed as a result of such rumours (Ito and Kagaya, 2006). On the night of February 26, 2004, the Livestock Hygiene Service Center in Kyoto Prefecture received a telephone call from a person stating that “A thousand chickens a day are dying at Asada Nosan Co.’s Funai farm...” Verification activities by the hygiene service center began immediately after the phone call, and cases of avian influenza at the same farm were verified the following day.

Even when harmful rumors spread, the amount of damage varies depending on how well confidence is restored at an early stage. For example, many harmful rumors concerning chicken eggs from Kyoto were widely circulated, and there were numerous instances of economic damage. For a period of time, sales of eggs from Kyoto plummeted by more than 30%. Industries with no relationship to chickens also suffered – large-scale retailers refused to sell vegetables produced in Kyoto, for example, and many travelers canceled reservations at lodgings near the area where the infection occurred.

Even as conditions gradually returned to normal after the crisis-over declaration in April, the harmful rumors continued, and in August 2004, six months after the discovery of the infection, a spokesman for Kyoto Prefecture poultry farm producers commented, “Sales have still only recovered to about 80%” (Kyoto Shinbun, 2004).

Two months prior to the avian influenza outbreak, a chicken-egg business in Kyoto Prefecture had been found to have falsely labeled six-month-old eggs. When a Kyoto poultry breeder was then found to have concealed avian influenza infection for one week, trust in all poultry farming businesses in Kyoto collapsed.

Following discovery of the avian influenza infection, television channels and newspapers carried very few reports addressing the safety of chicken eggs and chicken meat, but reported extensively on the concealment of the infection and the fact that large numbers of fowl had been shipped. In an era when harmful rumors can spread more rapidly than ever, the use of ICT is necessary to simultaneously transfer knowledge based on specialists’ opinions to large numbers of people. (Hirose & Sonehara, 2008)

This is because information, such as statements concerning the safety of a food product, can be misunderstood by some people after they hear about it through a television report or newspaper article. Such misunderstanding can then be expressed through an Internet bulletin board or personal blog, resulting in information without valid grounds being spread to a vast number of people at unprecedented speed. This can have a huge effect on confidence in the subject of the rumours.

Ordinary customers typically lack the knowledge necessary to understand management of a financial institution. For example, at the end of 2003, an incident occurred that led to a run on ‘Bank A’, a

regional bank, as the result of a single customer of 'Bank A' sending an e-mail stating that "Bank A has failed" to 20 friends. Although the bank was being managed well enough that it was unlikely to go bankrupt from a financial point of view, confidence in the bank was lost and panic ensued as a result of this point being misunderstood by ordinary customers.

Gender, Age and Ethnicity

One rather interesting aspect discovered through the course of the research for this paper is that there are very distinct differentiations between the attitudes regarding trust in Information Technology over different genders and ethnicities, upbringing and geographic location. According to Fukuyama (1995), the willingness to trust various classes of persons in the economic sphere is related directly to differences in social structure and kin relations. Laforet and Li (2005) found the issue of security to be the most important factor that motivated Chinese consumer adoption of mobile banking.

Baba (1999) found, in his case studies, that there were different 'boundary-maintaining distancing mechanisms' between co-workers, including discrimination against and refusal to interact with certain parties, throwing things "over the wall" and re-entering data manually, on-site audits, rumors of dirty dealing by or incompetence of the other party, requirements for face-to-face review of data, and differential security clearances and regulations. (Baba, Fall 1999)

According to Carey, *et al.* (2002), people that have 'utopian views' may be more knowledgeable of Internet threats through general usage of the computer and Internet. One possible explanation for users' knowledge and security practices may be drawn from theories of social inequality. (Downs, Ademaj, & Schuck, 2009)

Men have been found to be more likely victims of cyber-crime than women (*e.g.*, 57.6% vs. 42.4%), and when victimised, men tend to suffer more financial loss than women (median loss US\$765 vs. US\$552). This is likely to be due to the onset of fake love-interest E-mails. Females, on the other hand, are expected to feel more concerned about privacy than males.

Many other different social aspects have been discovered, such as: younger people are expected to be less concerned about privacy than their elders. Expert web users will feel less concerned about privacy than beginners. Frequent web users will feel less concerned about privacy than occasional ones. Users who benefit from high speed Internet connection will feel less concerned about privacy than those who have low Internet connection. Interestingly, Web users browsing for buying purpose will be less concerned about authenticity than those requiring information and those who are simply browsing at will. (Gauzente, 2004)

According to Frimpong Twum of the Kwame Nkrumah University of *Science* and Technology in Kumasi, Ghana, the majority of people aged between 20 and 40 believe that Internet banking is secure, while the majority of people over 60 believe the opposite, suggesting that age also plays a significantly-contributing role. This could also be due to the understanding of technology that those in the younger age bracket would have, having grown up with technology. This in turn could relate to the trust that older people have in the old system of physical deposits, and their unwillingness to adapt to the new changes. (Twum, 2012)

Conclusion

While there are many threats that affect the e-Commerce sector, the public should not be afraid of using the services, but rather embrace them, as there is massive potential for progress to be made. However, the public needs to understand that there are associated risks in using these services, and should be made aware of how to act accordingly. The use of IT also carries the danger of impersonalising relationships, which, in turn, could lead to reduced trust, commitment and value-creation.

Organisations should give basic Internet Technology training to all of their employees, not just those in the IT sector, as a single employee in any capacity could inadvertently have created a vulnerability that allows access to the entire company system. Because of this, employees should have their access levels broken down and isolated to only the components that they need to conduct their work. This will help minimise the loss of data should a breach occur.

For the individual, when providing private information, they should ask themselves exactly why the other party needs, and more importantly wants, the information. They should be very cautious regarding any requests for passwords or any form of monetary transaction.

Knowing what the risks are, how one's business can be vulnerable and how attacks could potentially affect that business is paramount in maintaining security. By understanding the problems, they can empower themselves to protect both themselves and their companies to deal with any security issues as they arise.

Bibliography

- Baba, M. L. (Fall 1999). Dangerous liaisons: Trust, distrust, and information technology in American work organizations. *Human Organization*, 331-346.
- Bashein, B. J., & Markus, M. L. (1997). A Credibility Equation for IT Specialists. *Sloan Management Review*, 35-44.
- Downs, D. M., Ademaj, I., & Schuck, A. M. (2009). Internet security: Who is leaving the 'virtual door' open and why? *First Monday*.
- Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 219-229.
- Gauzente, C. (2004). WEB MERCHANTS' PRIVACY AND SECURITY STATEMENTS: HOW REASSURING ARE THEY FOR CONSUMERS? A TWO-SIDED APPROACH. *Journal of Electronic Commerce Research*, 18.
- Gish, W. (2013). *The Effects of Computer Hacking on an Organization*. Retrieved from Chron: <http://smallbusiness.chron.com/effects-computer-hacking-organization-17975.html>
- Grabner-Krautter, S. (2009). Web 2.0 Social Networks: The Role of Trust. *Journal of Business Ethics*, 19.

- Griffin, P. (2013, July 27). Chaos Groups zap traditional order. *Listener*, p. 52.
- Hirose, Y., & Sonehara, N. (2008). Management of information-credibility risk in an ICT society: A social implementation. *Internet Research*, 14.
- Houser, D. (2000). Reputation in Auctions Theory, and Evidence from eBay. *Journal of Economics & Management Strategy*, 353-369.
- Jenkins, J. (2010, November 3). *Internet Security and Your Business - Knowing the Risks*. Retrieved from Symantec: <http://www.symantec.com/connect/articles/internet-security-and-your-business-knowing-risks>
- Kini, A. (1998). Trust in Electronic Commerce: Definition and Theoretical Considerations. *System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on*, 51-61.
- Kini, A. D., & Choobineh, J. (2001). An Empirical Evaluation of the Factors Affecting Trust in Web Banking Systems. 185-191.
- Roca, J. C., García, J. J., & Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, 96-113.
- Ryssel, R., Ritter, T., & Gemunden, H. G. (2004). The impact of information technology deployment on trust, commitment and value creation in business relationships. *The Journal of Business & Industrial Marketing*, 197-207.
- Sophos. (2009, December 6). *Sophos Australia Facebook ID probe 2009*. Retrieved from Sophos: <http://nakedsecurity.sophos.com/2009/12/06/facebook-id-probe-2009/> & <http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx>
- Teixeira, R. (2007, June 4). *Top Five Small Business Internet Security Threats*. Retrieved from Small Business Trends: <http://smallbiztrends.com/2007/06/top-five-small-business-internet-security-threats.html>
- Twum, F. (2012). Internet Banking Security Strategy: Securing Customer Trust. *Sciedu: Journal of Management and Strategy*, 78-83. Retrieved from Sciedu: Journal of Management and Strategy: <http://www.sciedu.ca/journal/index.php/jms/article/view/1944>
- Walton, R. (2013). How Trust and Credibility Affect Technology-Based Development Projects. *Technical Communication Quarterly*, 85-102.
- Wathen, C. N., & Burkell, J. (2002). Believe it or not: Factors influencing credibility on the Web. *Journal of the American Society for Information Science and Technology*, 134-144.