Fall 2009

Computer Crime and Identity theft

Harry A. Hunter
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Abstract

The problem at hand is the increased amount of vulnerabilities and security hazards for individuals engaging in e-commerce, business transactions over the World Wide Web. Since the majority of people aren't paying their bills by mailing in their payment to the vendor, they pay for the items they purchase online, which makes them open to hackers and social engineering attacks. They place their credit card/debit card numbers, their phone number and home address, and even their birth date information on company websites. All these security vulnerabilities make the risk of identity theft increasingly high. Identity theft is when an individual's personal (confidential) information, such as social security or account numbers, is stolen and used against them.

Acknowledgements

I would like to acknowledge all the mentors I have had in college as well as in the workplace. Thanks to them, I have been able to gain the knowledge I have needed to complete my Master's in Information Assurance. One of the mentors I would like to thank is Professor Paul Vieira. He was not only my professor for two of my courses throughout my Master's curriculum, but he motivated me to continue pursuing my studies when I was busy with work at the same time. My passion for computer security and wireless technology has enabled me to pursue a career that has rewarded me in various forms. I would like to also thank my family for believing and taking the time to encourage me to pursue a large goal in my life.

Table of Contents

Executive Summary. X

Chapter 1: Introduction. 1

Chapter 2: Review of Literature and Research. 2-13

Chapter 3: Methodology. 14-31

Chapter 4: Project Analysis and Results. 32-52

Chapter 5: Project History. 53

Chapter 6: Lessons Learned and the Next Evolution of the Project. . . . 54-57

References. 58-62

List of Figures

Figure 1- IDT Surveys- FTC 2003/Javelin 2006 Annual Rates & Cost of Identity Fraud

Figure 2- Common Forms of Identity Theft

Figure 3- ID theft by years

Figure 4- Phishing Report

Figure 5- The increase in phishing reports

Figure 6- Chart: World Growth in Mobile Subscribers

Figure 7- GVU Study

Figure 8- Security as a factor

Executive Summary

The impact of identity theft on the emerging e-commerce processes and markets is growing. More people are using mobile devices which have access to the Internet to make online purchases. Having personal information on vendor websites makes personal and confidential information vulnerable to malicious attacks by hackers. Hackers and crackers are using many different ways to access consumers' private information. Among the ways of gathering information are social engineering, phishing and pharming. Whose responsibility is it to protect the information from being stolen? Many individuals install firewall systems on their personal computers to ensure that don't get infected by viruses. Larger organizations and institutions such as banks have a responsibility to the user to ensue that measures be put in place that will lead to the reduction of identify theft and fraud. It is both the consumers' and the organizations' responsibility to ensure that they are taking every possible measure to ensure that the security in business transactions.

What measures can be taken to prevent identity theft from occurring in such large numbers? The number of attacks and the chance of identity theft and virus attacks are increasing and the importance of security is therefore becoming a central issue in all aspects of Internet privacy and online transactions. One of the measures an individual can take to ensure security is to check that any site dealing with the input of sensitive information data has a web address that starts with "https" not just "http". Government agencies are continually monitoring fraud and fraud related aspects linked to computer crime and identity theft.

Chapter 1 – Introduction

Understanding the extent of the problem with regard to identity theft is a prerequisite to insight into the other aspects of this topic. The literature points to the accelerating problem of computer and other forms of identity fraud. The general situation with regard to identity theft and fraud is summed up in the following quotation. "This 21st century fraud combines deception (aka social engineering), impersonation, and automation to steal authentication credentials such as passwords and account numbers from individuals over the Internet, and uses this information for ill gain." (Wetzel, 2005. p.46) Furthermore, various reports and studies illustrate the extent of this problem. For instance, a Federal Trade Commission survey found that "… some 30 million people have fallen victim to identity theft in the past seven years." (Young, 2005, p.86) The survey also found that "this crime is quickly becoming an epidemic because it's relatively easy to get hold of other people's personal information…" (Young, 2005. p.86)

Chapter 2 – Review of Literature and Research

The literature on the subject of identity theft and the related area of computer privacy is extensive and cuts across many disciplines and data sources. These include issues from the online and computer environment to legislation and governmental policy, as well as to the burgeoning field of the study of security and online commerce. The latter area of study has in recent years received close attention in the literature due to the increase of online fraud and security breaches.

However, at the same time many pundits point out that while there has been a surge of studies, reports and theses in the last few years on identity theft and computers, there is as yet no definitive or established body of research or documentation on identity theft. This important point is raised in an article from the Journal of Consumer Affairs entitled *How Well Do Consumers Protect Themselves from Identity Theft?* by George R. Milne (2003) Milne clearly illustrates the status of research in this area.

> The literature addressing the issue of identity theft is sparse. Law review articles have provided a general overview of the problem (e.g., Hoar 2001), while others have evaluated the effectiveness of the courts and existing statutes to provide a remedy to the victims of identity theft (e.g., Alwin 2002; Saunders and Zucker 1999). In the marketing and public policy literature, identity theft is not directly addressed. (Milne, 2003. p. 388)

The above article also serves as an excellent overview of the central issues and problems involved in the research on identity theft.

On the other hand it should also be noted that since the date of publication of this article (2003) there has also been a resurgence of articles and studies on this subject, which has become more germane to the growing field of ecommerce and individual online usage. In this regard there has been an increase in the number of comprehensive and valid online sites and database sources which provide a vast array of documentation and that deal with the fight against this type of crime, with a growing number of references and up-to-date information. There are numerous studies and reports as well as surveys that provide a general and useful overview of the problem of identity theft. For example, an article entitled, *Internet Commerce Grows 88 Percent by Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a Concern*, provides a comprehensive overview of the problem. The article deals not only with the extent of identity theft but also focuses on the important aspect of the way that security issues like ID theft are perceived and understood by the general public. As will be discussed in the various sections of this study, the awareness and the requisite knowledge about identity theft is one of the most important factors in dealing with and fighting this insidious crime.

The above article provides some insightful and relatively contemporary statistics on the extent of ID theft. For example, the author notes that in recent years the "…. United States remained the top source country for security events generated with an overwhelming 79 percent, followed by Canada (5.7 percent), Taiwan (2.6 percent), Korea (2.5 percent) and the U.K. (2.4 percent)." (Internet Commerce Grows 88 Percent by Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a Concern)

Another online source that provides a wealth of relevant and contemporary data on these issues is FraudWatch International (http://www.fraudwatchinternational.com).

This is one of the better online resources and the Identity Theft section of this site is constantly updated with some of the latest information and data and provides a wealth of information on ID theft practices such a phishing, as well as possible solutions to these problems. An article that was particularly useful with regard to ascertaining the effects of identity theft and fraud on the corporate and banking security was *Debit's Growing Popularity* by Lauren Bielski (2006). This article explores the extensive impact of identity theft and fraud on various sectors and some alarming statistics. “Looked at as a group these incidents suggest a security flame-out and the perception that electronic information housed in computers is vulnerable. They also suggest that fraud seems to be mutating at a rate…”(Bielski, 2006).

How Well Do Consumers Protect Themselves from Identity Theft? by Milne, (2003) is an article that not only exposes the various ramifications of the effects of identity theft on the consumer, but also takes an in-depth look at measures that can be used to counter this intrusive crime. Like many similar studies, the extent of the problem is reiterated in this article;” The Economist (2001) reports that identity theft, defined as the appropriation of someone else's identity to commit fraud or theft, continues to be one of the fastest growing white-collar crimes in the United States.” (Milne, 2003, p. 388) The article explores in detail the impact of this form of crime and the invasion of privacy on individual and business concerns.

It should also be noted that there are numerous studies, report and surveys that repeat figures and statistics which emphasize the increasing rate and incidence of identity theft in the electronic and digital environment. While many of these studies will be referred to in the course of the present study, this aspect will not be repeated ad nauseum

and only some of the latest and most cogent data reflecting this factor will be referred to. There are also many other general overviews and studies of the ramifications of identity theft that will be cited in this thesis.

While there are many general studies that cover a wide and diverse range of information in this field, one locus that can be used as a baseline as it were in the literature is the impact of identity theft on the emerging ecommerce processes and markets. The reason for this is that it is in this area that contemporary research on identity theft is focused due to the consumer popularity and the increased importance of online commerce and shopping for all shades and styles of entrepreneurship and business. There has therefore been more research focus on this area than any other.

In this regard a work by Miyazaki and Fernandez, *Consumer Perceptions of Privacy and Security Risks for Online Shopping* (2001) is notable. The article provides some of the most significant information on this subject area. The authors discuss the issue of online shopping and the way that identity theft has influenced buying perceptions and views. One of the aspects of this article is the clear and concise outline of identity theft and the negative impact that it has on ecommerce.

In terms of online shopping and ID theft one should also bear in mind the plethora of information from reliable and validated sources on the Internet. It is to be expected that this topic should be of particular concern to online pundits and those involved in ecommerce. One study that should be mentioned in this regard is *Online Privacy and Security: The Fear Factor* (2006) from the well respected e-marketer Web site. This particular site also provides extensive and up-to-date statistics and views for specialists in this area.

Another useful resource is, *OFT launches fact-finding market study of internet shopping*. This article from the UK Government site 'Office of Fair Trading' is a "… new fact-finding study into online shopping is launched today by the Office of Fair Trading." (OFT launches fact-finding market study of internet shopping) The site provides a wealth of data on the factors affecting ecommerce and the impact of identity theft.

Reports by research companies such as Gartner also proved to be a reliable and invaluable contribution to the research into this topic. Other research companies such as Cybersource also provide an essential service by monitoring the latest news and statistics on the situation with regard to identity theft. One cannot discount the important of Weblogs as an extremely important way of assimilating and collating important data on this topic. Even a year ago Weblogs would have been seen as a rather suspect data source. More recently Weblogs have matured and many of the specialists Blogs are a verifiable and useful source of data on the topic. For instance, the ZDnet Weblogs collect and cite reports and white papers from research companies such as Cybersource. An example is a report from Cybersource which is cited in the Zdnet weblog and which states that;

> Statistics and data abound on the various security breaches and infringements, as well as various types of fraud in online commerce. For example the research company Gartner has reported that … computer fraud increased 28% in the 12 months ending May 2005… 73 million adults report they definitely received a phishing e-mail, or a message that looked like one. More than 2 million people lost a total of almost $929 million.
>
> ($2.8 bln in e-commerce revenues lost to fraud in 2005)

Specialist Weblogs have therefore become a valuable way of monitoring various sources and consequently are a valid and important part of the literature on this subject. However, it must also be borne in mind that the authenticity of data on Weblogs is still open to doubt in some cases and only the most respected and peer - reviewed Weblogs can be used for research

As mentioned previously in this section, there are a number of areas in the literature that are in need of further in-depth research. Pundits also note that there has been comparatively little research in the relationship between privacy and security issues and consumer risk perceptions. This area of research has, according to Miyazaki, and Fernandez, also neglected that way that the perception of this relationship effects purchasing behavior. (Miyazaki, and Fernandez, 2001) "Indeed, a recent study of Internet users … was somewhat inconclusive regarding the impact of privacy and security concerns on consumers' online purchases." (Miyazaki, and Fernandez, 2001, p. 27)

There are also numerous studies which indicate that the importance of security, specifically in terms of online purchases and methods of ensuring transaction privacy, has become a central concern of ecommerce. There is an increasing realization that attention has to be given to security issues in order to build consumer confidence and to reduce the perception of risk in online sales, so that ecommerce can reach its true potential. It is also deemed to be important that the efforts made by business in this regard are seen by the public and that there is a reduction of any underlying doubt and suspicion relating to online transactions. There is the fear that if this is not achieved then media reports and

other sources may increase security fears and reduce online purchasing. As Miyazaki and Krishnamurthy in their study entitled *Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions* (2002) state:

> …changes in online retailer practices that are deemed to be consumer friendly will build confidence and reduce perceived risk in online shoppers as the shoppers encounter them via increased Internet experiences. Conversely, coverage of these issues by media sources, as well as negative online experiences, may decrease consumer confidence by highlighting the potential risks involved in online shopping and, thus, deter Internet users from making online purchases (Judge 1998).
>
> (Miyazaki, and Krishnamurthy, 2002, p.28)

An area of the literature which is of significance with regard to the individual as well as to business and government is the question of the costs that identity thefts incur. A study that sheds light on the implications in term of the costs of identity fraud to financial institutions is *Tackling Phishing: It's a Never-Ending Struggle, but the Anti-Fraud Arsenal Continues to Grow* by Wetzel (2005). An extract from this study underscores the severity of this situation. This refers not only to the obvious costs to institutions like banks, but the hidden costs that relate to the erosion of customer confidence as a result of ID theft.

> An April 2004 survey of 650 U.S. banking customers by software vendor Cyota shows that phishing is diminishing customer's trust in online interactions with their banks. In the study, 65 percent of account holders were less likely to use their bank's online services due to phishing, and 75 percent were less likely to respond to email from their bank because of phishing.
>
> (Wetzel, 2005, p.46).

Another important study that expands on the influence and impact of identity fraud is, *Is eCommerce Boundary-Less? Effects of Individualism-Collectivism and Uncertainty Avoidance on Internet Shopping* by Lim et al. This article explores the phenomenon of the avoidance of online commerce and purchasing due to the perceived threat of ID theft. (Lim, Leung, Sia, and Lee, 2004, p.545)

Another area of the literature on ID theft that is growing at an exponential rate is mobile fraud and ID theft in mobile computing and mobile phone fraud. This is a new area and one which will be discussed in the chapters to follow. The expansion of this area of research is largely due to the growth of the mobile industry in recent years; as well as the concomitant growth of online business via mobile devices. The growth of this industry has opened up new possibilities for economic development but it has also at the same time provided new avenues and opportunities for identity theft.

There are a growing number of reliable studies on this facet of ID theft. For example, an article entitled *Number Of Mobile Subscribers Worldwide To Rise To 3.96 Billion By 2011*, provides some useful background data and the outlines the potential threat of security issues such as identity theft in the expanding mobile industry. This is a

particularly important trend as it does not only apply to the United States but is also a burgeoning threat to developing economies throughout the world. This is expressed clearly in *Global Mobile Population Growing*. "This trend does not only apply to the Unites States or Western countries. The potential for mobile ecommerce and increased subscriber bases is even greater in China. In-Stat/MDR reports that Chinese handsets generated nearly $9-billion in revenue in 2003, and there are expectations that point to an amount of $16 billion being generated by 2008. "(Global Mobile Population Growing) Another study that is relevant in this regard is *Windows Wi-Fi attack discovered* by Espinar (2006)

Literature on combating the problem of identity theft

The literature on preventative methods and techniques for ID theft is possibly one of the most important areas of research and one where there is a great amount of debate and discussion. It is also the most important area of research in terms of the aims and objectives of the present study. There are numerous studies that have emerged in recent years which focus on solutions to the problem of identify theft. However, while there are many suggestions and proposals most studies recognize identity theft as a developing and ongoing threat which makes use of the latest technologies. This makes finding means of combating this threat a task that requires knowledge and awareness of how the latest technologies work and the vulnerabilities that can be exploited.

A study which explores the activities such as phishing and the problem and complexities of dealing with this issue is *Tackling Phishing: It's a Never-Ending Struggle, but the Anti-Fraud Arsenal Continues to Grow* by Rebecca Wetzel (2005) This article provides a succinct summary not only of the situation with regard to phishing

and ID fraud but also with regard to the measures and steps that can be taken to alleviate the threat. Other articles that deal with the issue of preventive measure and privacy safeguards are *Anticipating the Worst of Times* by James Radford (2001) and *What If the Virtual Walls Fall?* by Klein et al (2006)

A study which explores the various ways in which and individual can protect him or herself from intrusion and identity theft is *Consumer's Protection of Online Privacy and Identity* by Milne et al (2004). This article is a good example of studies that research the various options open to the computer user to protect themselves against identity theft. There is also a growing body of literature that deals with the attempts by government and governmental agencies to deal with the issue of ID theft. In this category of the literature one must of course include the various discussions and critiques of FACTA or The Fair and Accurate Credit Transactions Act of 2003. This important Bill is one of the main attempts by government to develop a policy to counteract identity theft and fraud in the country.

As might be expected in a rapidly transforming online world and economy, there have been numerous critiques of this Act in both a negative as well as a positive sense. This aspect will be discussed in more detail in the following sections of this thesis. One study that as found to be particularly helpful in providing an overview of the intentions of this Bill, as well as in discussing the various practical pros and cons of the Act *is Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken*, by Stefan Linnhoff and Jeff Langenderfer (2004) . This article provides a comprehensive review of the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

A related area that will also be of concern in this study is the role that larger organizations can play in the prevention of identity theft. Many studies in this regard posit the view that larger organizations and institutions such as banks have a responsibility to the user to ensue that measures be put in place that will lead to the reduction of identify theft and fraud. A useful study which covers much of the ground of this topic area is Lacey, D. and Cuganesan, S. (2004), *The Role of Organizations in Identity Theft Response.* In a similar vein there are also various studies that assert that the only real and viable response to identity theft lies in a synergistic and integrative approach and strategy, which includes the full participation of all those affected by ID theft. This is an important issue that will form much of the focus of the present study.

There are a range of journal articles and studies which relate to both the impact of ID theft as well as preventative measure that can be taken on many different levels. These include the following: *Identity Theft Really Affects Your Lifestyle* (2003) by David Breitkopf; *Identity Theft Survey Report*, prepared by Synovate (Aegis Group plc). (http://www.ftc.gov/os/2003/09/synovatereport.pdf); and *Identity Theft: Investigation and Preventative tools* from the 2006 National Community Policing Conference. (http://www.cops.usdoj.gov/mime/open.pdf?Item=1775)

Figure 1. IDT Surveys

IDT Surveys - FTC 2003/Javelin 2006
Annual Rates & Cost of Identity Fraud

	Mean cost per fraud victim	Fraud victims as percent of US adult population	US adult victims of identity fraud	Total one year fraud of cost
2003 Survey	$5,072	4.7%	10.1 Million	$51.4 Billion
2006 Survey	$6,383	4.0%	8.9 Million	$56.6 Billion

(This figure was retrieved from the following website: http://www.cops.usdoj.gov/mime/open.pdf?Item=1775)

Identity theft has traditionally occurred through offline methods, however, the "…online data collection of stolen identities can be easier and more efficient for thieves… with new approaches and scams being created and implemented under the cloak of electronic anonymity." (Milne, Rohm & Bahl, 2004. p217)

One of the aspects that should be considered is the effect that this practice has on the individual user, as well as on the business or organization and the society in general. "Identity theft threatens the very essence of an individual's sense of self and his or her capacity to participate in society. The consequences of this form of criminality are

significant and wide-ranging, with current assessments of its impacts exceeding billions of dollars each year…" (Lacey & Cuganesan, 2004. p.244) Lacey & Cuganesan (2004) describe some of the traumatic effect on the individual of this form of crime.

Identity theft is commonly defined as a crime that occurs "… when someone acquires your personal information and uses it without your knowledge to apply for credit cards, make unauthorized purchases, gain access to your bank accounts or apply for credit and obtain loans in your name." (Identity Theft) As have been referred to in this study, there has been a dramatic increase in Identity theft or ID theft in recent years. Statistics show that this threat has grown by more that 40 percent compared to 2003. The FTC (Federal Trade Commission) estimates "…that 4.7% of the U.S. population, or 10 million people were victims of identity theft in the last year, with total losses of US$53 billion, US$5 billion of this were losses by victims, the remaining losses were picked up by businesses." (Identity Theft)

This data therefore shows that ID theft is particularly insidious form of online security risk and has an important impact on the individual as well as on business and online shopping. This is due to the fact that ID theft provides various benefits for the criminal. These include the following aspects.

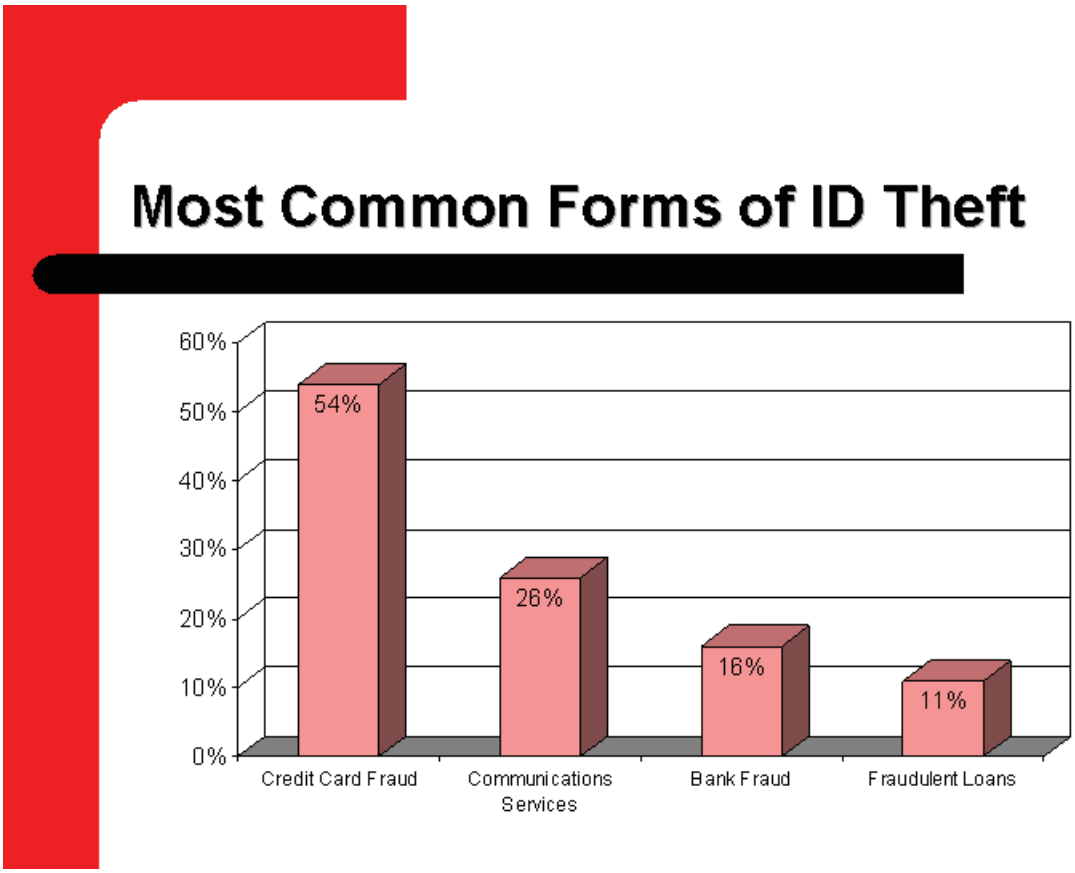
- The anonymous nature of the crime - allowing criminals to hide their true identities while they pursue illegal activities,
- The ease in committing the crime in this technological era,
- The relative ease to financially support themselves with fraudulent loans or credit card purchases.

(Identity Theft)

This form of theft has a devastating effect on the victims. Firstly the victims often do not find out about the theft until it is too late and they are turned down when attempting to obtain credit. Even more devastating is the fact that victims are often not able to get new credit cards or fail in their applications for loans due to their credit rating has been destroyed in the process. (Identity Theft) Personal problems for the victims also include "…. problems obtaining or using a credit card, harassed by collectors, rejection of finance, banking problems, insurance rejection, having utilities cut off, civil suits filed and criminal investigations." (Identity Theft) Milne (2003) also reiterates the way in which the consumer can be harmed by identity theft. "(1) having their privacy invaded, (2) suffering the psychological trauma of having their reputation ruined, (3) incurring financial liabilities, and (4) undergoing tremendous transaction costs to restore their names." (Milne, 2003)

It is therefore obvious that the danger of ID theft on the Internet is an aspect that can reduce the number of people who prepared to interact and do business online and who feel safe when using their credit cards online. Credit card fraud is one of the most common forms of identity theft; but it is not the only kind, as the illustration below indicates. However, the fact that the most common type of ID theft is credit card fraud, places the focus on online payment methods, which most often use this form of payment.

Figure 2- Common forms of ID theft



(This bar graph was retrieved from the following website: http://www.ftc.gov/os/2000/07/images/idtheft6.gif)

There are many reports which state that the awareness of identity theft particularly among consumers and shoppers has possibly become one of the central issues in ecommerce and security.

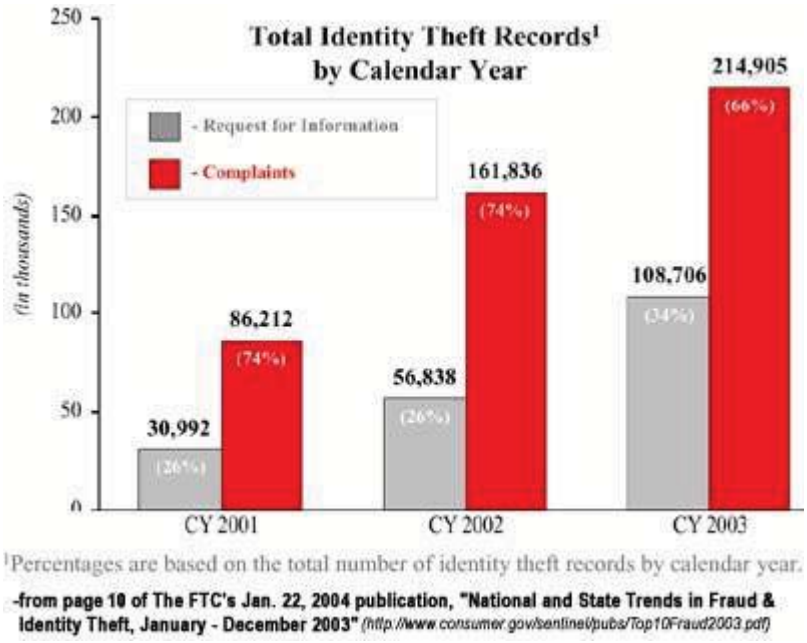
The fear of identity theft has gripped the public as few consumer issues have. Consumers fear the potential financial loss from someone's criminal use of their identity to obtain loans or open utility accounts. They also fear the long lasting

> impact on their lives that results from the denial of a mortgage, employment, credit or an apartment lease when credit reports are littered with the fraudulently incurred debts of an identity thief.
>
> (PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT….) [1]

The above data indicates that the online environment has increased the potential and the possibility for fraud and identity theft which has had a resounding effect on the importance of security systems and the way that they are implemented; and particularly the way that this implementation is perceived as being effective by the public. Identity theft has also been shown to be on the increase over the years. The following graph provides a clear indication of this increase

Figure 3. ID theft by years

[1] See Appendix, figure 1. The rise in security issues.



(This bar graph was retrieved from the following website: http://www.ou.edu/oupd/idtheft3b.htm)

Phishing and Pharming

The term 'phishing' refers to a slang word in IT technology which actually refers to "fishing for information." This usually refers to "phishing" for credit card numbers and other sensitive information that can be used by the criminal. Phishing attacks use "…spoofed emails and fraudulent websites to deceive recipients into divulging personal financial data, such as credit card numbers, account usernames and passwords, social security numbers etc." (Prevent Identity Theft and Safeguard Information Assets)

Phishing emails are "commonly used in association with a fake web site that looks very similar to a real website from the relevant institution." (What is Phishing?) The following is an example of phishing which focuses on the inculcation of fear in the recipient of the phishing attack.

> A typical phishing sends out millions of fraudulent e-mail messages that appear to come from popular Web sites that most users trust, such as eBay, Citibank, AOL, Microsoft and the FDIC. According to the Federal Trade Commission, about 5% of recipients fall for the scheme and give information away. Phishers wish to irrationally alarm recipients into providing sensitive information without thinking clearly about the repercussions. Victims might be told someone has stolen their PIN and they must click on the provided link to change the number.
>
> (Thompson, 2006. p. 43)

Once the criminal has obtained the information they can use it, for example, to make unauthorized purchases or to simply withdraw all the money for the victim's bank account. The information can also be sold to other parties. There are numerous studies that show the devastating effect that this practice has on the consumer and on the perception of online security. Fraud Watch International states that, as of the 24th of July, 2006, there have been more than 53,912 cases of phishing in the United States. (What is Phishing?) Studies also show that incidents of this crime are on the increase in other parts of the world beside the United States.

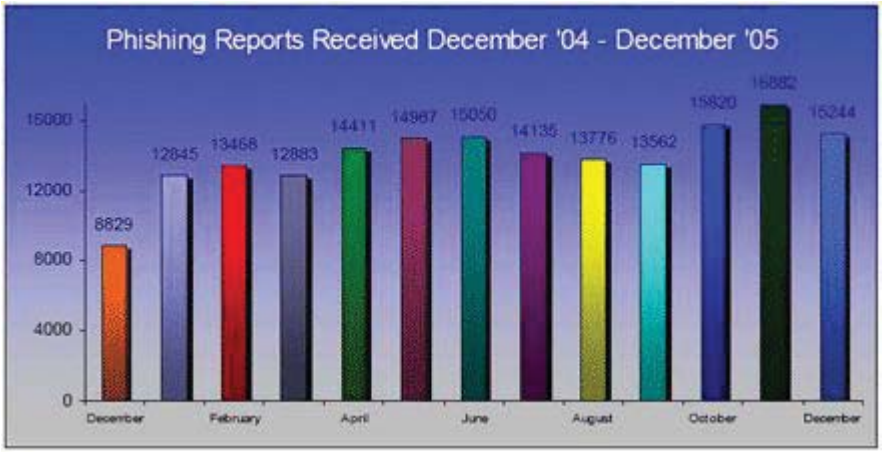
> Phishing and spyware seem to be the biggest challenges that corporate India is facing today. About 74% of IT managers across India report that their employees have received phishing attacks via e-mail or instant messaging on their office PC….32% of employees in India admitted to have given out their confidential data such as credit card numbers and corporate network passwords as a result of

phishing…

(74% IT managers receive phishing attacks)

One of the many reliable sources with regard to figure and statistics on this topic, the research company Gartner, recently produced the results of a survey of 5, 000 American adults, which showed that phishing attacks had grown at double-digit rates in the United States. ($2.8 bln in e-commerce revenues lost to fraud in 2005) The report stated that "…in May 2005, an estimated 73 million US adults who use the Internet said they definitely, or think, they received an average of more than 50 phishing e-mails in the past year. The number of consumers receiving phishing attack e-mails increased 28% in the 12 months ended in May 2005 compared with 12 months ended in April 2004…" ($2.8 bln in e-commerce revenues lost to fraud in 2005) An important factor in terms of business and ecommerce is that the report also found that 2.4 million online users reported losing money as a result of phishing attacks and about 1.2 million shoppers and consumers lost approximately $929 million in 2004. ($2.8 bln in e-commerce revenues lost to fraud in 2005)

Figure 4. Phishing report.



(Anti-phishing Working Group. This figure was retrieved from the following website: http://www.finjan.com/Content.aspx?id=180)

The study was based on a survey of 655 respondents conducted by Infosurv, an online market research company, and found that, among others,

- 44 percent of online banking customers use the same password for multiple online banking services. A password obtained by fraudsters can be used at a number of banks.
- 37 percent of online banking customers use the same password at other, less secure sites.
- 70 percent of account holders are less likely to respond to an e-mail from their bank, and more than half are less likely to sign up or continue to use their bank's online services because of phishing.

(Phishing Attacks Surge in Last Six Months)

The negative impact of phishing on online shopping is evidenced by many reports.

> Unfortunately, it seems that a popular online fraud scheme called phishing is keeping many potential holiday shoppers away from online stores. A survey commissioned by e-mail security vendor MailFrontier Inc. and conducted in October found that 29 percent of respondents decided not to shop online this holiday season out of concern over phishing schemes, in which scammers trick individuals into revealing sensitive personal and financial information by tricking them into visiting what look like legitimate Web sites.
>
> (New holiday online shopping trends emerge.)

Needless to say there are numerous studies that point to the increasing cost of phishing, not only the individual but also to the commercial institutions that are negatively affected. [2] "Phishing costs victims and financial institutions money and time. Victims must correct credit records and repair other phishing-related damage, while financial institutions must absorb customer losses, as well as costs from issuing new credit cards, answering calls and shutting down fraudulent websites. "(Wetzel, 2005, p. 46)

The cost to financial institutions is extensive, as phishing and other forms of identity fraud can reduce the trust between the client and the organization or

[2] Refer to Figure 1 above.

company.

> For financial institutions, of even graver concern than direct costs is the erosion of trust in online communications and transactions. Suspicion of legitimate online interactions between customers and their financial institutions is driving consumers from online banking to more expensive and labor-intensive channels such as telephone call centers or "bricks and mortar" branch offices.
> (Wetzel, 2005, p.46)

However, the costs incurred by phishing vary according to different studies. The research group Gartner, for example, estimates total U.S. phishing-related losses during 2003 at some $1.2 billion, Another study by the Ponemon Institute estimates total consumer losses as of September 2004 at $500 million per year, and a study by Financial Insights expects 2004 losses to tally as high as $400 million. (Wetzel, 2005, p.46)

Pharming is similar in some respects to Phishing. Pharming refers to the redirection of legitimate Web sites to false online addresses. Pundits claim that pharming can even fool experienced computer users and could become one of the most insidious privacy and security threats yet. Experts also state that pharming attacks are on the increase. Statistics from SANS Internet Storm Center indicate that at least 1,300 sites were compromised through pharming attacks in early March, 2005 (Anonymizer Now Protects Against Pharming Attacks)

Lee Itzhaki director of product management at Anonymizer Inc. states that "the rise of online shopping, Internet banking and electronic bill paying has created a large target for criminals to capture login information, credit card numbers, and more." (Anonymizer Now Protects Against Pharming Attacks)

Pharming works in the following manner: when a user correctly enters a web address to access online information about his bank and credit cards, it is probable that the web site that appears may be a sham and operated by scammers. The user assumes that the site on which he or she is entering the data is authentic, as it is a perfect replica of the legitimate site. The user then enters his or her credit card details or other sensitive information, with obvious consequences.

Pharming can be initiated in two ways. The first is when a small program is installed on a computer without the user's knowledge. The second way is though computers that deal with Web addresses, which can be harnessed and manipulated to send the user to a false site. The technique takes advantage of the fact that although websites have alphanumeric names the actual addressing is done with a sequence of numbers called an Internet Protocol, or IP, address. The computers that translate the names into IP addresses, known as Domain Name System servers, which are 'manipulated' to translate a particular name into a different numerical address, sending a user to a different and fake site. In other words, pharming attacks "poison" servers. This is achieved by changing the numerous addresses within large servers, for example on a bank's Web site, and by redirecting clients to a fake Web site. Passwords and information are then requested and identity theft takes place.

Both phishing and pharming redirect the user from authentic Web sites to phony sites without their knowledge. Pundits note that the most alarming aspect of pharming is, unlike phishing attacks, that this threat does not rely on the user taking any action; for example opening an e - mail. This means that the pharming attack can go completely undetected. “It is also very difficult for victims to detect – until they discover an unexpected hole in their finances, or a black mark on their credit rating.” (Pharming protection for internet users)

There are a number of prevention techniques that can be used. Among these are checking that any site dealing with the input of sensitive date has a web address that starts with “https” not just “http”. The former indicates a secure site. However, pharmers might also have their own secure site. One can also double-click on the padlock icons at the bottom of the page to check on the owner of the security certificate. “A fake site either won't have a certificate or it will be owned by an entity, possibly foreign, that appears unrelated to the site you want.” (New crop of thieves: Pharmers hit Net banking)

Figure 5- The increase in phishing reports.

(This chart was retrieved from the following website:

http://www.answers.com/topic/phishing)

Other security issues

The above is a brief description of only a few of the most common and often most dangerous security threats that can face the Internet user and which can threaten privacy and identity . There are many other security issues that have also become a problem with regard to potential identity theft. Hackers, for example, are computer experts who are able to find ways to access data from online users, often using unconventional methods. Viruses and Trojans are threats that are well known to online users. However, the threat of viruses has increased in recent years and there is a general acceptance that they have become more sophisticated and prevalent than ever before.

Other new security dangers include spyware and malware. The term spyware refers to:

> …a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party. (Spyware)

Another definition of spyware provides greater insight into its potential damage to online users.

> Spyware is a class of malware that collects information from a computing system without the data owner's consent. This data often includes keystrokes, screenshots, authentication credentials, personal email addresses, web form field data, Internet usage habits, and other personal information. Often, the data is delivered to online attackers who sell it to others or use it themselves to execute financial crimes, identity theft, or use it for marketing or spam. (Hackworth A.)

Therefore spyware which is often attached to emails makes it possible for criminals and hackers to view the contents of a user's computer. More importantly, private information such as credit card numbers is at risk. "When consumers provide credit card and personal information to Web sites, this information can be intercepted if the transfer is not encrypted using SSL (secure socket layer) protocols. Privacy can also be compromised with cookies that allow others to track clickstream history. "(Han J.)

It is estimated that as much as 52 percent of computers have been infected by spyware in some form. According to a recent survey, conducted by Websense Inc,"…32% of employees in India admitted to have given out their confidential data such as credit card numbers and corporate network passwords as a result of phishing". (74% IT managers receive phishing attacks)

However, there are often erroneous perceptions of security threats among many online users. An example of the way in which the risk perception of online security is possibly exaggerated by lack of knowledge and experience is the use of cookies. A cookie is defined as, "A message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server" (Cookie). The central purpose of a cookie is "…to identify users and possibly prepare customized Web pages for them. "(Cookie)

Cookies are in fact relatively innocuous bits of information that are stored on a user's computer by a Web site with the intention of identifying visitors and personalizing online shopping. Therefore ordinary cookies do not invade privacy in a malicious way and they cannot access information that is not already provided by the customer. Once the true nature of cookies are understood this tends to reduce the fear of intrusion considerably. However, this does not mean that other forms of malware and spyware cannot be security risks.

On the other hand, however, the view is also prevalent from many major research groups, such as Gartner, that "There's definitely a reason for both consumers and merchants to feel more concerned about data security and privacy issues compared with previous years…" (Vijayan J.)

Mobile threats

There has certainly been a rapid increase in the number of mobile users in the world over the past few years. Commentators and pundits are of the opinion that mobile usage shows increasing signs of becoming the dominant trend in online computing. For example, in a report from 2005, it was estimated that there would be more than 2-billion subscribers to mobile telecommunications services by the end of that year. (2 billion mobile subscribers by end of 05) An indication of the radical increases in the mobile environment is that there were already about 1.5 billion subscribers by June of 2005. In statistical terms this suggests that during that year there were more new subscribers to mobile services each month than was the case in the entire 2004. More importantly, the study also predicts, on the basis of present trends that by 2010 there will be over 3-billion subscribers to mobile services. "This is a penetration rate of nearly 43% of the total global population." (2 billion mobile subscribers by end of 05)

Another survey by In-Stat/MDR (instat.com) estimates that the global wireless market is expected to add an average of 186 million new subscribers each year, which will result in a total of more than 2-billion by 2007. (World Market Data, Quotes And Domino Buzzwords) In a 2006 study, Portio Research predicts that, " … 50% of the world's population will be using a mobile phone by the end of 2009…" and that the number of number Of Mobile Subscribers Worldwide will increase to 3.96 billion by 2011. (Number Of Mobile Subscribers Worldwide To Rise To 3.96 Billion By 2011)

These statistics and data are also borne out in recent reports on various areas. A 2006 BBC news report states that "More than 90% of UK mobile users cannot get through the day without using their phone…" (Britons 'dependent on mobile use') The

important issue with regard to this study is that, at the same time that there are numerous reports and studies which reflect the increase in the business potential for mobile usage and the increasing amount of mobile users throughout the world, there are also increasing concern about the security issues that accompany these commercial prospects.

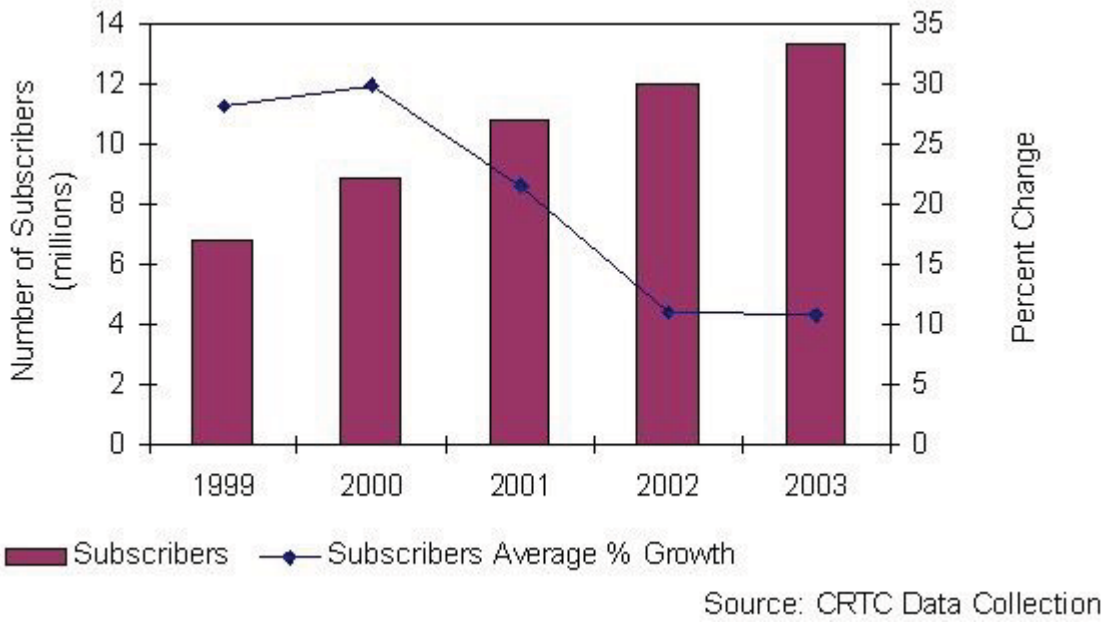
Reports from experts in the field of online security suggest that mobile devices are facing new and malicious security threats. For example, the view that 2006 and 2007 can expect to see more mobile malware has been suggested by McAfee Avert Labs. They state that the number of malicious software programs threatening mobile devices could reach 750, compared to 225 at the end of last year. One reason given for this is the increase and proliferation of Smartphone technology. Experts also expect the threats to translate rapidly to converged strategies such as cellular/Wi-Fi devices. (Malicious Software Expected to Increase)

Therefore the issue of security and identity protection is becoming serious in terms of mobile computing and mobile transactions. The increase in the use and subscriber base for mobile devices has also meant the increase in ecommerce using these devices. While this provides a potentially lucrative field for the entrepreneur, it is also an area that is highly susceptible to fraud and identity theft, among others. Therefore the same principle that increased online access can mean potentially greater security risks, also applies to the new and burgeoning arena of mobile computing.

There are numerous reports and studies that attest to the above view. Besides the security issues that have already been mentioned with regard to mobile services, there are also various other aspect that are possible security risks. ”The physical devices themselves have to be protected, along with the data stored on them, the users and the

network connections, especially wireless." (Cox. J.) Furthermore, there are presently reports of new spyware products which can be used on mobile devices. One of these is a program "…designed to help people spy on their loved ones' mobile phone usage…" (Hines M.) This is raising concerns in the industry that programs like these may pose a new threat to mobile computing. In essence, as mobile phone software becomes more technical and widespread, unfortunately so do vulnerabilities to security and ID threats.

Figure 6- Chart: World Growth in Mobile Subscribers



(This bar chart was retrieved from the following website: http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2004/image665.jpg)

The malware threat to mobile system was first discovered in 2004 when it was found that malware could affect Symbian operating systems. Recently experts have

detected a new group of viruses spreading on Symbian Ltd. smart-phone devices. (Triple Trojan Threat Calls on Symbian Cell Phones) Symantec Corporation has also reported that latest malware is capable of seriously affecting and disrupting Bluetooth-enabled Symbian devices. The Symbian operating system powers some cell phone models manufactured by Nokia, Siemens AG, Sony Ericsson Mobile Communications AB, Motorola Inc. and Panasonic Corp. of North America. (Triple Trojan Threat Calls on Symbian Cell Phones) In a related report, Tom Espiner of ZDNet states that the windows Wi-fi feature contains a potential vulnerability. "A Windows feature that automatically searches for Wi-Fi connections can be exploited by hackers, a security researcher has warned." (Espiner T. 2006)

Chapter 3 – Methodology

In 2008, 10 million Americans were affected by identity theft and each year, businesses around the world lose over $220 billion due to identity fraud. Identity fraud is an ongoing problem that must be addressed. Credit cards are primary means of buying things on the Internet. Credit card information is what is most often stolen in a data breach case. If someone is constantly connected to the Internet, they should invest in personal firewall protection. The hackers and crackers have their computers scan the Internet to find helpless computers they can hack into for personal information, such as Social Security numbers and credit card numbers.

Identity theft awareness is at all-time high due to several visible incidents in the United States. For the individual victims of identity theft, the repercussions are best time- consuming and annoying and worst of all they can be damaging to a person's financial history. In addition, another set of victims consisting of retailers and financial institutions have had to absorb millions of dollars due to fraudulent actions by perpetrators of identity theft.

Many of the recent newsworthy identity theft incidents occurred, because enterprises entrusted with the Personally Identifying Information (PII) of individuals did not adequately protect that information. Recent legislation compelling public disclosure of such incidents means that an enterprise's mistake with PII data can expose that organization to extensive financial losses, a loss of trust with customers, partners, employees and shareholders, significant amounts of terrible press, and even criminal charges.

Privacy architecture protects and governs the use of PII. The components of the organization's privacy architecture should compliment one another and be designed to realize the same overall goals. The first component of privacy architecture is made up of a privacy policy. This document will define what the PII consists of, how much information can be used, and how it must be protected. Business controls and processes that define how the business itself will collect, manage, and use PII are the second component of the privacy architecture, and should be created to fulfill the strategy and privacy policy across the enterprise. The third component, the technical infrastructure consists of the hardware and software infrastructure over which PII data is going to be stored, passed on, and operated. The infrastructure should then be designed to enforce the privacy controls that have been established.

An organization's privacy architecture should consist of a persistent effort to understand the nature of the privacy risks facing the organization, an assessment of how

best to collect and secure PII, and constant education regarding privacy issues for employees who might come into contact with PII. The first assessment and implementation of the enterprise privacy architecture must then be followed with caution and audit to ensure that any continued gaps in the program or breaches are identified and addressed. Like any other characteristic of an organization's information security program, managing privacy risk is a repeated activity, rather than a one-time task.

Most companies do not have any single point of ownership for any privacy issues that may appear. The lack of privacy ownership within the organization can aggravate incident prevention, because in the absence of clear privacy leadership, privacy concerns will tend to not be taken as seriously. The organization should avoid a situation in which all security and audit teams believe that privacy is “someone else's problem” and therefore nothing ever gets done to address privacy challenges. Many organizations have established a chief privacy officer (CPO), or have given the responsibility for privacy to a chief security officer (CSO). This type of clear ownership is necessary so that all organization have an unambiguous source of privacy direction within the organization.

The present study has also shown that there are many measures that both the business concern and the customer can take to prevent identity theft. This includes preventative techniques such as firewalls and software which detects and prevents phishing and other attacks on privacy. There are also a host of studies that suggest practical ways of preventing ID theft. Users are encouraged for example to be very attentive to the fine print and policies on Web sites that offer online transactions in order to make sure that the privacy and security are adequate. (Adkins S.)

What is encouraging is that online users are beginning be more knowledgeable about security issues and procedures to protect their information as the Internet and online shopping become more ubiquitous. The link between knowledge and actuality and a more realistic perception and understanding of the realities of online securities are being better understood. There are also increasing signs that the ecommerce and retail industry are also realizing the importance of consumer perceptions and there is a greater emphasis on the education of consumers and online shoppers.

In summary the above research points to a number of central concerns. The first is that security and Identity theft is still a major issue in the development of online shopping and ecommerce as well as in ordinary computer usage. To reiterate, the result of a recent survey of consumers shows that "…although 78 percent of U.S. Internet users plan to shop online this year, more than 69 percent of those shoppers will limit their online purchasing because of concerns associated with the safety of their personal information." (Vijayan J.)

On the one hand the customer needs to be able to distinguish between the real and fictitious realities of online security. This can only be achieved through knowledge and through experience on the Internet. Research has established that there are many myths about the extent of security risks related to online shopping. It is also equally true that with the advent of mobile commerce there are new and increasingly sophisticated methods of breaching privacy and security. Hackers are becoming more adept each year at finding easy ways of obtaining private information and breaching security. As has been evidenced in the above study, this fact is becoming even more of an issue than ever

before. The increase in the highly vulnerable mobile computing and shopping market is also another factor that tends to increase the importance of attention to and awareness of online shopping risk, rather then a reduction of these concerns.

In order to change this situation there is a need for responsible action on the part of the commercial sector, as well as from the side of the customer. The commercial concerns need to ensure that the client can conduct online transactions in safety – or at least as safely as would normally be the case in the offline environment. This also implies that shoppers must also take the necessary precautions, such as the installation of a firewall as well as various software programs to guard against internal and external attacks on security.

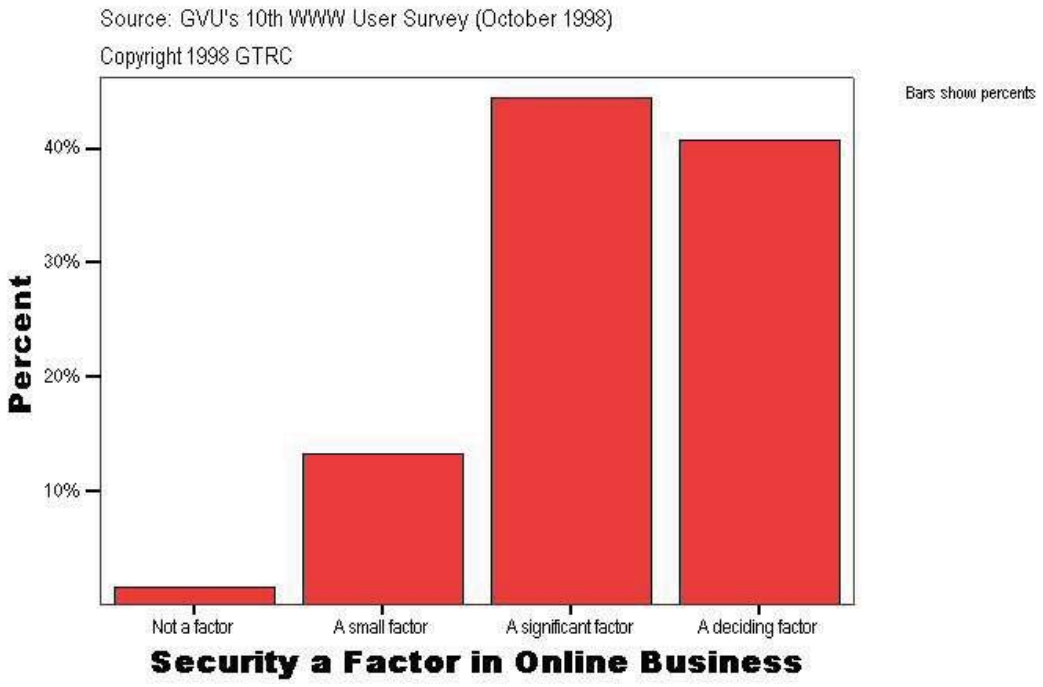
There is also a greater consciousness today of the need for an integrated approach to combat these security threats. For example there have been reports of cohesive and integrated efforts by various related stakeholders to improve online security. One report states that. " Several public and private organizations banded together to launch a new anti-Internet fraud initiative for consumers …" (Wagner J.) This report also refers to a combination of interested parties that have come together to educate consumers about the dangers of online security as well as about the type of unsafe Internet practices which can lead to ID theft and other dangers. "The FBI, Monster Worldwide … the National White Collar Crime Center (NW3C), the U.S. Postal Inspection Service, Target Corp. … and the Merchant Risk Council established LooksTooGoodToBeTrue.com, a Web site containing a variety of educational tools to keep consumers safe from fraudsters."(Wagner J.)

However, what the literature on this topic shows time and again is that all the various methods, while partly successful, are not sufficient to deal with the problems. It must also be borne in mind that the method and the sophistication of ID theft are on the increase and that no one individuals or company can keep pace with all the latest developments. Therefore in the final analysis identity theft is a problem that has to be shared. In the first instance the individual and consumer should be educated about the threat of ID fraud and at the same time there should be better and more accessible ways of cooperation and interaction between government, business and organizations; and this collaboration should be passed onto the consumer.

Chapter 4 – Project Analysis and Results

The issue of security has become a particularly important area of concern for online shopping and ecommerce. Business concerns have become increasingly aware of the damaging effects of identity theft and other forms of privacy invasion. There are various studies which clearly indicate the importance of security measures for business. Studies conducted by the GVU Centre, for example, indicate that online security is a critical factor in for business.

Figure 7- GVU Study



(Source: Security a Factor in Online Business)

The above chart indicates strongly that most of the responses to the GVU study saw online security as an important aspect of commerce. This is supported by data which shows that online security is in fact a deciding and crucial factor in the short and long term assessment of businesses on the Web.

Figure 8: Security as a factor

Security a Factor in Online Business

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not a factor	23	1.6	1.6	1.6
	A small factor	197	13.3	13.3	14.8
	A significant factor	658	44.4	44.4	59.2
	A deciding factor	604	40.8	40.8	100.0
	Total	1482	100.0	100.0	

(This figure was retrieved from the following website: http://www.gvu.gatech.edu/user_surveys/survey-1998-10/graphs/privacy/q16.htm)

The importance of security for online business and ecommerce is therefore seen from both the point of view of the user and the business enterprise as an essential component of online transactions. This is repeatedly stated by a wide range of reports and studies over recent years. “The issues of privacy and security have been labeled by government and consumer organizations as two major concerns of e-commerce…” (Miyazaki, and Fernandez, 2001, p. 27)

A central concern that has become one of the major issues in online trading is that of privacy and the ability of the business or online seller to ensure that there is no interference or transgression of a customer's private details – such as credit cards numbers. Without the necessary protection for online credit transactions there can be no assurances that would inspire online shoppers to make use of Internet sites. "The privacy of consumer information that is collected for commercial purposes is seen as a distinct consumer right from both legal and ethical perspectives. In addition, the secure storage and transmission of consumer information is seen as an integral step in maintaining that privacy …." (Miyazaki, and Fernandez, 2001, p. 27)

This need for security expressed by consumers and shoppers has been acknowledged by business and ecommerce vendors. There are an increasing number of reports and studies focused on consumer views and opinions, which suggest that "…these issues may play a significant role in the development of online retailing." (Miyazaki, and Fernandez, 2001, p. 27)

There is therefore little doubt that security issues and the role of business and retailers to protect customers against privacy invasion from the growing plethora of fraud and credit card infringements, is a central concern in contemporary ecommerce. As one study clearly states:

> Compliance pressures have led bankers (and the rest of corporate America) to seek out better ways to secure data while continuing to deliver online services and to generally function, as most companies do, in an increasingly paperless way… companies are to the point where active grousing about fallout from recent

> security faux pas have made outwitting fraudsters, hackers, and malicious insiders a higher priority…
>
> (Bielski, 2005, p. 7)

However, the following important point is also made by Bielski (2005): "Yet comparatively few [in society] are aware of the risks imposed by distributed computing. That puts all of us in a more vulnerable position." (Bielski, 2005, p.7) This is an aspect that goes to the very heart of the present study. The threat of identity theft through the use of distributed computer networks is an area, as was pointed out in the literature review section, has as yet not been fully researched or documented. Simply stated, it is the lack of awareness of the potential for identity theft that is the greatest weakness that is faced by both the individual and the business concern.

In the light if the above view it follows that the perception from the point of view of the purchaser or individual user is also a determining factor in the assessment of whether security issues are affecting online shopping in a negative sense.

However, the central aspect that plagues most first-time shoppers is security and the question of trust with regard to the results or the outcomes of the transaction. (Lim, Leung, Sia, and Lee) In other words, will his or her information or money be stolen or diverted in some way without the knowledge of the customer? Therefore, ecommerce and online business has to ensure the development of a sense of trust in their security mechanisms and process. Trust has become a crucial part of the relationship between the client or customer and the online business.

> Trust is a valuable facilitator of many forms of exchange (Doney et al., 1998; Griffith et al., 2000; Marshall and Boush, 2001), primarily because in uncertain environments, trust reduces uncertainty and hence perceived risk. With the inherently high uncertainties involved in Internet shopping, trust becomes critical to the success of an online business
>
> (Lim, Leung, Sia, and Lee, 2004, p. 545)

Furthermore, trust is defined as the "… willingness of a consumer to expose him/herself to the possibility of loss during an Internet shopping transaction, based on the expectation that the merchant will engage in generally acceptable practices and will be able to deliver the promised products or services. "(Lim, Leung, Sia, and Lee, 2004, p. 545) To develop and maintain this sort of customer trust is an essential part of the success of any modern online enterprise. To this end online companies attempt to upgrade their security systems and ensure the customer that his or her transactions are completely secure in order to eradicate the uncertainty factor.

One of the ways that business is addressing this issue is through increasing their authentification certificates. This is based on the fact that third - party certification of the site security from hackers has boosted sales on some sites by as much as 20 percent. (Online retailers enjoy 20 percent sales boost…) For example, one company states: "…participating retailers recorded an average increase of 20.4 percent in number of sales after visitors saw ScanAlert's HACKER SAFE certification mark." (Online retailers enjoy 20 percent sales boost) Studies indicate that sites that pay attention to

authentification tend to be more successful and attract more online shoppers. As one ecommerce company spokesman states "We've all seen statistics where consumers say one of their biggest concerns with shopping is online insecurity. The fact is that these concerns hold back Internet sales. Posting a certification logo addresses those concerns…" (Giesen, L.)

Research has further emphasized the significance of authentification logos on business sites. A study by the London-based TNS PLC, a market research company, in a study in April, 2005 found that "… 75% of online shoppers surveyed say they have abandoned a retail site at one time or other due to security concerns. When those customers who admitted to site abandonment were questioned further, 90% said they would have gone ahead with the sale if they had seen a recognized security market…" (Giesen, L.)

Another essential method used by business against ID theft is the firewall. A firewall is essentially software or hardware which monitors and protects against unauthorized intrusion and attacks. This form of protection has become a requisite form of the fight against hackers and intrusive programs that try to insinuate themselves on a user's computer. The plethora of virus protection programs have become common and required protection on all computers and particularly in a business environment where online transactions and identity can easily be compromised.

There is also the need for institutions and ecommerce to find solutions to the perceived risk of online shopping security. For example, many Internet users feel that banking institutions should implement more comprehensive security measures. On the other hand there is also the responsibility from the side of the user to ensure that he or she

is doing enough to prevent any identification theft or not providing any avenues for the criminals to access private information. In this regard there are various measures that the online user can take to protect against security infringements. These aspects will be discussed in the last section of this study.

There is also a consensus among online shoppers that it is the responsibility of the cyber-business to ensure protection against security threats. In one survey it was found that, "…84% of respondents to the Forrester survey said they don't think retailers are doing enough to protect their customers online." (Giesen, L.) This has resulted in a concerted effort by many companies to provide the maximum amount of security to clients to offset any perceptions of risk. This is often achieved by security audits by companies as well the popular methods of security authentication. "In some cases, these companies conduct full-blown security audits and in other cases, they authenticate the identity of the retailer to fight against phishing or other scams where criminals set up web sites pretending to be legitimate retailers, with the sole purpose of stealing credit card numbers." (Giessen, L.)

Large companies have taken to extreme measures to allay the fears of consumers and to persuade them that online shopping is a more secure and comfortable process. For example many companies protect their customers through a technology called SSL or Secure Sockets Layer. SSL is described as;

> …a set of rules followed by computers connected to the Internet. These rules include encryption, which guards against eavesdropping; data integrity, which assures that your communications aren't tampered with during transmission; and

> authentication, which verifies that the party actually receiving your communication is who it claims to be.
>
> (Online Shopping)

In essence SSL is intended to protect transactions in the process of transmission. Despite these important precautions in general it has been found that while the popularity of online shopping is increasing as well as a general growth of faith in online security, there are also many users who are not convinced of the security of online transactions. This leads to the issue of uncertainty and risk perception among online shoppers.

However while all of these security methods are regularly employed by almost all businesses that have to deal with online transactions, yet, as has been shown in this section, the case of fraud and ID theft continues to increase. This has led to the realization that new and more extensive strategies are needed in business.

The point that many ecommerce retailers and service businesses make is that, while the business Web site can protect the user from immediate security threats during shopping and conducting online transactions, yet in the present climate of increased security risk it is also incumbent on the user to take the necessary security precautions. This also applies to spyware or malware attacks. In other words, if the consumer allows or does not take the steps to protect his or her computer system from programs or malicious code that may lie dormant and compromise credit card and other sensitive information, then there is little that the online retailer can do. This again boils down to the issue of sufficient knowledge and an understanding of the realities of the online environment as well as the way that security affects Internet functions.

In general there is also a growing awareness in the business community in general that greater measures have to be taken to reassure and ensure customers of their online security. “For the business community, the implications … are that companies such as online content providers, retailers, and credit card firms must take responsibility …for the security of sensitive customer information in the …online context.” (Milne, George R., Andrew J. Rohm, and Shalini Bahl, 217) There is a concern as well that the self – regulatory measures in the online industry are not proving effective enough in reducing security risk. In a study by Business Week is was found that “…two-thirds of the financial services firms included in the study collected sensitive personal information on their Web sites, yet did not employ security features to safeguard that information…” (Milne, George R., Andrew J. Rohm, and Shalini Bahl, 217) This would seem to imply that more comprehensive and wide ranging efforts have not been taken to ensure the more integrated and standardized approach to security is implemented.

At the same time customer education is a central facet of the overall view of dealing with online security. As the study by Milne et al (2004) states, “… businesses must also work with the public sector to expand educational programs geared towards consumers. These programs could be used to encourage consumers to be more cognizant of the risks of online identity theft as well as to take more aggressive actions to defend themselves” (Milne, George R., Andrew J. Rohm, and Shalini Bahl 217) In this regard there are some positive and encouraging signs from the online business communities. For example, “Visa U.S.A. Inc. and MasterCard International Inc. will release new security rules in the next 30 to 60 days for all organizations that handle credit card data, a Visa official said last week.” (Vijayan J. 2006)

This is a central facet that will be explored in the final section of the present study. This refers to the increasing importance of shared knowledge and awareness between the user and the business about the nature and extent of ID theft. Therefore it is gradually becoming an endemic part of modern business practice to ensure that this knowledge is passed onto the consumer and that a mutual and symbiotic action strategy is implemented against the problem of ID theft.

Measures Taken by the United States

The impact of identity theft and related security issues have had repercussions throughout the society and the business community and have subsequently led to the involvement of the government and governmental agencies. Government agencies are continually monitoring fraud and fraud related aspects linked to computer crime and identity theft. For example, the FBI's cyber division has noted that there has been a radical increase in the number of reported fraud case in recent years. "…consumers have filed more than 207,000 complaints to the Internet Crime Complaint Center in 2004, a 66% jump from 2003, totaling $68 million in estimated losses." (207K complaints on cyber-fraud logged in 2004)

Beside the awareness of the crime on the part of agencies like the FBI, there is legislation that has been enacted specifically aimed at the prevention of identity theft and the apprehension of those who are guilty of this crime. This refers mainly to The Fair and Accurate Credit Transactions Act of 2003 or FACTA. A study on the effectiveness of FACTA in relation the prevention of identity theft states that "…FACTA represents an

important step toward reducing the incidence of identity theft as well as ameliorating the damage that it causes." (Linnhoff & Langenderfer, 2004, p.204) However the same study also notes that, "… unless and until Congress addresses the extensive use and distribution of Social Security numbers and the safeguarding of data, identity theft is likely to continue to wreak financial and social havoc." (Linnhoff & Langenderfer, 2004, p.204) The study goes on to repeat the plethora of statistics illustrating the growing incidence and the prevalence of this crime.

Other legislation that has been enacted to prevent identity theft includes The Identity Theft and Assumption Deterrence Act (1998) which made identity theft a federal crime, and the U.S. Patriot Act , passed after the event of September 11th terrorist attacks, which "… makes it more difficult for impersonators to open bank accounts." (Linnhoff & Langenderfer, 2004, p. 204) Furthermore, from January 2003, 24 bills were introduced that deal specifically with identity theft. This has led to the promulgation of FACTA in 2003 which is in effect a "…a statute that makes permanent many uniform national standards for credit reporting as well as addressing identity theft problems at the federal level." (Linnhoff & Langenderfer, 2004, p.204)

FACTA is a bill which deals with the problems of identity theft on many different levels. These measures include, among others, "…compulsory credit card number truncation on receipts, mandates to card issuers to investigate change of address and new card requests, fraud alert requirements by credit reporting agencies, mandatory blocking of identity theft-related information on credit reports, and free annual credit reports." (Linnhoff & Langenderfer, 2004, p.205) The bill also makes allowance for the divulgence of,

> … credit reporting agencies to divulge consumer credit scores, provides for the improvement of the resolution process once identity theft has occurred, and includes several measures limiting the sharing of medical information in the financial system. The statute substantially improves the balance of power between identity thieves and consumers and addresses many of the most pressing concerns."
>
> (Linnhoff & Langenderfer, 2004, p.205)

Among the many ways that FACTA acts against the consequences of identity fraud is by limiting the potential damage to credit histories as a result of ID fraud. This is achieved largely through a fraud alert. " A fraud alert can limit the potential damage from identity theft by making the acquisition of additional credit difficult following an identity theft discovery by the consumer, because such an alert is likely to motivate potential creditors to verify identification prior to extending credit." (Linnhoff & Langenderfer, 2004, p.205) Another way in which FACTA works against identity theft and fraud by enabling consumers "…to prevent information rooted in identity theft from being given to third parties." (Linnhoff & Langenderfer, 2004, p.205) The legalization therefore allows consumers to "…only to identify themselves and turn in a police report (called a "no-fault letter" … to halt access to fraudulent data." (Linnhoff & Langenderfer, 2004, p.205)

There are many other aspects that could be mentioned in relation to FACTA. In essence the Bill is aimed at both reducing the prevalence of identity theft as well as reducing the negative impact of ID theft. Critics state that the most effective area of FACTA is in the reduction of the fallout from identity theft. "More effective are FACTA's provisions to limit the damage post-theft. One-call fraud reporting will reduce the burden on victimized consumers as will the credit report blocking and re-pollution measures." (Linnhoff & Langenderfer, 2004, p.205) However, studies also note that the Bill falls short of dealing in an entirely effective way with the problem of Identity theft. Among the critiques of the Bill are the following: "First, the Act preempts state law and thus limits individual state efforts to impose stronger privacy policies than are set at the federal level." (Linnhoff & Langenderfer, 2004, p 205) Secondly,

> …the statute fails to address in any meaningful way the pervasive use of SSNs that not only threatens consumers with identity theft but also provides both legitimate businesses and criminals with the ability to quickly assemble a very complete dossier on virtually any American. This ability is troubling not only because it increases the incidence of identity theft but also because of the privacy implications.
>
> (Linnhoff & Langenderfer, 2004, p. 204)

In this regard it should be noted that there are also new legislative proposals that are in the offing and which are intended to limit the extent and the effects of identity fraud. One of these aspects is legislation designed to prevent the exploitation of Social

Security numbers by fraudsters. These laws are intended to curb the exploitation of Social Security numbers by,"… limiting their use to their original purpose--identification for tax and Social Security reasons only … "(Linnhoff & Langenderfer, 2004, p.204)

A third and important criticism of the Bill is that FACTA, to a great extent, places the onus and the responsibility for the detection of identity theft on the individual and is more concerned with the management the consequences of ID theft. "… FACTA predominantly puts the burden of fighting identity theft on a (hopefully) watchful public." (Linnhoff & Langenderfer, 2004. p.204) This is an aspect that will be expanded on in the following chapter which deals with the implications of shared responsibility in the fight against identity theft and fraud.

Steps to Best Enable Secure Transactions

As the above sections have pointed out, there are very sophisticated and multivalent methods of compromising and stealing sensitive information from users who wish to shop online. Some of the concerns that face the online shopper or computer user are similar to common experiences when ordering from a catalogue or by phone: for example, is the person of business taking my information, legal or phony? Another issue is whether someone can falsely use a customer's credit card for themselves. These fears are magnified by the anonymous nature of the Internet and the numerous threats that have been discussed in the previous sections.

The important point with regard to business is that online commerce needs the client to feel safe and to not have any fears about shopping online. The perception of the customer or client is essential in this regard as they are far less likely to purchase online if

they do not feel secure. As has been discussed, companies and institutions have implemented extensive technological methods such as authentication as well as SSL or Secure Sockets Layers to deal with identity theft. Despite these efforts and even the best efforts of governmental institutions, the problem of ID theft continues to grow. This has led to a number of central realizations in the business and online community.

One of the essential factors in reducing the degree of risk of ID theft lies in establishing a better reciprocity between customer and client as well as the need for a perceived sense of control and choice. Online privacy research has shown that one of the most effective ways of providing a sense of online security for shoppers is to provide a real sense of control and choice in terms of personal information. In this way the customer feels that he or she has more direct access to how personal information is stored and manipulated. This relates to many accusations that often "Organizations and government agencies sometimes unwittingly post consumers' personal information online…" (Han J.) Therefore, it is felt that providing more choice and control on the part of the customer will create an environment where there is a better understanding and interaction between the customer and business in the fight against ID theft. .

Coupled with the above concern is the fear that even after companies store and process data there is still the possibility of this information being compromised by external threats and hackers. Taking these concerns into account, privacy advocates have suggested methods and procedure that the customers can take to improve the projection of online data. These include the following common pointers.

1. Look for privacy policies on the Web.

2. Get a separate e-mail account for personal e-mail.

3. Teach your kids that giving out personal information online means giving it to strangers.

4. Clear your memory cache after browsing.

5. Make sure that online forms are secure.

6. Reject unnecessary cookies.

7. Use anonymous remailers.

8. Encrypt your e-mail.

9. Use anonymizers while browsing.

10. Opt-out of third party information sharing.

(Milne, Rohm, and Bahl)

The above points also resonate with regards to the mobile industry. In relation to the issue of the burgeoning of the mobile industry and the recent growth of shopping potential, studies have found than many wireless consumers lack basic security protection. This problem is acerbated by the fact that "…more homes are connecting to the Internet using wireless networks…" and, "… too few of these users are set up to protect against intrusion. More than one out of four homes had a wireless network (26%), and nearly half of these homes (47%) failed to encrypt their connection, a safety precaution needed to protect wireless networks from outside intruders." (Milne, Rohm, and Bahl)

While the above points are useful, experts warn that while users can protect themselves to a certain extent, security threats are becoming broader and more dangerous. The extent of the danger to online users and those making transactions on the Internet is emphasized by Tatiana Platt, Senior Vice President and Chief Trust Officer for AOL.

> When a single virus, a simple scam or hidden spyware program can shut down your computer or cause a person to lose their bank account, their family pictures, or all of their personal records, it is vital that consumers take every possible step to protect themselves. You can't lock just a few of the windows in your house and expect to stay safe from thieves."
>
> (Han J.)

Other research findings also lead to the view from many pundits that online users are not yet fully cognizant of the dangers that can occur in the online environment. These include the fact that it has been found that about three quarters of users in one survey use their computers for sensitive transactions. More than two - thirds of computer users retain sensitive information such as credit card numbers on their computers and more than half of users have been infected by viruses in the past. (Han J.)

There are numerous studies that suggest measures that can be taken against specific ID threats such as phishing. These studies also point out the crucial fact that phishing or pharming are complex forms of intrusion and require a multifaceted and multidimensional approach to reduce their threat to privacy.

> The fact that the phishing attack life cycle consists of many phases, each encompassing a diverse and changeable set of activities, makes phishing a kaleidoscopic problem for which no single solution can suffice. Multiple solutions are called for, and the earlier in the life cycle an attack can be countered, the better the outcome for targeted victims and financial institutions. (Wetzel, 2005, p.46)

Wetzel suggests numerous methods and strategies that can be used by both business and clients against phishing attacks. These include the following:

> …better mutual authentication; spam filtering; detecting infringed domain names; and alerting consumers when they are being directed to fake websites… Because impersonation is a prerequisite to successful phishing attacks, better mutual authentication between a financial institution and its customers is an essential weapon… better customer authentication can keep attackers from successfully impersonating customers in the fraud phase…. Email sender authentication schemes help identify attempts by fraudsters to impersonate clients….(Wetzel, 2005, p.46)

Furthermore there are also new software packages that are increasingly more adept at discovering phishing websites. " Technologies from Billeo, EarthLink, Geotrust, Netcraft, Phish-Free, Collective Trust, Webroot Software and WholeSecurity alert customers during the collection phase, when target victims are visiting a bogus website. "(Wetzel, 2005, p.46) However the experts are emphatic that ID theft and phishing are problems that are difficult to solve in the short term.

> Phishing is destined to become a never-ending cat-and-mouse game, in which today's solutions may not work as well tomorrow. Solution providers and financial institutions must pedal hard to keep up. Because so much is at stake, counter-phishing will continue to attract money and innovation, and vendors will increasingly be called upon to offer integrated solutions that address multiple facets of this complex problem…
>
> (Wetzel, 2005, p.46)

This leads to the central point and a focal issue that emerges for the research; namely that, <u>despite all these counter measures and various technical innovations that can be implemented there is a growing realization that ID theft can only be effectively dealt with synergistically and with the involvement of all the various parties concerned</u>. This important view is reiterated by Milne, Rohm & Bahl, (2004) who also states that this problem has global implications.

> …online identity theft is a global rather than domestic problem … The ease with which electronic data flows across borders makes consumers vulnerable to privacy invasions and identity theft, especially when the data is transferred to countries that don't have appropriate legislation to safeguard consumers against online privacy invasions and thefts…
>
> (Milne, Rohm & Bahl, 2004. p.217)

Milne also suggests that the most effective strategy against identity theft is one which "… depends upon the collective actions of government, businesses, and

consumers. “(Milne, 2003, p. 388) Milne notes that this means that government must implement appropriate legislation and take counter measures to influence and improve business policy with regard to ID theft. In conjunction with this interaction is the imperative to educate consumers and users to enable them to protect their on privacy. (Milne, 2003) For example, there is a need to make the consumer more aware of the importance of small but important details, such as the choice of passwords to protect their private information.

> More education is needed to encourage consumers to establish non-obvious passwords. Students, perhaps because of the greater computer experience, are more likely to follow the practice than are non-students, yet both groups need to be reminded of the importance of not using their mother's maiden name, pet, birth date, or last four numbers of their social security number…
> (Milne, 2003, p. 388)

The same study also found that in many cases consumer awareness of the dangers of ID theft was comparatively low and this factor is in need of adjustment in order for a more integrated and holistic approach problem is to be effective. (Milne, 2003)

There are a number of studies that also address this important question of a lack of knowledge as a central causative factor in ID theft. This is related to an increasing concern about the lack of security with regard to personal and sensitive data from public sources. As Milne, Rohm & Bahl, (2004) state, “It is not just the thieves that are contributing to the rise of online identity theft, however. Organizations and government agencies sometimes unwittingly post consumers' personal information online.” (Milne,

Rohm & Bahl, 2004. p.217) The authors go on to cite specific examples of these flaws in security. "Cohen (2001) mentions that state government agencies have posted public court records on the Web, which advocates consider a privacy risk." (Milne, Rohm & Bahl, 2004. p.217)

Another aspect that is often referred to in the search for solutions to the problem of ID theft is the important role that larger organizations can play. "…often overlooked is the important function of organizations in enabling and preventing identity theft." (Lacey and Cuganesan, 2004, p. 244). Organizations can for example, act as detectors of identity theft as well as a "…site where a fundamental social imperative exists to ensure responsible action is taken to address this form of criminality." (Lacey and Cuganesan, 2004, p. 244) This refers to the view that organizations are seen to have a responsibility towards the larger community and the individual with regard to helping to prevent crimes like identity theft. Therefore, as Lacey and Cuganesan in their study on this subject state; "…it is important to consider organizational initiatives in formulating holistic policy responses to identity theft. "(Lacey and Cuganesan, 2004, p. 244) This again points to the increasingly prevalent view that the realistic solution to Identity theft lies in a more holistic and integrative approach.

Chapter 5 – Project History

The project evolved from various main ideas to a well researched thesis paper. Once the decision for the topic was made for the Master Thesis paper: "Computer Security and Identity Theft" and it was approved by the Regis University advisor, the first step was to begin to do a thorough research of both primary and secondary sources. The primary references used in this master thesis include interviews with co-workers and colleagues in the IT Security field. This allowed for the gathering a more subjective or personal view of the extent of the problem. The secondary resources included periodicals such as journal article, books, and websites that shed like into the subject. These resources not only served as an aid in producing a detailed literature review, but allowed for the support the argument or problem in the document.

The work was developed by watching a business being restructured. Many ideas were also based on its employees having had identity theft. Some of the things observed at a major local university were lack of awareness, training and instruction. Many local businesses observed in the South Florida area lacked an IT Department. After conducting several months of research, the next step was the process of brainstorming ideas and getting ready to produce a rough draft of the paper. The time frame of the master thesis was approximately two months of proofreading and editing and finally generated the final draft.

Chapter 6 – Lessons Learned and Next Evolution of the Project

The above sections of this study and the various views gleaned for the research can be summarized in the following way. The solution to the increasing problems of ID theft is one which requires a holistic approach, where business, consumers, organizations and government all work together in order to counter the threat of ID theft. However, as has also been noted from numerous sources and in the literature review in this study, at present there is no integrated document to plan in place that outlines such a holistic and integrated view of the problem. The research therefore tends to suggest that concerted efforts should be made towards a more comprehensive understanding of the context and the extent of ID theft.

References

$2.8 bln in e-commerce revenues lost to fraud in 2005; available from http://blogs.zdnet.com/ITFacts/index.php?cat=33&paged=2; Internet; accessed17 November 2006.

2 billion mobile subscribers by end of 05; available fromhttp://www.smartmobs.com/archive/2005/08/25/2_billion_mobil.html; Internet; accessed17 November 2006.

74% IT managers receive phishing attacks; available from http://www.financialexpress.com/fe_full_story.php?content_id=98848; Internet; accessed 17 November 2006

207K complaints on cyberfraud logged in 2004; available from http://blogs.zdnet.com/ITFacts/?p=9372; Internet; accessed17 November 2006

Adkins S. 2005. *Internet Security Threats Will Affect U.S. Consumers' Holiday Shopping Online*; available from http://www.bbb.org/Alerts/article.asp?ID=637; Internet; accessed 17 November 2006

Anonymizer Now Protects Against Pharming Attacks; available from http://www.marketwire.com/mw/release_html_b1?release_id=85321; Internet; accessed13 November 2006

Bielski, L. 2005. Security Breaches Hitting Home: Phishing, Information Leaks Keep Security Concerns at Red Alert. *ABA Banking Journal, 97*(6), 7.

Bielski, Lauren. 2006."Debit's Growing Popularity." ABA Banking Journal 98.1: 37.

Blair, Kevin. 2001."Moving Fast: Competition Heats Up on Credit Card Security." *ABA Banking Journal* 93.4 (2001): 63.

Britons 'dependent on mobile use'; available fromhttp://news.bbc.co.uk/2/hi/business/5204454.stm; Internet; accessed 17 November 2006

Cookies; available from http://www.webopedia.com/TERM/c/cookie.html; Internet; accessed 13 November 2006.

Cox. J. 2006. *Mobile users face knotty security issues*; available from http://www.networkworld.com/news/2006/071706-mobile-users-security.html?fsrc=rss-security; Internet; accessed13 November 2006.

Espiner T. *Windows Wi-Fi attack discovered 2006*; available from http://news.zdnet.co.uk/0,39020330,39247302,00.htm; Internet; accessed18 November 2006

Internet Commerce Grows 88 Percent by Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a Concern; available from http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_028572.html; Internet; accessed 17 November 2006

Giesen, L. Hand-holding; available from http://72.14.221.104/search?q=cache:dwW8k_AH9soJ:https://images.scanalert.com/pdf/press/2006_03_01.pdf+Effect+of+Internet+Security+on+Online+Shopping&l=en&l=za&t=clnk&d=29; Internet; accessed13 November 2006.

Gips, Michael A. "Security Management Online." *Security Management* Dec. 2000: 16.

Global Mobile Population Growing. 2004. 20 July, 2006; available from http://www.clickz.com/showPage.html?page=3377511; Internet; accessed15 November 2006

Hackworth A. Spyware; available from http://64.233.161.104/search?q=cache:inC-sbguIvMJ:www.cert.org/archive/pdf/spyware2005.pdf+spyware+and+online+shopping&hl=en&gl=za&ct=clnk&cd=34&lr=lang_en&client=firefox-a; Internet; accessed15 November 2006.

Han J. *One in Four Computer Users Hit by Phishing Attempts Each Month, According to Major In-Home Computer Safety Study*; available from http://www.staysafeonline.info/news/press_dec07_2005.html; Internet; accessed15 November 2006.

Hines M. 2006. *Cell Phone Spy Program Raises Concerns*; available from http://www.eweek.com/article2/0,1895,1944472,00.asp; Internet; accessed15 November 2006.

Identity Theft; available from http://www.fraudwatchinternational.com/identity-theft; Internet; accessed15 November 2006.

Identity Theft: Investigation and Preventative tools. 2006 National Community Policing Conference. ; available from http://www.cops.usdoj.gov/mime/open.pdf?Item=1775; Internet; accessed15 November 2006

Identity Theft Survey Report. Prepared by Synovate (Aegis Group plc) ; available from http://www.ftc.gov/os/2003/09/synovatereport.pdf; Internet; accessed15 November 2006

Jones, Radford. 2001. "Anticipating the Worst of Times." *Security Management* Apr. 2001: 42.

Klein, Dan, Beverly Canfield-Woods, and Peter Piazza. 2001. "What If the Virtual Walls Fall?." *Security Management* Aug. 2001: 76.

Lacey, D., & Cuganesan, S. 2004. The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic. *Journal of Consumer Affairs, 38*(2), 244+.

Lim, Kai H., Kwok Leung, Choon Ling Sia, and Matthew K.O. Lee. 2004. "Is eCommerce Boundary-Less? Effects of Individualism-Collectivism and Uncertainty Avoidance on Internet Shopping." *Journal of International Business Studies* 35.6 (2004): 545+.

Linnhoff, S., & Langenderfer, J. 2004. Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken. *Journal of Consumer Affairs, 38*(2), 204.

Malicious Software Expected to Increase; available from http://www.wirelessweek.com/article/CA6299498.html?spacedesc=Departments: Internet; accessed15 November 2006.

McMillan R. *DOJ: Identity theft hit 3.6M U.S. families in six months of '04* ; available from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110139; Internet; accessed15 November 2006.

Milne, G. R. 2003. How Well Do Consumers Protect Themselves from Identity Theft?. *Journal of Consumer Affairs, 37*(2), 388.

Milne, G. R., Rohm, A. J., & Bahl, S. 2004. Consumers' Protection of Online Privacy and Identity. Journal of Consumer Affairs, 38(2), 217.

Miyazaki, Anthony D., and Ana Fernandez. 2001. "Consumer Perceptions of Privacy and Security Risks for Online Shopping." *Journal of Consumer Affairs* 35.1 (2001): 27.

Miyazaki, Anthony D., and Krishnamurthy S. “Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions." *Journal of Consumer Affairs* 36.1 (2002)

New crop of thieves: Pharmers hit Net banking; available from http://www.azcentral.com/specials/special37/articles/0419pharming19.html; Internet; accessed15 November 2006

New holiday online shopping trends emerge. July 20, 2006; available from http://www.itworld.com/Tech/2403/041223shoppingtrends/pfindex.html; Internet; accessed15 November 2006

Number Of Mobile Subscribers Worldwide To Rise To 3.96 Billion By 2011; available from http://www.wi-fitechnology.com/displayarticle2542.html; Internet; accessed15 November 2006

Online Privacy and Security: The Fear Factor; available from http://www.emarketer.com/Reports/All/Privacy_retail_apr06.aspx; Internet; accessed17 November 2006.

Online retailers enjoy 20 percent sales boost by certifying their security against hackers according to new research: available from http://64.233.183.104/search?q=cache:g7_LUIXuRbYJ:https://images.scanalert.com/pdf/press/ScanAlertBehavioralAnalysisReleaseMediaKit.pdf+%22Results+of+new+consumer+behavior+research+released+today%22&hl=en&gl=za&ct=clnk&cd=1&lr=lang_en&; Internet; accessed15 November 2006.

Online Shopping; available from http://browser.netscape.com/ns8/security/basics_shopping.jsp; Internet; accessed15 November 2006.

OFT launches fact-finding market study of internet shopping; available from http://www.oft.gov.uk/News/Press+releases/2006/81-06.htm; Internet; accessed17 November 2006

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT Before the SUBCOMMITTEE ON TECHNOLOGY, TERRORISM AND GOVERNMENT INFORMATION of the COMMITTEE ON THE JUDICIARY. UNITED STATES SENATE Washington, D.C. 2000. available from http://www.ftc.gov/os/2000/07/idtheft.htm; Internet; accessed14 November 2006

Prevent Identity Theft and Safeguard Information Assets; available from http://www.finjan.com/Content.aspx?id=180; Internet; accessed13 November 2006

Pharming protection for internet users; available from http://www.out-law.com/page-5601; Internet; accessed13 November 2006

Phishing Attacks Surge in Last Six Months; available from http://www.clickz.com/showPage.html?page=3458321; Internet; accessed13 November 2006

Spyware; available from http://en.wikipedia.org/wiki/Spyware; Internet; accessed13 November 2006.

Triple Trojan Threat Calls on Symbian Cell Phones; 2006; available from http://www.eweek.com/article2/0,1895,1913830,00.asp; ; Internet; accessed13 November 2006.

Thompson, S. C. 2006. Phight Phraud: Steps to Protect against Phishing. *Journal of Accountancy*, 201(2), 43.

Vijayan J. 2005. Security Worries Cloud E-Commerce; available from http://www.pcworld.com/news/article/0,aid,123849,00.asp; Internet; accessed18 November 2006

Vijayan J. 2006. *Visa, MasterCard Unveil New Security Rules*; available from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=112332; Internet; accessed18 November 2006.

Wetzel, R. 2005. Tackling Phishing: It's a Never-Ending Struggle, but the Anti-Fraud Arsenal Continues to Grow. *Business Communications Review*, 35, 46+.

What is Phishing?; available from http://www.fraudwatchinternational.com/phishing-fraud/phishing-home/; Internet; accessed13 November 2006

World Market Data, Quotes And Domino Buzzwords; available from http://www.turtleweb.com/turtleweb.nsf/list4lookup/marketinfo?opendocument; Internet; accessed18 November 2006.

Young, S. 2005. Stolen Lives: Identity Theft Is the Country's Fastest Growing Crime. Here's How to Protect Your Most Valuable Asset-You! *Black Enterprise*, *36*, 86.