Journal of E-Business

Combined Issue: Volume V, No. 2 – Volume VI, No.1 **ISSN: 1542-0846** **www.journalofe-business.org**

TABLE OF CONTENTS

The Journal of E-Business is a refereed journal. It is published *online* by the International Academy of E-Business (www.iaeb.org) periodically, typically twice a year. Its contact e-mail: adm@iaeb.net. All rights reserved.

EDITORIAL BOARD

EDITORIAL NOTE

Welcome to ***the Journal of E-Business (www.journalofe-business.org)***, the online publication of the International Academy of E-Business. As one of the pioneers in the field of e-business, both the Academy and its refereed publications have been making significant contributions toward the theory and practice of strategic management in profit and not-for-profit organizations. (Additional details at www.iaeb.org)

This peer-reviewed Journal is published periodically, typically twice a year, to encourage and disseminate research studies in all aspects of e-business strategies and practices, including e-commerce, supply chain management, data storage and mining, management of information systems, global marketing and communications, human resource management, financial analysis and planning, entrepreneurship, research and development, and technology management.

Outstanding articles from the academic researchers, teachers, policy makers, business practitioners, and others, are accepted for publications on the basis of the recommendations of reviewers, who are members of the Editorial Board. Both exploratory and conclusive research studies are welcomed and, subsequently, peer-reviewed and considered for publication. Articles do not have to be empirical in nature. Case studies dealing with specific business situations are acceptable.

As with most leading journals, academic activities and publications depend on volunteers for their scholarly involvement and contributions.

The Academy is extremely grateful to so many individuals, who are experts in their respective fields and are serving on our Editorial Board. As reviewers, editor, or in other capacities, these individuals willingly participate actively in spite of their constant time and resource constraints. Sometimes the declining support on college and university campuses reaches a point where it is almost impossible for some individuals to remain active and participate in worthy activities.

Because of certain unavoidable circumstances, Professor Raj Garg, who had been serving as editor of *the Journal of E-Business* since its inception in 2001, has found it difficult to continue his editorship effective immediately. We are all grateful to Professor Garg for his years of service, and, of course, we will all miss his experience and leadership.

The Academy will seek and appoint the Journal's new editor as soon as possible. In the meantime, we have decided to put together this issue so that the new editor could start with a clean slate.

In this current combined issue of the Journal, we have included certain refereed articles which were submitted for publication in the Journal's special issue on "Cyber Security." Professor Mohan Menon of the University of South Alabama assisted the Academy as "Guest-Editor" in the review and selection process.

We are also publishing in this combined issue the top five outstanding papers of the Academy's 6th Annual Conference in Orlando in March 2006. Papers were chosen on the basis of reviewers' recommendations. We hope that the individuals who were not able to attend the conference find these papers useful too.

We feel our authors and readers deserve the publication of these exceptional studies without any further delay while the Journal is going through the editorship transition. Those who wish to submit their articles for publication should follow the guidelines, which are updated periodically on our Website www.iaeb.org.

Please note that as a scholarly Journal, the publication contains a wide variety of contributing individual's views, opinions, thoughts, and so forth. The contributing authors or their contents do not speak for, or represent, the official position of the Academy. All inquiries and comments related to the articles should be directed to their respective authors.

Editor-in-Chief

Publication Policies and Submission Guidelines

A brief summary of the International Academy of E-Business publication policies and manuscript/article submission guidelines is outlined below. Authors and co-authors, who intend to submit their individual manuscript for publication consideration, should fully read and understand them.

- The International Academy of E-Business (the Academy) reserves the right to change its policies and guidelines at any time without prior notice.
- The International Academy of E-Business reserves the right to publish or not to publish any manuscript for any reason at any time – even after the manuscript had already been accepted for publication.
- Submission of manuscripts for possible publication implies that the authors have read these policies and guidelines.
- Submission of manuscripts does not necessarily constitute its acceptance for publication by the Academy. Neither does it mean that the manuscript has been received by the Academy.
- All manuscripts submitted for publication go through a review process, which typically takes several weeks during the regular academic year -- longer during summer months and holidays.
- COPYRIGHT: Submitted manuscripts should be original, and they must not violate or infringe upon any intellectual property rights of any individual or organization. If a manuscript is accepted for publication or published, the copyright ownership is presumed to have been transferred by the author(s) to the International Academy of E-Business, irrespective of whether the transfer was carried out formally or not.
- The International Academy of E-Business retains all copyrights over all of its published content and materials, unless some other arrangements have been specifically agreed upon in writing by the Academy's Administrator or its Executive Director. Typically, the author(s) of the accepted manuscript for publication would receive additional copyright information and a copyright transfer form for each author's signature. Failure of the author(s) to return the copyright form in a timely fashion will result in publication delays.
- The International Academy of E-Business respects the intellectual property rights and ownerships of individuals and/or organizations, in addition to all other rights. Furthermore, the Academy does not encourage, nor approve, anyone to infringe on the rights of others. If there are right violations from manuscript publication, each author of the violating manuscript bears the total liability—solely and/or collectively. Each author of the accepted manuscript for publication agrees to hold the International Academy of E-Business harmless, in case of right violations, and each author furthermore guarantees to protect and defend the innocence and the lack of any responsibility of the Academy, its officers and/or its representatives.
- Inadvertently errors, omissions, and/or other mistakes may occur when manuscripts are published. Even though the International Academy of E-Business regrets such occurrences, it assumes no legal or financial responsibilities. All manuscripts are accepted and published, subject to errors. To minimize such errors, manuscripts should be prepared for consistency, style, and easy uploading.

- ***SUBMISSION***:

1. *Before you submit your manuscript, please visit www.iaeb.org to check whether or not any of the guidelines is changed.* ***Please use the updated address for submissions to expedite the review process.***

2. Submit 3 hard copies of your manuscript, in addition to its electronic version on a diskette or CD, to the International Academy of E-Business Administrative Offices, Box 631064, Nac, TX 75963-1064 USA. *(No electronic submissions without hard copies are accepted unless it is arranged specifically in advance.)*

3. Also, submit one electronic copy of your manuscript as an attachment to submissions@journalofe-business.org with subject line: "JEB Submission." (*Your electronic version should be in MS Word in XP or 2000 plus version.)*

4. Please keep your manuscript in reasonable length, preferably no more than 15 pages (single spaced with one inch margin on all sides), including charts, graphs, exhibits, references, appendix, and so forth.

5. Please use **"Times New Roman" and 10 point font. (Exception: Title: 14 point, bold, capital letters, centered; headings: 12 point, bold, centered; subheadings: at left margin, 10 point, underlined)**

6. Cover Page: ***Important*** Staple a cover page to the manuscript indicating only the article title (used for anonymous refereeing).

7. Second "Title Page", which should not be stapled to the manuscript, and it should include full authorship information--name, address, telephone, affiliation, e-mail, rank, etc.

8. ABSTRACT page should follow the second "Title Page" and should have 100-150 words abstract.

9. The manuscript should be free of all spelling, grammar and punctuation errors.

10. Inconsistencies: Please be sure that you are consistent in the use of abbreviations, terminology, and reference citations throughout your paper. When you use an abbreviation for the first time, please write it in full within brackets. For example, BEM (Big Emerging Markets).
11. TABLES, FIGURES AND DRAWINGS: All tables, figures, illustrations, etc. should be embedded at the appropriate place within the text of the article. In the paper version, they could be appended to the article at the end.
12. REFERENCES: References, citations, and overall manuscript style should be similar to those used by the American Psychological Association or the Journal of Marketing. References should be placed in alphabetical order at the end of the article. Examples:

    Garg, Rajendar K. (1996), “The Influence of positive and negative wording and issue involvement on reponses to likert scales in Marketing Research”, Journal of the Market Research Society, Vol. 38, No. 3, 235-246.

    Kaynak, Erdner and Vinay Kothari (1984), “Export Behavior of small and medium sized manufacturers: Some policy guidelines for international marketers”, Management International Review, Vol. 24, No. 2, 61-69.

13. Please check for grammatical and spelling errors before submitting. Manuscripts with many errors or “sloppy” work and style are likely to be rejected.
14. REVISIONS & ALTERATIONS: Often, a manuscript may be accepted by the Editor contingent upon satisfactory inclusion of changes mandated by anonymous referees and members of the Editorial Review Board. If you are asked to revise your manuscript, please make the necessary changes and resubmit the revised version following the Editor’s specific instructions.
15. Please allow 3 to 4 months for the review process. During this time you may try to avoid unnecessary inquiries about the status of your submission. The Editor will contact you immediately after the review process is completed. Please bear in mind the time and resource constraints, and don’t be alarmed in case of delayed responses.
16. Please write to adm@iaeb.net for additional information or any serious concern.
17. Please note that submission of a manuscript for journal publication represents a certification by the author(s) that the work contained in the manuscript is original, and that neither the manuscript nor any version of it has been previously published or under consideration by any other publication simultaneously. *(Under certain circumstances exceptions may be permitted if there is a mutual understanding in advance, in-writing.)*

.

SECURING CYBER BANKING TRANSACTIONS: TWO-FACTOR AUTHENTICATION AND OTHER IDEAS

Mohan K. Menon, University of South Alabama, USA

ABSTRACT

If information is money, then the Internet is the perfect tool to collect and turn it into cash. The use of the Internet both by consumers and financial institutions for mutual benefit has resulted in an unwelcome consequence – fraud. All instances of fraud, leave the consumer feeling more vulnerable and therefore reticent on the use of one of the greatest technological revolutions of our time. Fortunately, consumers, industry, and the government are taking steps to prevent fraud. Unfortunately, fraudsters are one step ahead of the rest and so the game goes on. This paper explores the extent of the problem, a proposed framework for authentication, industry responses, and recommendations by the Federal Financial Institutions Examination Council.

INTRODUCTION

With extensive use of the Internet in almost all walks of life it was only a matter of time before its misuse got more ink. Today, it seems one cannot escape news about ID theft, bank fraud, phishing, Trojans, etc. on a regular basis. With the increasing complexity of today's scams and problems, it makes one long for the good old days of simple viruses and Nigerian emails!

At the same time, it must be emphasized that even though digital scams get more publicity, old tricks still rule. According to a 2004 survey of ID theft victims who knew how their confidential data was stolen, 68 % reported offline methods were used while only about 12 % reported that online methods were used (Javelin Strategy & Research, 2004). Offline methods included lost or stolen wallet/checkbook/credit card, friends/relatives, and offline transactions, corrupt employees, stolen paper mail, garbage theft, etc. Online modus operandi included spyware, online transactions, computer virus/hacking, and phishing scams.

In order to get a perspective on the situation and the problems, the paper will focus on one significant facet of cyber security namely those related to Internet banking. As banks provide more interactions via the World Wide web in order to control costs, it is imperative to review the security policies and suggestions to enhance them. The discussion is also topical since bank regulators in the United States and elsewhere are currently calling for stronger access protocols to safeguard customers' accounts and information. For instance, the Federal Financial Institutions Examination Council (FFIEC) has recently issued some guidelines. For banks, FFIEC suggests enhanced authentication methods to use when authenticating the identity of customers using the on-line products and services. Financial institutions in the U.S are expected to achieve compliance with the guidance by the end of 2006.

According to a federal report, there has been significant increase in the "incidents of fraud, including identity theft." (FFIEC 2005) Of the $1.3 trillion in transactions done with Visa credit cards in 2004, only 0.05% were fraudulent, the same level as 2003, and down from 0.07% in 2002. (USA Today 2005) The significance of this encouraging report is lost when one hears about data theft at ChoicePoint, DSW Shoe Warehouse, CardSystems of Atlanta, and other businesses in 2005. In the case of CardSystems, about 40 million Visa, MasterCard, Discover, and Amex card numbers along with the CW2 codes were exposed. Sometimes, companies are partly to blame for such debacles. DSW Shoe Warehouse had unencrypted data on computers that were hacked into. ChoicePoint accidentally sold consumer data to crooks posing as legitimate businesses. CitiFinancial sent a box of consumer information via UPS that went missing in transit. Bank of America lost back up tapes of information about federal government workers.

Advocacy groups point to the need for a national privacy law to prevent similar incidents. “For most U.S. companies, the only notification of ID theft that's required by law is the one mandated by a California ID theft statute, which obligates companies doing business in the state to notify customers if their personal information has been accessed by an unauthorized person. The California law went into effect in July 2003.” (Gross 2005)

Reviewing multiple published survey results, paints an ominous profile of some of these cyber security problems. About 73 million adults say they have received 50 phishing emails in the previous twelve-month period and 13 percent of all Internet users have had a member of their household victimized by identity thieves and 41% stated that they were buying less online due on account of threats to the financial security. Eighty percent of consumers’ computers were infected with spyware. About 63% of the large companies say their main security concern is increasing complexity of cyber attacks while 91% of companies and government agencies surveyed stated that they lost $31 million worth of proprietary data and spent $43 million to clean up viruses. (USA Today 2005).

MODES OPERANDI

As mentioned earlier old-fashioned methods, such as dumpster diving, are still prevalent today. For instance, employees might sell data for profit. Eight employees of PNC, Bank of America, and a couple of other banks were caught selling customer information to an agency operated by criminals.

At the lower end of technological sophistication are criminals lifting information from company databases and selling to criminals or syndicates for handsome returns. (Verton 2005). Sometimes, hacking into unprotected computer systems maintained by companies can provide a wealth of consumer information. Such was the case with DSW Shoe Warehouse and CardSystems.

Sophisticated crooks have shifted to more dangerous attacks on a smaller number of computers that over time infects millions of other machines while not raising any suspicions. There are new ways of attaching Trojans to free and downloadable files - Trojans can be buried on popular websites or in email attachments. Downloading an infected files or visiting an infected Web site can unleash the Trojan on unsuspecting computer users.

At the same time, some phishers moved up the pecking order by deploying “SQL Injections” aimed at duping pages linked to company database into providing data on customers and employees. The Anti-Phishing Working Group reported about 13,776 unique types of phishing attacks in August 2005. Another recent report by the same group indicates that phishing scams are now targeted at smaller banks and credit unions. “A surge in phishing e-mail scams targeting regional credit unions and local banks is the latest sign fraudsters are shifting to narrow tactics.” (USA Today 2006). This is probably because smaller banks or credit unions are less likely to have robust defenses and secondly, such small-scale scams might elude the attention of law enforcement.

Stolen IDs are also fair game for the crooks looking to make a quick buck. The market for stolen IDs is becoming more specialized. An FTC survey of consumers found about 10 million Americans were victims of ID thefts in 2003. In monetary terms, it costs consumers about $5 billion and companies about $ 48 billion.

A FRAMEWORK FOR AUTHENTICATION

Given the prevalence of fraud and ID theft, the Internet banking environment must offer effective and functionally dependable forms access and authentication. Such a system is critical for protecting "customer information, for preventing money laundering and terrorist financing, for reducing fraud, for hampering ID theft, and for promoting the legal enforceability of electronic agreements and transactions in the banking system." (FFIEC 2005) Not implementing and enforcing stronger authentication is not in the long-term interests of the banking system. Besides, some of the provisions of the USA Patriot Act demand that banks tighten their customer verification / authentication requirements.

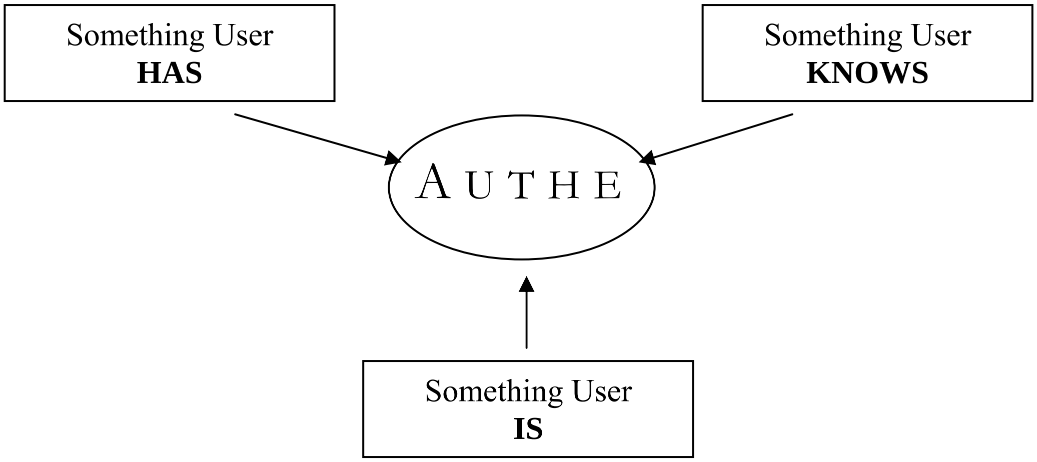


Figure 1: Authentication Factors

As indicated by Figure 1, authentication procedures are based on three factors:

(1) something the user has in his/her possession that is tangible in nature such as a smart card or ATM card or other verifiable physical item or tokens that is required to be utilized in the access procedure;
(2) something the user knows such as a PIN code, password, login ID, etc. that he/she can recall during the transaction; and
(3) something the user is. This includes physical attributes of the user such as fingerprints, iris composition, voice patterns, hand geometry, etc. Also called biometric factors, these are likely to play an increasing role in authentication procedures in the future.

Usage of any one of the above factors (i.e., single factor authentication) is likely to be vulnerable to compromise compared to two or even three-factor authentication using in a combination of the factors. Whether or not to implement appropriate authentication procedure is influenced not just by the available technology but also by business policy.

Implementation of the appropriate authentication protocols is dependent upon certain conditions. For instance, customer convenience might be an overriding factor in the selection of the authentication protocol. Multifactor authentication protocol is considered secure but might be inconvenient for customers. Another critical variable is the assessment of potential risk. Not all situations warrant multi-factor authentication. According to the FFIEC report, risk assessment should take into consideration the type of customer (retail vs. institutional), the type of transaction (bill payment, wire transfer, loan origination, etc.), the sensitivity of the information transmitted, ease of use, and the volume of transactions. (FFIEC 2005) In other words, the level of authentication should match the level of perceived risk.

Most experts consider any form of single-factor authentication procedure to be inadequate for higher risk transactions. They recommend that Internet banks and financial institutions consider both the current state and future sophistication of ID fraud and implement a robust multifactor procedure. An impetus for implementing better authentication systems is the USA Patriot Act.

A robust authentication system must include other elements such as the ability to monitoring and report, and the ability to audit and implement control. An effective system should provide for constant monitoring of activities with a view to detecting fraud and improving the overall performance of the procedures. Customers should also be educated on the need for and usage of the system. In essence, the system should be comprehensive in dealing with the situation. Figure 2 represents some of the essential features or criteria for such a system.

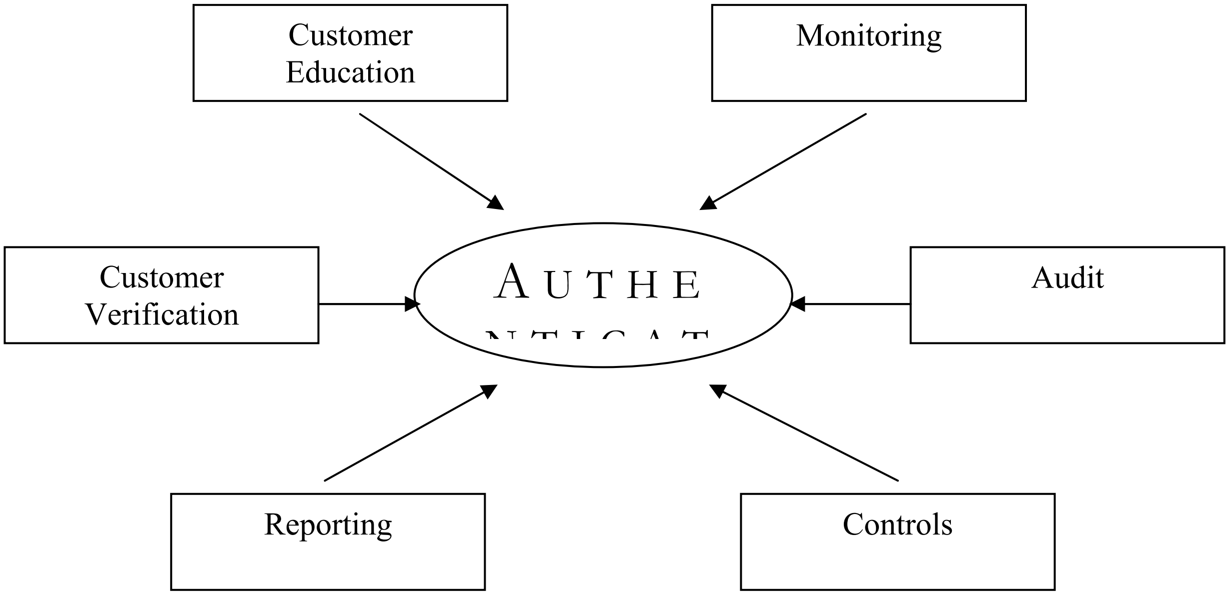


Figure 2: Essential Criteria for an Authentication System

AUTHENTICATION TECHNIQUES IN USE

Some of the authentication techniques that are being used or proposed are discussed in this section. As mentioned earlier, it is imperative that the financial institutions consider the level of risk with the strength of the authentication techniques or procedures.

What a User HAS:

Also called tokens, these physical devices are vital to a multifactor authentication system. They can be USB Token devices, smart cards, password generating fobs, etc. USB token devices (first authentication factor) plugs into the user's computer. Once installed, the user gets a prompt to enter his/her password (second authentication factor) to access.   These devices, similar to USB storage drives, are easier to carry and do not need special software to install on PCs.

Smarts cards, on the other hand, are credit/debit card sized cards (first authentication factor) that have a microchip for storing data. When the card is inserted into a card reader connected to the computer, the stored data can be utilized by the authentication system to prompt the user to enter a passcode (second authentication system) to complete the access process. Smart cards, unlike credit cards, are harder to copy but easier for the user to carry. The microchip can be used to store various types of data, including financial and medical. A minor inconvenience is the additional hardware (the card reader) that needs to be installed on the computer.

Passcode generating tokens or fobs are similar in size to USB devices but has the ability to generate disposable or one-time passwords valid for a few seconds, typically 30 or 60. These fobs have small LCD screens that display the passcodes. When trying to access a secure account, the user enters his/her user and first password (first authentication factor) and then the fob generated password (second authentication factor). If the two authentication factors are matched by the server, access is granted. These devices can generate passwords for up to 5 years before they need to be replaced. Given the disposable nature of the password and its randomness, this method is considered secure.

Similar to electronic passcode fobs, physical scratch cards similar to bingo/lottery card can also be used. These cards have alphanumeric characters arranged in a grid with a number of cells. Once the user has input the first authentication factor (user ID and password), he/she is required to input characters contained in a randomly selected cell in the grid.

Unfortunately, all these types of authentication factors suffer one major drawback – the user losing or misplacing the device much like losing one's keys. Secondly, electronic items might not work due to wear and tear over a course of time.

What a User KNOWS:

These are techniques have been in vogue for over a decade and works well in many non-critical situations. They are considered the first line of defense. Information such as user ID and password are shared between the user and the authenticating server. In many instances, the user has the ability to change passwords. Some companies have added a secondary layer of protection by requiring a password question in case the user forgets the original password. Users select the question-answer set when he/she signed up for the service.   By allowing the user to choose an ID, password, and a password question-answer, there is the likelihood that he/she will select access information that is easily remembered. Since most users never change their access information, there is greater likelihood of compromise over time.

There are some "out-of-band" techniques that have been used in the past. In this case, a transaction request online by the user is verified via telephone calls by the bank using user provided telephone number. The user is then asked for some predetermined information as a way of verifying the legitimacy of the request. Financial institutions have used this technique when money transfer or stock purchase/sale is being requested. Currently, these out-of-band procedures can be handled by servers placing telephone calls or generating emails or instant messaging.

What a User IS:
When authentication procedures involve recognition of some physical characteristics of the user, the ability to duplicate is virtually zero. As a factor in a multifactor authentication procedure, biometrics is effective. Common biometric techniques include, fingerprint, face, iris, voice, retinal recognition. Keystroke and handwriting recognition along with hand geometry are also considered biometric authentication techniques. Most people have been introduced to these techniques through Star Wars, Star Trek, or James Bond movies.

In a typical biometric procedure, identifying physical characteristics are sampled and data obtained. This data is converted into a mathematical model that is included in a "database on which a software application can perform analysis." (FFIEC 2005) A user subjected to a scan will have data gathered by the device and matched with the information in the database. A match authenticates the user and access is granted. London's Heathrow airport uses an iris scanner authentication procedure for frequent flyers to New York helping them save valuable time.

A non-biometric technique that has been used in certain transactions is the IP address locator or Geo-locator. In both instances, a user's default computer's IP number and/or location is logged by the authentication server and used to verify the legitimacy of the request generation. Unfortunately, these are not fool-proof methods since IP information is sometimes hard to obtain in an environment that assigns random IP numbers to computers. Hackers can also spoof IP numbers in some instances.

A system of mutual authentication may be relevant in some instances. (FFIEC 2005) Similar to the bank's server authenticating the customer's identity, the customer or his/her computer should be able to authenticate the bank's Website. Phishing scams are often successful because they exploit this loophole in the system. Visually a customer cannot tell the difference between the legitimate site and a spoofed site but his/her computer might be able to. Mutual authentication is relatively easier to achieve through the use of digital certificates, encrypted transmissions, sharing of secrets such as digital images and so on.

INDUSTRY CONFRONTING THE PROBLEM

A small Philadelphia-based institution, Stonebridge Bank, utilized a two-step access to customers' bank accounts via the Internet. Besides the using a username and password, customers have to enter a unique and disposable pass-code generated by a key fob. The technology seems promising but the larger question is will other banks, especially big ones, use it? To some extent, greater security could compromise the ease and convenience of Internet banking. Other institutions such as American bank also from Philadelphia, and E-Trade Financial Services makes available these methods of access to customers on an optional basis. E-Bay in partnership with VeriSign may offer a system of security in the near future. (USA Today, 2005)

According to a study by USA Today, many of the bigger banks have not indicated their response to the federal mandates (2005). A survey by BITS, the education and training arm of the Financial Services Roundtable representing many of the large American banks and financial institutions, found that the main obstacles to deploying any additional security or access requirements are customer resistance, cost, and lack of technical readiness. (USA Today 2005). Banking analysts envision banks trying to meet the federal requirements by requiring customers to use mouse clicks to enter passwords and similar cost effective methods. ING Direct, an online only bank, implemented this system in 2005.

The largest bank in the country, Bank of America, implemented SiteKey system of access in many of its markets. According to the bank's Website, SiteKey is "Bank of America's new anti-spoofing and anti-phishing program, to avoid being a victim of website or email fraud." (Bank of America 2006). In effect, the program "asks customers to acknowledge a (customer) pre-selected image and phrase to verify they have reached the authentic B of A Website." (USA Today 2005). There are additional requirements if customers try logging in from computers other than their default machine.

Security provider companies such as RSA Security and others are pitching their proprietary systems to various banks. Some of these systems include USB tokens, access code scrambler technologies, and programs to allow mobile devices to generate pass-codes.

At the wholesale level, Visa and MasterCard are requiring merchants to use their new system of security standards called PCI. There are other efforts by the financial services industry including sponsoring a free ID Theft Assistance Center to help victims.

Federal response has been issuing he FFIEC guidelines that are to take effect by the end of this year. Five federal banking agencies have developed a "two-factor authentication" strategy they feel will minimize the instances of security breaches. The Federal Financial Institutions Examination Council report, referenced in this paper, provides guidelines that apply to both consumer and commercial transactions. (FFIEC 2005) The fundamental premise of the report is that the authentication technologies utilized by the financial entities should commensurate with the risks associated with specific products and services offered. In other words, a basic login ID – password combination for access might be sufficient for non-monetary transactions while stronger authentication is necessary for bank/credit card account access.

Various legislations aimed at addressing these problems are also working their way through Congress. For instance, Senator Feinstein sponsored a bill that would set a national standard for mandatory disclosure when consumer records are compromised. Another bill would slap fines on companies that lose records. (Steven and Stone 2005) The state of California has, to date, the toughest law. It requires businesses to notify consumers if hackers gain entry to computers that contain unencrypted personal information such as credit card numbers, pass codes needed for use of personal accounts, Social Security numbers or driver's license numbers, etc. (OAG 2004) Consumers must be notified immediately after a privacy breach occurs. Customers affected by a violation of the law can file civil suit to recover damages.

CONCLUSION

As long as information can be turned into cash or other valuables, there is likely to be ID theft and fraud. Even though locks at home and in cars have become more sophisticated burglaries continue to grow. Similarly, even with the implementation of newer and more robust authentication systems, data theft is likely to grow. As history reveals, any new authentication or security system is vulnerable to newer types of account hijacking schemes and Trojans. For instance, a newly discovered "man-in-the-middle" Trojan allows criminals to get between the customer and the bank without either one detecting their presence. The offender can then modify the messages transmitted. Hijack Trojans can let criminals access accounts while the legitimate customers are logged in and transfer monies. At times, it might seem like a losing fight but to continue the fight without losing hope is paramount to making the promise of the Internet a reality.

REFERENCES

Federal Financial Institutions Examination Council (2005). "Authentication in an Internet Banking Environment." http://www.ffiec.gov/pdf/pr080801.pdf

Gross, Grant (2005). "ChoicePoint's Error Sparks Talk of ID Theft Law." PC World, February 23, 2005. http://www.pcworld.com/news/article/0,aid,119790,00.asp.

Levy, Steven and Brad Stone. (2005). "Grand Theft Identity." Newsweek, July 4, 2005. 38 – 47.

Office of the Attorney General. (2004). "Identity Theft." http://ag.ca.gov/idtheft/index.htm

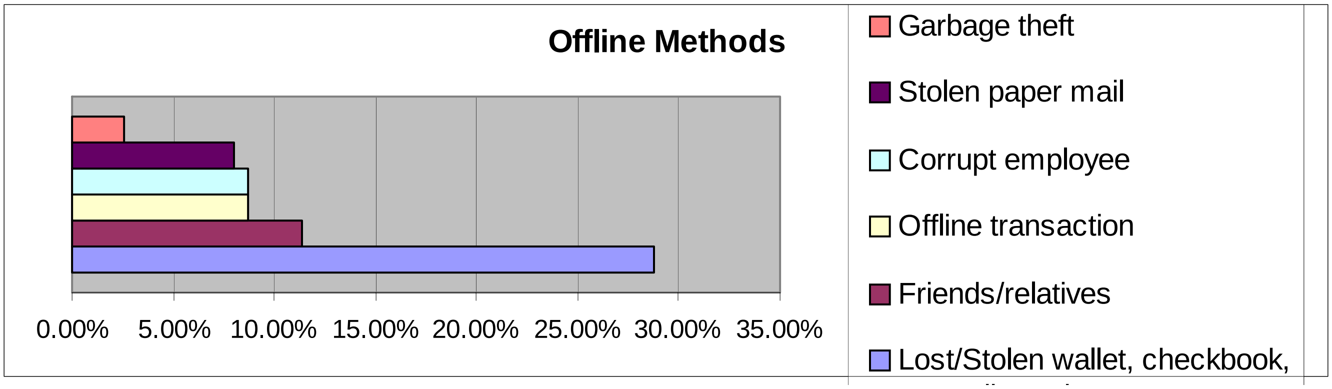
Verton, Dan. (2005). The Insider: A True Story. (Tamarac, Florida: Llumina Press).

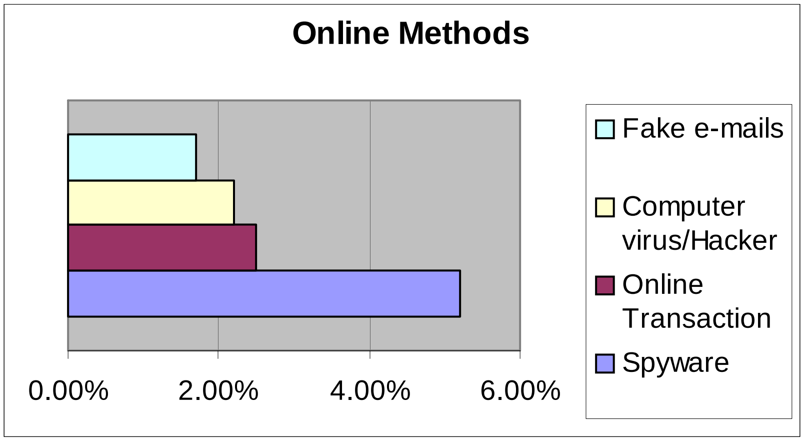
USA Today (2005). "Cyber Safecrackers Break into Online Accounts with Ease." November 3, 2005, 1A – 2A.

USA Today. "This Little Fob could Foil A Cyber Bank Robber." November 3, 2005, 1B – 2B.

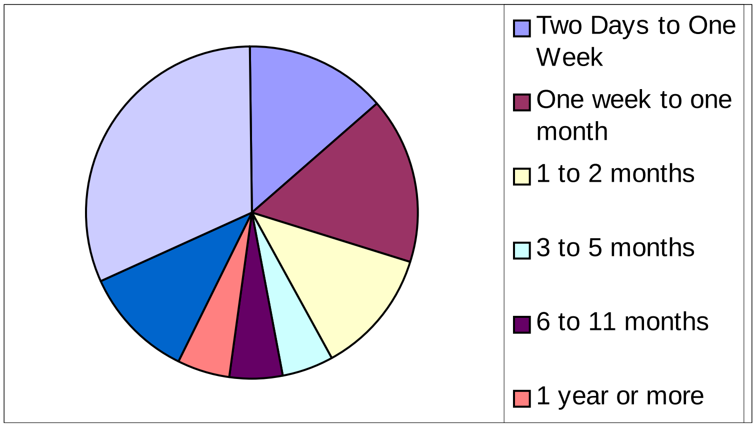
USA Today (2006). "Phishing Scams Aim to Bilk Smaller Prey." March 13, 2006. 1B.

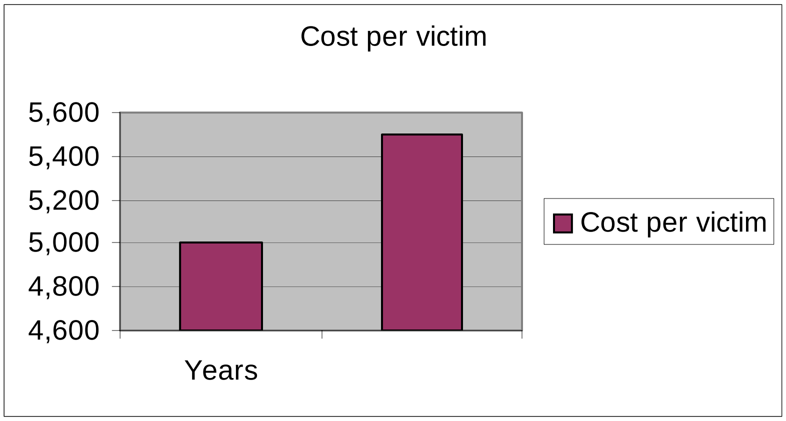
Bank of America http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_tips





Recovery Time




Cost per victim
5,600
5,400
5,200
5,000
4,800
4,600
Years
Cost per victim

USER RATING SYSTEM FOR THE INTERNET (URSI) AND CENTRAL AUTHORITY FOR INTERNET SECURITY (CAIS)

Gonca Telli Yamamoto, Okan University Social Sciences Institute, Turkey
Faruk Karaman, Okan University Social Sciences Institute, Turkey

A. INTRODUCTION

In regards to the Internet, the most important issue is apparently security. Anti-virus and anti-spyware programs, firewalls and other methods of encryption all try to achieve enhanced security; however, all these solutions proved to be still insufficient. Without resolving security problems, the full potential of Internet and e-business cannot be achieved.

Formerly, the Internet was mostly text-based and users were more technically oriented. With added multimedia capabilities, new web browsers and the explosion of other web applications, the user has become broadened. However, the newcomers are extensive consumers with general knowledge of web rather than computer professionals armed with TCP/IP, routers, switches, ports etc...

A complete new approach to Internet Security (IS) is urgently needed. The end user should not be responsible for his or her own security nor should be an expert in complex, computer technical details. This would be unrealistic. A Central Authority for Internet Security (CAIS) is needed to lessen the burden on the end-users. In this study, we tried to model such a central authority and develop a User Rating System for the Internet (URSI). This system aims to establish a large-scale security infrastructure that will be the solution to a great majority of the security threats faced over the Internet.

B. COMPONENTS OF THE URSI SYSTEM:

The URSI system has the following components:
Internet Access Point Protection (IAPP),
Central Authority for Internet Security (CAIS),
Centralized Database for User Ratings (CDUR),
User Ratings Software (URS),
Conflict Resolution Committee (CRC),
Country-based Internet Security Offices (CISO),
Firm-based Internet Security Departments (FISD),
User Ratings Client Software (URCS),

Naturally, the proposed URSI system needs to be much more complicated than the outline above. However these components give an idea about the overall picture. In Figure 1, a simple organizational chart of the CAIS is given.

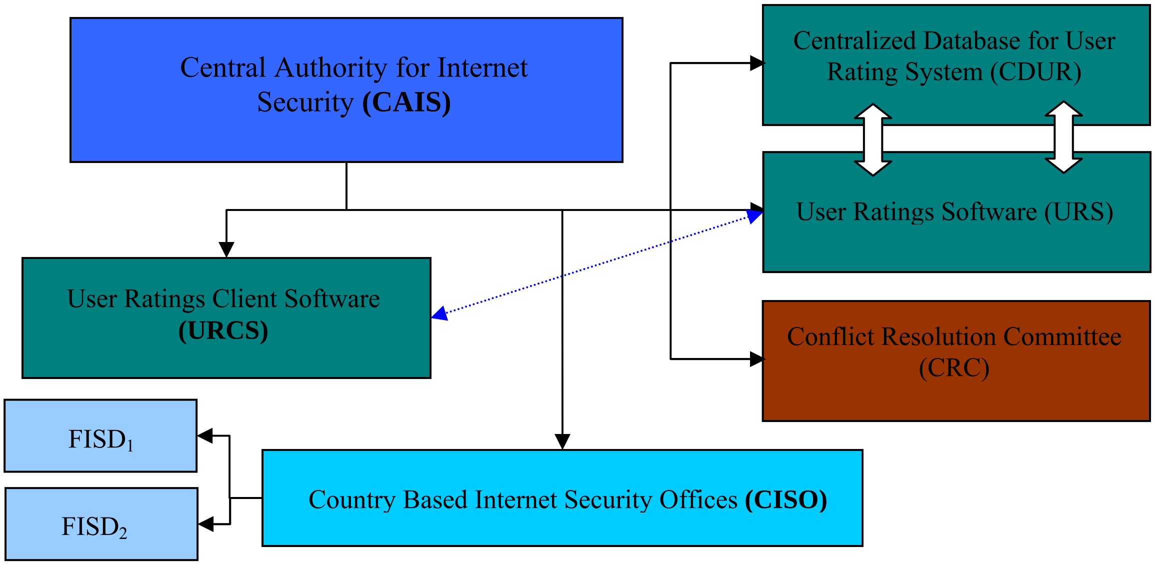

Central Authority for Internet Security (CAIS)
Centralized Database for User Rating System (CDUR)
User Ratings Software (URS)
User Ratings Client Software (URCS)
Conflict Resolution Committee (CRC)
FISD1
FISD2
Country Based Internet Security Offices (CISO)

Figure 1. Organizational Chart of the Central Authority for Internet Security **(CAIS)**

C. A GLOSSARY OF THE TERMINOLOGY AND ITS COMPONENTS:

The Internet Security ID (ISID)

Under the URSI system, each Internet user will have an Internet Security ID (ISID) and Internet Security Password (ISPW) given by the Central Authority of Internet Security (CAIS). The user first applies to the country-based Internet Security Offices (CISO) and the CISO will personally contact with the user and verify and collect information such as pictures, addresses, telephone numbers of, names of, occupations etc. The authorized CISO office is the office of the country the user is living. Once the ISID and ISPW are given, the user can travel to another country and can use the CISOs of that country for user information updates. The ISID and ISPW should be valid for only two years and users are required to re-apply for the nearest CISO office to update information.

In addition, the data collection will be based on classical methods, not via Internet or by means of digital technology. However, user information will be later transformed into the digital form as well.

User Ratings Client Software (URCS)

After getting the CAIS's approval for user application from the CISO office, the user can set access to the CAIS's user management website. The user will next download the User Ratings Client Software (URCS) to his or her computer. For public computers, the web-based version of the URCS will be used which will keep track on the user using that particular computer. Companies and institutions can install the corporate version of the URCS and give each of their employees an ISID and ISPW after a corporate-wide application has been put into use.

The IAPP Component

This component of the URFI system encompasses the software and hardware utilities used at Internet access points to ensure Internet security. The Internet access points here are defined as Internet Service Providers (ISP) and Telecom operators. Each ISS and Telecom operator will install the IS technology to ensure that each user has a unique ISID and ISPW number and can only access the web-sites and web-pages his or her user ratings allow.

In other words, the IAPP component is another enforced wall or layer of security to ensure that each user has only one ISID and one ISPW number. In fact, the URCS component can normally perform this task; however ways to circumvent the URCS security may be available for experienced users. Once a security loophole is available to advanced users, it finally becomes available to ordinary users via the programs written by those advanced users. Therefore, IS mechanisms should target the most knowledgeable and advanced users. New layers of security should be frequently added when possible.

User Ratings Software (URS)

The CAIS uses the data it collects to base its rating decisions. These decisions are automatically performed by globally centralized software called the User Ratings Software (URS). The URS uses the CDUR database maintained by the CAIS.

CDUR Database

This is a huge database including ISIDs, ISPWs, user pictures, addresses, e-mails and past Internet usage. CAIS uses data mining applications to discover fraudulent and malicious behavior. But, ISPs and Telecom operators can not access user information. They can not collect and establish their own database as well. But CISO's can apply for collecting user information. However, user ratings can only be given by the CAIS. The user or the CISO's can object to the ratings.

The CDUR database is the most controversial part of the URFI system. Naturally, Internet users, companies, governments ... etc. will be uneasy about the possible abuses of the CDUR database. There is an apparent trade-off here. For a much secure Internet a centralized database and a user rating system are needed. However, such a database shifts the power to the CAIS and its workers. Therefore, a Conflict Resolution Committee should be established for this purpose. Also, the CDUR and rating departments should be totally separate to divide the power among the departments.

Reporting Illegal User Activities

The CISO offices and FISD departments can report illegal user activities to the CAIS, but the final rating decision should be given solely by the CAIS. This is to ensure that no single company, country or individual can misuse the rating system. The users, companies, and countries can apply to the CRC committee of the CAIS to object about a particular rating.

The Conflict Resolution Committee (CRC):

CRC committee, although part of the CAIS organization, is a totally, independent legal foundation established to audit the CAIS especially the CDUR and the ratings department. The CRC committee can be established by nominees from all countries and should consist of IS professionals and lawyers. The CRC committee is very crucial for the overall system. The CAIS is an independent ratings agency to rate Internet users and CRC is an independent legal body to control CAIS's activities. The CRC will also be responsible from streamlining the individual country jurisdictions according to the International Internet Regulations (IIL) and International Internet Security Regulations (IISL). CRC is to be a member of the legal body developing the IIL and IISL regulations. ISID and ISPW thefts and pseudo-ISIDs' and pseudo-ISPWs' issues should also resolved by the CRC.

D. USER RATINGS SCALE

In this section we suggest a user rating scale. This scale is only for descriptive purposes and is by no means the final word as with every concept in this paper.

A-Rating:
This user can access the Internet freely, just as today's unmonitored and free Internet user. No restrictions for his or her activity exist, however user activities is to be monitored by the CAIS through his or her ISID. Internet activity is to be stored in the CDUR database but not in details. The disadvantage is: by doing so, the resources of the CDUR database can be exposed to malicious users.

B-Rating:
This user has been convicted with several spam activities and at least three authorized Internet companies (web-site, messenger, ISP, telecom operator) reported such activity to the CAIS. Thus, the user's rating was downgraded from A to B. This user can access to the Internet. However, this user is subject to mailing restrictions. The number of total mails that the user receives and number of total recipients the user sends are limited.

C-Rating:
This user is a through spammer and tries to circumvent CAIS activities to track his activity or limit his actions as a result of his B-rating record. As a result of the user's record, his or her rating has been downgraded to a grade of C. In this situation, the user's mailing quota is highly restricted and in some cases requires approval. In addition, this user's Internet activities are stored in the CDUR database in a more detailed manner than the A-rated or B-rated users since this user is a candidate of illegal uses of the Internet.

D-Rating:
This user tries to access other users' PCs and this has been proven by certain means caused not by a virus. This particular user has intentionally violated the privacy of other users. In this case, this user's Internet usage is restricted and s/he cannot use critical services such as financial banking, consumer ordering, and credit cards. After a certain time period if the user stops malicious behavior, s/he may be released from the restricted status. However, repeated violations may result in more severe restrictions.

E-Rating:
This user tries to access a company's computer system and the user's action has been proven to be intentional and not result of a virus. Such a user will be under very restricted Internet access. He or she can receive e-mails but cannot post him or herself. The user also can also access a very restricted number of web-sites allowing other E-rated individuals to access their websites.

F-Rating:
This user tries to access a governmental agency's databases or an international agency's systems, have stolen or tried to steal credit card numbers or other critical user information, or committed another type of severe crime over the Internet. Such users are totally banned from the Internet for a period suitable to the crime they committed. Their ban period is determined by the CAIS in accordance with the International Internet Law (IIL) and International Internet Security Law (IISL).

E. CONCLUSION

In this study, we tried to highlight several important issues about Internet security (IS). The need for
A Central Authority for Internet Security (CAIS),
All Internet users to be given a single and unique Internet Security ID (ISID) and Internet Security Password (ISPW),
All users to be given URFI ratings ranging from A to F,
To stop Internet users who commit malicious behavior from being treated equivalently and having equivalent rights and freedom over the Internet,

There are some disadvantages as follows:
The establishment of an effective and powerful CAIS requires approval and participation from most of the countries if not all,
Internet companies should have the willingness to take part in the Worldwide Internet Security System (WISS),
The IAPP component means a technological shift to ISP and telecom operators and may require huge investments in new hardware and software,
The CDUR database maintained by CAIS may raise privacy issues and individuals, companies and countries may fear possible abuses from users.

Even such a centralized user rating system will not solve all of the IS problems. However, such a system will provide a base for more sophisticated systems. Once each user has a single and unique ISID and ISPW to access the Internet and be given an Internet rating, it will be much easier to monitor illegal activities over the Internet.

For enhanced security over the Internet; individuals, companies, institutions, and countries should cooperate. That cooperation should be organized by means of a centralized organization such the CAIS. The CAIS can be a part of the United Nations or a part of a larger Central Internet Authority formed by present regulatory bodies or organizations such as the Internet Activities Board (IAB), the Internet Research Task Force (IRTF), the Internet Society (ISOC), the Internet Engineering Steering Group (IESG), the Internet Assigned Numbers Authority (IANA), and the Internet Corporation for Assigned Names and Numbers (ICANN).

Up until this date, the Internet is unmonitored, and unsupervised. That makes it a haven for criminal activity, but that image should change if we as human beings want to exploit the full potential of the Internet and e-commerce. This will mean less freedom and less privacy. Without sacrificing freedom and privacy, we cannot obtain more security.

A less free, less open, less private but much more secure Internet is much more beneficial to the individuals, companies, countries, and to humanity as a whole. As Internet fraud and crime will explode to a great extent this point will become much clearer and a need for a Central Authority for Internet Security (CAIS) will become much more apparent. If the need for CAIS is widely accepted, the rest will be more straightforward. In the early days of the automobiles, there were no traffic rules and regulations. Today, we have a highly regulated traffic system with user databases, traffic polices,...etc. Presently, the Internet may be unregulated but this cannot continue. The Internet version of traffic laws, polices, central organizations should be established in the future. However, every step in establishing the CAIS will shorten the era of virtually unrestricted freedom and crime over the Internet. This study aims to be one such step.

MOVING TOWARDS A PROACTIVE APPROACH TO MALWARE PREVENTION

Samuel Falkinder, University of Ballarat, Australia
John Van Beveren, University of Ballarat, Australia

ABSTRACT

The proliferation of malware attacks on the Internet has become a concern for computer users and system administrators worldwide. In spite of the large infection rates of the malware, a relatively small amount of studies have been completed that investigate malware distribution methods, target determination and infection. Many of these studies contain biased samples of malware or are based on a single case study and experimentation of a single strain. A systematic and unbiased study of all of the available malware is needed. The study of a sample of available malware in this dissertation will provide a broad categorisation, enabling the development of techniques for a proactive approach to prevent future malware attacks and infection. The results of this exploratory study have provided insight into the popular malware attributes among virulent strains. The findings of this study will help inform users and administrators of the vulnerabilities that need to be protected within computer and network systems.

INTRODUCTION

Recently much malicious software, such as viruses, worms and trojans, commonly called malware, have been written and released onto the Internet to intentionally cause damage. The technology news website - ZDNet, has declared the first half of 2004 as a terrible period for malware. From the beginning of 2004 until June 2004, an average of 50 worms and viruses were discovered each day. Cumulatively this amounts to 9,100, almost half (4,400) of which are variants of original viruses, worms and trojans. This is in addition to the predicted 18,000 that will be detected in the second half of the year, totalling more than all the malware discovered in 2003 (Network Associates, 2004). McAfee Inc. ® (2004) declared 31 of the worms and viruses detected in the first half of 2004 as medium to high risk. This is compared to 20 in the same category for the whole of 2003. It has been estimated that there are over 81,000 known malware threats that currently exist on the World Wide Web (Network Associates, 2004).

Due to the large reach and generally expedient distribution, huge costs can be incurred globally. It has been estimated that the combination of Sobig, MyDoom, Klez, Mimail, Yaha, Swen, Love Bug, Bugbear, Dumaru and SirCam, has cost over $US135 Billion to businesses and individuals worldwide since their releases onto the Internet (Mi2g cited by WholeSecurity, 2004).

The potential loss from infection of a worm or virus is attributed to the impact that the payload could deliver. A payload is defined as “the malicious activity that the virus performs” (Symantec, 2004). The effectiveness of the payload depends on what the malware was created for. For example, some payloads may be aimed at deleting all the files of a computer once the computer is infected. Others may open files and take the information from them without the user knowing.

Various categories of payloads have been identified (Elder & Kienzle, 2003; Harrison, 2004; Weaver, Paxson, Staniford & Cunningham, 2003). The categories include those that: cause system instability, compromise security settings, degrade system performance, delete files, modify files and/or release confidential information. The categories are not mutually exclusive or independent. Crucial files required to run the operating system or programs are deleted causing system instability or degradation of system performance. Similarly, security settings may be compromised by creating accounts, which the perpetrator can use to gain unauthorised access to the system. These accounts are often termed as 'backdoors'. Furthermore 'backdoors' can lead to the deleting or modifying of files. Confidential information stored on a computer may also be leaked, information including credit card numbers, bank details or usernames and passwords, sensitive files or emails could be copied or taken and distributed on the Internet.

Malware containing hybrid payloads have been released. For example a worm named MyDoom was released on the 27th of January, 2004. It was reported to be the most destructive worm found on the Internet (F-Secure cited by News.com, 2004). It compromised security settings and provided avenues to delete files, modify files and release confidential information. MyDoom was a mass mailer that sent large amounts of email, which was junk mail or contained an attachment containing the malicious code of the worm. The malicious component was disguised in an attachment with one of the extensions .bat, .cmd, .exe, .pif, .scr, or .zip. The intention of the payload was to open Transmission Control Protocol/Internet Protocol (TCP/IP) ports on a machine to allow an attacker to access information on the infected computer and computers connected to it via a network. In addition to the 'backdoor', MyDoom was set to carry out a Distributed Denial of Service (DDoS) attack on the Santa Cruz Operation (SCO) at a particular time and date.

At the start of its active life MyDoom was contributing to 20 to 30 percent of all email traffic. On the day of its release infections reached over 500,000 computers in one day (F-Secure, 2004). It was reported that Network Associates® received 19,500 emails with MyDoom attachments from 3,400 unique email addresses in one hour (News.com, 2004). Over the duration of its short life the original MyDoom and all of its variants (which are still filtering throughout the Internet) cost users over $US22.6 Billion worldwide (Mi2g, 2004; WholeSecurity, 2004). The potentially devastating impact of malware is apparent in the MyDoom example.

MyDoom and other malware released recently, such as MSBlaster, Sobig and Melissa, have been well publicised and well reported by the victims, but there are also victims who do not report the occurrences of viral attacks. Due to the world wide distributions of malware it is possible that malware statistics could be even greater.

One of the first major successes in apprehending malware authors was possibly the capture and prosecution of the Melissa author David L. Smith in 2002. He was sentenced to 20 months in prison and ordered to pay a $5,000 fine; in addition he was condemned to 3 years of supervised release with no Internet use, network or bulletin board access (Bowman, 2002). Although the Melissa virus was not malicious in that it did not delete or render system files unusable, its distribution still caused chaos by blocking up email systems worldwide, costing $US80 Million globally.

It is apparent that the motive behind the payload of Melissa was to cause disruption and exploit Microsoft's® software vulnerabilities. In November of 2003 Microsoft® offered an incentive of $US250,000 for anyone who supplied information which could lead to the capture of the suspected malware authors of other notorious malware such as SirCam, Code Red, Slammer, Nimda and MyDoom (USInfo, 2003).

The amount of destruction that the viruses and worms incur, may suggest that the prevention techniques adopted by individuals and network/system administrators in organisations are insufficient. Simply utilising a security gateway between a private network and Internet or a firewall and 'up-to-date' antivirus software may not be enough to prevent the infiltration of malware into a network. Lack of social awareness is a large contributor to malware infections. The payload causes the most damage; awareness of the payload may prevent infections from being so prevalent.

Recent research into different distribution methods (Fryar & Van Beveren, 2004) has shown that there are links between the motives of malware attacks and the distribution methods employed. Furthermore, payload is directly related to the distribution methods employed and intrinsically the motives behind the attack. Further research is required to investigate whether there are certain distribution methods and payloads that are effective in executing certain types of attacks. Such insight may well help inform computer users of techniques they can employ to be more proactive at preventing infection and attack. The purpose of this study is to systematically investigate the distribution methods and payloads of malware and illuminate the main methods employed by malware writers.

LITERATURE REVIEW

Writers of malware have various motives for creating them. To understand these motives two options are available. First would be to interview those writers who are arrested (cf. Jordan & Taylor, 1998). However, this approach has limitations in that the sample and results may be biased. Those captured are a subset of those writing malware and their reported motives may be contrived and untruthful. The second option is to investigate the attributes of malware and their consequences. This approach involves studying the malware itself and the effects that it has post release.

Malware

The literature that specifically investigates malware can be divided into three types of studies. A small number of studies have investigated the specifics of individual notorious viruses and worms (Moore, Paxson, Savage, Shannon, Staniford & Weaver, 2003; Eichin & Rochlis, 1989; Brown, Moore & Shannon, 2002). Other studies have focussed on the prevention techniques concerning these worms (Bakke, Beattie, Cowan, Grier, Hinton, Maier, Pu, Wagle, Walpole & Zhang, 1998; Twycross & Williamson, 2003; Williamson, 2002). Few studies have provided a broad overview of malware looking at factors such as target discovery, distribution methods, activations, payloads and motivations (Elder & Kienzle, 2003; Weaver, Paxson, Staniford & Cunningham, 2003).

Moore et al. (2003), Eichin & Rochlis (1989) and Moore et al. (2002) respectively investigated specific malware code for the Slammer, Morris and Code Red worms. They provide an in depth look at almost every aspect of the virus throughout its life - from initial release, inner workings, victim response, damage caused, downfalls and containment. Moore et al. (2003) and Moore et al. (2002) who investigated the Slammer worm and Code Red worm respectively have utilised a case study data collection method often providing a limited view of malware as a whole. Because they are individual cases they can often not be generalised to illustrate malware as an entirety, due to the diversity of worms and viruses. The Morris paper by Eichin and Rochlis (1989) still only focuses on an individual attack demonstrating the same deficiencies. Eichin and Rochlis (1989) have simulated the release of the virus into the wild by capturing an instance of it on a local network and studying its behaviour illustrating an exploratory and experimental method of data collection.

Despite the limited scope of these papers in terms of generalisation applicable to other pieces of malware, they cover the individual viruses thoroughly, providing detailed descriptions. This may prompt further investigation into individual pieces of malware in a more comprehensive way, providing detailed insight to the overall prevention and detection techniques, to restrict the spread and payload devastation.

Weaver et al. (2003) and Elder and Kienzle (2003) provide a broad overview of viruses and worms as a whole. Each paper attempts to divide all different types of malware into categories. The survey by Elder and Kienzle (2003) presents less than fifty worms that are considered to be “breakthrough or novel”, discounting a large amount of data, which didn’t fit into this category. The categorisation of the worms is then made, based on the worm’s characteristics. Although the five categories may be sufficient enough to capture the chosen sample, the more thorough categorisation for worm organisation outlined in the paper by Weaver et al. (2003) may be more appropriate. Weaver et al. (2003, p.1) has constructed a “preliminary taxonomy of various possible worms, payloads and attackers as an initial guide to plausible defences”. The taxonomy is presented in five sections: target discovery, propagation carriers, distribution mechanisms, activation and payloads. Each section provides real world examples, generally illustrating how and where the malware of today fits over the categories. The exploratory nature of the study prompts Weaver et al (2003) to admit to the incompleteness of the taxonomy due to the constant stream of new tactics, payloads and attackers rendering a number of examples redundant to future readers.

Prevention

Prevention and protection are large factors that need to be taken into consideration when discussing malware. Cowan et al. (1998) Twycross & Williamson (2003) and Williamson (2002) look at the use of traditional prevention and protection methods such as firewalls, antivirus software and user vigilance in association with newer revolutionary techniques such as virus throttling and buffer overflow attack (adding more information to a buffer than it was designed to hold, leading to instability) and preclusion, which has been utilised in such viruses as, Nachi, Lovesan, Sasser, Bagle and MyDoom.

Cowan et al. (1998) investigates Automatic Adaptive Detection and Prevention of Buffer Overflow Attacks. They claim to provide a “systematic solution” to buffer overflow malware attacks. The buffer overflow error is said to be a “serious security fault in software that result from minor programming errors” (Cowan et al., 1998, p.10). The paper is presented in 6 sections: buffer overflow attacks (explained in technical detail), how to defend against buffer overflow attacks, stack guard performance (experimental results), implications, further research and conclusions.

Although buffer overflow attacks have been occurring since 1988, in the Morris attack, only a small set of commands to correct a bug in a computer program known as ‘patches’ have fixed the problem in the past. Cowan et al. (1998) presents a technical overview to provide a more robust solution to the problem. Experiments are used to collect the data. Cowan et al. (1998) searched the web to find examples of the buffer overflow code to test the resistance and the performance impact on the computer system. Considerations of cost, time and performance are included in the discussion. Cowan et al. (1998) provides a specific solution to a wide spread problem, with experiments and technical examples. Though the information presented is successful in preventing the buffer overflow attacks it is by no means a total solution to the malware epidemic.

METHODOLODGY

Forty (40) species of malware were extracted from the Symantec® database, which contains 32,255 records, for analysis. The selection of the sample involved simple random sampling 15% of the sampling frame (15% of the 32,255 records); removal of duplicates, removal of records that are not viruses, trojans or worm; and stratified sampling to select those that are considered to be virulent in terms of distribution and damage caused by their infection.

The secondary data attained for the technical details of malware from Symantec® is qualitative and predominantly textual. The appropriate data analysis technique for this data is thematic analysis. Thematic analysis involves a coding process with three phases: open coding, axial coding, and selective coding (Babchuk, 1997). Each phase of the coding is systematic and breaks down the data for further analysis. Open coding is the initial phase which involves breaking down the data. Open coding data is gathered and grouped together via constant comparison to form categories and properties. Each of the technical details for the 40 species of malware were analysed and keywords and phrases were extracted, 427 keywords and phrases associated with the attributes were identified. The axial coding phase involves forming hypothetical relationships between categories and subcategories. Strauss and Corbin (1990, p.97) explain this phase as putting "data back together in new ways by making connections between categories and subcategories". Selective coding is described as the process by, which categories are related to the core category ultimately become the basis for the grounded theory (Babchuk, 1997).

FINDINGS

Malware Categories

This chapter presents the findings relating to the formation of categories discovered from the thematic analysis of the data. From the technical details of the 40 most virulent malware (6 viruses and 34 worms) contained in the sample, 427 keywords were identified and clustering of the keywords formed 16 categories. Three of these categories contain three sub categories and the Major Malware Actions category contains nine further sub categories. Each of the categories are presented in alphabetical order and are discussed in this chapter.

The 16 categories formed from the sample are: Action/Condition Required, Display Attribute, Authentication, Email, File, Language, Major Malware Actions, Microsoft®, OS/Network, Payload, Ports, Protocols, Random, Registry, Target Determination and Vulnerability Exploitation. The categories were formed from the identified keywords in the sample (a piece of malware may have several keywords from a range of categories) which were derived from the open, axial and selective coding process as discussed by Babchuk (1997) and Strauss and Corbin (1990) and outlined in the data analysis section of the methodology. The keywords were clustered according to their similarity. For instance all Microsoft® related keywords such as a particular operating system, a Microsoft® file extension or a Microsoft® program such as Office®, formed the Microsoft® category and subsequently the Microsoft® sub categories; Microsoft® Applications, Microsoft Office® Template files and Microsoft® Operating System Version. Some pieces of malware in the sample featured in several categories making them particularly virulent.

Action/Condition required describes situations where the malware can only deliver its payload to the target when an action or condition occurs. Such conditions or actions can result from either the user or an action of the operating system, or other software. Nine pieces of malware contained within the sample had attributes of this nature. Some of the malware are set to run on the start up of Windows® and therefore need no action or a condition as this is a part of the malware's initial infection. If the malware needs a trigger to begin its infection it can be automatic and activate on a specific user action, or may require the user to physically click on a link or download a file or carry out a task in the operating system. User education and vigilance is a major role in preventing attacks which result from a task being carried out either automatically or manually triggering the malware to infect the systems.

Authentication refers to the details needed to access a computer system, file or folder. Often a malware infection will exploit weak or non existent authentication, causing problems with data integrity and confidentiality. Three pieces of malware from the sample contained identified keywords with characteristics concerning authentication and authentication breaches. Authentication and password protection is one of the best methods of protecting data on a computer system but weak passwords or inadequate authentication, can leave a system or network open to attacks, which may result in breaches of file continuity, confidentiality and integrity.

Display Attribute refers to when the malware changes the visual appearance of the operating system or application programs. For example, the background picture of the computer may be altered, or the properties of the mouse or keyboards display type may be altered, as in the piece of malware W32.HLLW.Cydog@mm from the sample. W32.HLLW.Cydog@mm "Attempts to change some mouse and keyboard parameters, such as the cursor blink rate or the character repeat delay" (Symantec, 2005).

Email is a keyword that occurs in many of the malware in the sample. It refers to the method of distribution and/or a method of infection. Email is the most widely used method of distribution for the malware in the sample. 90% of the sample contains an email related action in either the distribution, infection or both. In most cases the malware is distributed via email to addresses that are harvested from address books found on the infected systems from popular programs like Microsoft Outlook® and then distributed via the computers email account details, mail server or the malware's built in SMTP engine (Simple Mail Transfer Protocol, used for delivering email).

The sample contained 29 pieces of malware that used client email (not inbuilt SMTP) as one of their methods of distribution, which contained a mass mailing routine. This mass mailing routine enables the malware to propagate to harvested and/or hard coded email addresses. When malware does not propagate via a mail server or local email account, it may propagate independently with a built in SMTP engine. The sample yields seven examples of malware that use this technique. The W32.Yaha.AF@mm worm extracts target addresses from a number of sources on the computer such as the Windows® address book, MSN®, Windows Messenger®, Yahoo Pager® and/or ICQ Pager®. W32.Yaha.AF@mm attempts to use the default SMTP address in the computer to send the email. If there are no SMTP addresses on the system, the malware will use one of its own many hard coded SMTP addresses.

File is a category which contains three sub categories; Files, File Sharing/Chat and File System. The category is made up of keywords, which relate to file names and extensions. These keywords are found in the technical details of the malware from the sample and relate to the name of the files infected by the malware and/or the aliases they utilise to hide from being discovered.

Files is a sub category of File. It deals with file names and extensions associated with the infection and targets of a piece of malware. Every piece of malware in the sample contains an association with a file, generally a file from the operating system that is infected when the malware's payload is delivered. Executable files with the .exe extension are a particularly popular target for the malware. W32.Alcarys.B@mm copies itself infecting the hard drive as a range of .exe files creating new files and overwriting existing system files required for the operating system to function correctly. An unstable or unusable operating system can compromise the integrity and convenient access of data on the computer.

File Sharing/Chat is the second most prevalent method of malware distribution from the sample, after email. Seven pieces of malware from the sample utilise file sharing and/or chat.

File sharing has become particularly popular in recent times. Free file sharing programs enable access to millions of computers world wide via a shared folder available to all other file sharing users to download a range of files such as: audio, video, images, word processing documents, virtually any file. Some malware authors have utilised the shared folders to distribute their malware. When unsuspecting users download what they think is a legitimate file, which is actually malware, their computer becomes infected. The files are cleverly named as popular desirable files that users want to download for no cost, which many people will download, infecting a large number of targets.

Chat is also a popular medium for malware distribution, which is closely related to the file sharing distribution method. Chat programs like IRC® (Internet Relay Chat), MSN Messenger®, Yahoo Chat® and ICQ® are used by millions (mIRC, 2005; Moore, 2003) of people around the world. Users chat on channels and on downloaded programs which they authenticate to for access. IRC® uses channels whereby a user may connect according to interests from general chat to movies and games. MSN Messenger®, Yahoo Chat®, ICQ® and the like are all downloaded programs that users install and authenticate to with their email address and a password. Once connected users have a list of contacts that are using the same program to facilitate real time communications and subsequently real time malware infection. Infected files can be sent via the chat programs. This distribution technique is utilised in five pieces of malware in the sample.

File System refers to file names, attributes and network related system commands. Some category keywords include: read-only, encrypted, hidden, sets the attributes, current folder, deltree, unprotect and delete. Twelve pieces of malware in the sample contain keywords identified specifically as file system related. Other pieces of malware in the sample contain file system related data, but not directly related to the keywords identified in the data analysis. The worm from the sample W32.Mylife.M@mm contains the DOS deltree command that deletes all files and folders in the root of drive C, which generally contains system information and data on Windows® based computers.

Language is a category that refers to the language, which is used in the workings or notification of the infection of the virus. Five pieces of malware in the sample all feature a language other than English. Identified keywords in the samples technical details included: Chinese, French, Hungarian and Spanish. Malware authors may use different languages as a social engineering tool to deceive users into running the malware. Different languages may also indicate the origin and/or the nationality of the malware's author, compromising their anonymity and perhaps leading to their apprehension and prosecution.

Major Malware Actions is a category made up of the main actions that are performed or can potentially be performed by a piece of malware in the sample. It contains nine sub categories which include: modifies, adds, copies, creates, deletes, disables, infects, overwrites and renames. All sub categories relate to the malware in terms of how the malware behaves or attributes it may possess.

Adds is a keyword found in the 26 of the technical details of the malware in the sample. The malware adds values or information into the Windows® registry, which is the database used to stores settings and options for hardware, software, users and preferences. The Malware generally alters the startup details to enable its operation on startup, adds services and/or processes to infect once the computer has been started without the users knowledge.

Copies is an attribute of the malware that facilitates its distribution used by all malware from the sample. The malware copying itself onto the hard drives of their target enables the infection to begin. On occasion when the infected file is copied it masquerades as another file to hide from detection. VBS.Annod.B, from the sample copies itself to the Windows system folder as a range of different files relating to sex, music, computer programs and operating system files. The malware is copied to the hard drive with no regard to the overwriting of essential system files required, to ensure the correct functionality of the operating system being infected.

Creates is similar to the adds keyword, but creates new files and registry keys rather than adding to existing files to alter system settings. The same 26 (65%) malware examples in the sample contain references to creation. W32.Lovgate.Y@mm's technical description includes several references to the creation of files and registry entries. The worm creates files in the Windows system folder which facilitates its backdoor routine. Registry entries that make the worm run on the startup of the operating system (contains several registry variations to ensure the worm starts no matter what Microsoft® operating system is installed on the computer) are created. Network shares and infected file sharing folders are also created to aid distribution.

Deletes relates to the deletion of files (user and system) and registry entries, which can lead to the loss of important files and the corruption and instability of the operating system, resulting in unusability. 17 pieces of malware in the sample all contain a command to delete. W32.Galil@mm from the sample contains a command, which instructs the malware to delete all of the files on the D, E, F and G drives, which are generally optical drives on most personal home computers but can contain vital data on servers.

Disables is a keyword found in several of the pieces of malware in the sample. To enable infection, security settings are disabled through the altering of the registry and the deletion of files related to a security product. System services that run antivirus and firewall programs can also be disabled to prevent them functioning. Ten pieces of malware in the sample contained technical details that referred to disabling.

Infects is a keyword that relates to the malware's action upon a file. Three of the four pieces of malware that make up the Infects category have a reference to Microsoft Office 97® programs, and exploitable functions such as macros and templates. Macro security settings are set to low and the default template is replaced by the virus, infecting the computer when the program is started. W32.Gunsan infects the network shared folders that the computer is connected to as a secondary distribution method with mass mailing.

Modifies is similar to the deletes and disables categories and relates to the modification of the registry and files. The registry can be modified to allow easier passage for the malware to infect successfully and deliver its payload. Modification can relate to any file, but in the case of the malware from the sample modifies refers to the modification of Windows® system files integral to the stable operation of the operating system. These files include Autoexec.bat, Config.sys, System.ini, Win.ini.

Overwrites is a keyword that appears in four of the technical details of the malware from the sample. Similar to the characteristics of the adds and creates keywords, overwrites alters files and registry entries to facilitate the infection and distribution of the malware.

Renames is the final major malware action identified in five of the technical details of malware in the sample. The renaming of registry keys and file names that relate to system functionality can lead to system errors and unusability preventing function of programs and the computer system.

Other attributes were identified but not deemed as major due to the frequency of their appearance in the technical details of the sampled malware. Actions identified in the malware attributes category are important in the malware's infection but do not appear as regularly as the keywords from the major malware actions category.

Microsoft is a category that relates to anything identified in the technical details of the malware that refers to Microsoft® applications, template files (associated with Microsoft® application Office®) and Microsoft® operating systems, which are the only operating systems that are targeted for infection.

Microsoft Applications are a prevalent target for infection of the malware in the sample. Programs like Microsoft Word®, Excel® and Outlook® from the Office® suite, which are word processing, spreadsheet and email programs respectively, are all exploited by the malware from the sample. Other Microsoft® applications such as MSDE 2000®, SQL Server 2000®, IIS®, Paintbrush® and Exchange® are also targets for infection of the malware in the sample where the ports required to run the programs are exploited by the malware, leaving backdoors open for malware authors to take control of the infected computer.

42% of the sample, targets the Microsoft Outlook® email program during the distribution and infection of the malware. This illustrates the malware authors' exploitation of the wide spread use of the program to enable infection of as many computers as possible. Three pieces of malware contain commands that exploit the Word® and Excel® programs. An example is the macro settings alteration, leaving users open to infection and the overwriting of templates with infected templates to enable the malware's operation when the program starts up. The vulnerabilities and wide spread use of Microsoft® applications ensure the products will be a popular target for malware infection and subsequent destruction of files and the loss of system stability.

Microsoft Office Template files are infected by malware O97M.Cybernet.Gen and W97.Melissa.A from the sample. The template files used in the Microsoft Office® programs are a target for infection as they can be easily edited and facilitate easy infection as the templates run on the startup of the program. Once the malware runs, the security settings for the programs are set to low and the infected template is installed over the default template without the user knowing.

Microsoft Operating System Version lists Microsoft operating systems from Windows 95® to Windows 98®, Windows NT®, Windows ME®, Windows 2000®, Windows XP® and Windows Sever 2003®. Some malware infect effectively on a single version or a limited number of versions while others are effective across all Microsoft® operating system versions. All malware in the sample target Microsoft® operating systems.

OS/Network category keywords that concern drive mappings and general networking commands, all related to Microsoft Windows®. Malware can infect the Windows® file system through network shares and printer shares. The malware infects important system files required for the stable and satisfactory operation of the computer putting the data at risk. All malware from the sample have attributes that alter the operating system to aid the infection as discussed in the Major Malware Attributes category.

Payload category contains the description of the actions that the malware performs when it is activated. Although only five keywords (Malicious payload triggered, Execute this payload, Virus copies itself under a random name, Unusual payload and Payload period) were identified during the coding phases, all malware in the sample contain characteristics of a payload. The email distribution and infection of files are payloads that are delivered by all malware in the sample.

Ports are a point of vulnerability in any operating system. A port is a logical channel for network communications. Port numbers range from 0 to 65536; the first 1024 ports reserved for privileged ports such as: HTTP (Hyper Text Transfer Protocol) on port 80 is used for Internet communications and FTP (File Transfer Protocol) on port 20 and 21 is used for file transfers locally and remotely. Email, which has proven to be the most popular method of distribution, uses the protocols SMTP (Simple Mail Transfer), POP (Post Office Protocol) and IMAP (Internet Message Access Protocol).

Protocols are methods and rules which are adhered to when computers communicate with each other. As discussed in the Ports category, there are particular protocols that are used in the distribution of email as well as general activities. As ports are exploited by the malware, protocols can also be exploited and used to the benefit of the malware. MAPI or Messaging Application Programming Interface is a protocol, which is used by email programs as a standard to communicate. It is used to facilitate the harvesting of email addresses from programs such as Microsoft Outlook® for mass mailing routines.

Random contains key words that refer to the random nature and characteristics of the malware. Malware that contains a random attribute can often be unpredictable and be harder to detect due to its ever changing nature. Four pieces of malware from the sample contain references to a random element. W32.Mydoom.F@mm's technical details contained the keywords: Randomly generated data, randomly named copies, randomly selected folders and randomly generated file names. All of the attributes relate to the creation of the infected file that contains random data, has a random file name and is in a random folder in the operating system. The random nature of the infection makes the initial detection of the worm more difficult.

Registry is identified as a keyword in the data due to the frequency of its editing to facilitate the malware infection. The registry is a database in the Windows® operating system that stores settings and options for hardware, software, users and preferences. The major application of the registry changes (modification and addition of keys) from the malware in the sample is to set the malware to run on the startup of the operating system. This enables the infection of the local computer and allows distribution to continue. Only three pieces of malware from the sample did not contain the identified registry keywords in their technical details.

Target Determination's technical details contain information pertaining to the method, in which the malware determines its target for infection, most of which are extracted from address lists associated with email and chat programs. The identified keywords from the technical details also refer to predetermined targets found in hard coded lists written into the malware and details relating to the generation of random addresses for distribution.

Vulnerability Exploitation refers to the exploitation of known vulnerabilities when the malware infects. The vulnerabilities are often found in application programs, such as Microsoft Word® and Excel®, and they are also found in the operating system itself. Microsoft® programs are the source of the vulnerabilities of all associated malware in the sample. The existence of the vulnerabilities makes systems that possess them an easy target for infection. Often it takes time for companies like Microsoft® to release program updates to prevent malware authors taking advantage of the flaws in their system. The solution may be the thorough testing and patching of software before it is sold to users, leaving them less susceptible to immediate infection.

Overview of Identified Malware Categories
Table 1 depicts the attributes that correspond to the malware sampled in this study. Some of the categories (File, OS/Network, Malware, Target Determination) are excluded from the table as they occur across all species contained in the sample. The subcategories for Major Malware Attributes are presented on the right hand of the table and represent the actions resultant of infection. The set of categories on the left portion of the table represent the necessary conditions and programs that are required for the malware to be effective.

The relationships between 10 of the 16 identified categories and the malware contained in the sample are presented in table 1. File, Malware, Microsoft, OS/Network, Payload and Target Determination are categories associated with all malware in the sample which are excluded from table 1. The wide spread of these attributes in the sample indicate that all malware from the sample infect target files on Microsoft® operating systems via the determination of a target usually utilising email harvesting in order to deliver a malicious payload.

DISCUSSION

Microsoft Windows® is the most popular network operating system used by hundreds of millions of people worldwide with a 97.34% market share in 2003 (OneStat, 2003). In comparison, Apple Macintosh and Linux operating systems are used by 1.49% and 0.51% of the market share respectively. This market share is reflected in the sampled malware as 100% of the samples target Microsoft Windows® operating systems. A vulnerability of the Microsoft® operating systems is the registry and the editing of the Microsoft® registry is a popular method of attack. 90% of the malware in the sample contain a reference to deleting, disabling, modifying, coping, adding, creating, overwriting or renaming attributes of the registry to facilitate the malware's infection and payload delivery. The Windows's® system files required to run the operating system are also a popular target for attack through the major malware attributes identified on the right hand side of table 1.

The sub categories of Major Malware Actions, adds, copies, creates, deletes, disables, infects, modifies, overwrites and renames are included in the right hand side of the table as they are attributes of many of the malware in the sample and provide insight to the targets of the malware. The main themes that are derived from the sample and illustrated in the table were a frequent occurrence of the attributes copies, adds and creates. These attributes were common actions performed with the Action/Condition Required, Vulnerability Exploitation, Authentication and Protocols attributes in the malware from the sample, but were also found with all other attributes in the sample, although less frequently.

The Email category and the identified attributes associated with them were found in 90% of the sample. Email distribution coupled with the address book Target Determination methods discussed in the findings proves to be a successful technique to ensure maximum spread and infection in the sample.

Table 1: Summary of the Malware Attributes Against Sampled Malware Species.

Malware Name/Category	Action/Condition Required	Authentication	Display Attribute	Email	Language	Ports	Protocols	Random	Registry	Vulnerability Exploitation	Infects	Deletes	Disables	Modifies	Copies	Adds	Creates	Overwrites	Renames
O97M.Cybernet.Gen	X			X				X			X	X	X	X		X			
VBS.Annod.B	X			X											X		X		
VBS.Bingd@mm	X			X	X				X					X	X	X			
VBS.LoveLetter.BJ	X			X			X		X							X	X		
W32.Alcarys.B@mm				X					X			X		X	X	X	X	X	
W32.Beagle.AW@mm				X					X				X		X	X	X		
W32.Blaster.E.Worm	X						X	X	X				X			X			
W32.Bugbear.B@mm				X					X				X		X		X		
W32.Darby.B				X	X				X	X			X	X	X	X	X		
W32.Dumaru.Z@mm				X					X			X	X	X	X	X	X		
W32.Erkez.A@mm	X			X	X				X						X	X	X		
W32.Erkez.C@mm	X			X	X				X				X	X	X	X	X		
W32.ExploreZip.F.Worm				X			X		X					X	X				
W32.Galil@mm				X					X			X			X	X	X		
W32.Goner.A@mm				X					X							X			X
W32.Gunsan				X			X		X		X	X		X	X	X	X		
W32.HLLW.Backzat.B				X					X						X	X	X		
W32.HLLW.Cult.C@mm				X					X						X	X	X		
W32.HLLW.Cydog@mm			X	X					X						X		X		
W32.HLLW.Gaobot.gen		X				X			X	X			X		X	X	X		
W32.HLLW.Lovgate.C@mm		X		X			X		X					X	X	X			
W32.HLLW.Nebiwo									X						X				
W32.HLLW.Oror.AI@mm				X					X										
W32.Jantic@mm				X	X														
W32.Lavehn.A@mm				X					X			X			X				
W32.Lovgate.Y@mm				X			X		X						X	X	X		
W32.Mimail.J@mm	X			X					X						X	X			
W32.Mumu.B.Worm		X							X						X		X		
W32.Mydoom.F@mm				X				X	X					X	X	X	X		
W32.Mylife.M@mm				X					X			X			X	X		X	
W32.Naco.B@mm	X			X		X	X		X			X	X		X	X			
W32.Nimda.B@mm				X					X					X					
W32.Pandem.B.Worm				X			X		X						X	X			
W32.Sober.E@mm				X			X		X						X	X	X		
W32.Sobig.E@mm				X		X			X						X	X			
W32.Swen.A@mm				X			X	X	X	X				X	X	X	X		
W32.Yaha.AF@mm				X		X			X				X	X	X	X	X	X	X
W32.Yarner.A@mm				X			X		X			X			X	X	X		
W97.Melissa.A				X			X		X		X		X			X	X		
W97M.Service.A				X					X		X								

Ports are essential for the connection of a computer to a network to allow communication. Microsoft® operating systems are known for activating vulnerable ports on default installations and being unprotected, allowing unsolicited entry and infection. The use of ports is a less frequent attribute that was discovered in the malware in the sample but still has constant references to the identified keywords disables, modifies, copies and adds. Ports need to be open or set to stealth for the computer to communicate using them. Preferably the ports should be set to stealth to prevent the identification of openings by the malware with scanning cabailities. A hardware or software firewall can be a convenient way of securing ports. Computers that do not have software or hardware firewalls to prevent malware scanning and infiltration are open to attacks. Random is a keyword that was identified from the technical details. Although it was not utilised in many of the malware in the sample, the potential that this attribute has to wreak havoc on a computer system is significant. The random nature of a piece of malware makes it more difficult to detect, enabling it to stay resident on a computer system. This causes problems when it is coupled with a delete attribute and enables the infection more targets over a longer period of time before its detection and eradication. Until the antivirus (antimalware) programs create signatures that detect the potential combinations of random letters and numbers, it is quite difficult to identify malware. This enables the worm to infect more targets before it is detected and stopped.

MANAGERIAL IMPLICATIONS

From what is understood with regards to Microsoft® vulnerabilities and the potential open access provided by systems being homogeneric, where potential hackers and malware writers are familiar with how these systems are structured, we suggest that computer users and administrators might be able to rename files and folders so that their system is less familiar. Further study is required to validate whether altering these file locations, filenames and folder names will allow the system to continue to operate effectively.

The findings also indicate that once a computer has been sent a piece of malware, the infected email message has the malware attached to it, which may facilitate easy infection when an uneducated user opens an infected attachment. User intervention is required for the activation and distribution of this malware, thorough user training of the identification of infected email, including the types of attachments added and the information in the body of the infected emails will lead to user vigilance and in turn reduce the amount of infections.

LIMITATIONS

The intention of the study was to conduct a systematic analysis of known malware. Although throughout this study this intention was maintained by the researcher and robust research methods were employed, some unforseen limitations with the sampling frame and available data emerged that potentially compromised the outcome from what was desired.

Sampling provides a convenient method to gather data for analysis when the initial sampling frame is too large or unpractical to analyse entirely. The limitation is present as the sampling method will invariably exclude important data. The data for the sample extracted from Symantec® and the Network Associates VIL® encyclopaedias had some differences, including missing and conflicting data which led to the need for cross tabulation to ensure there was adequate information available for the formation of the malware categories. The cross tabulation removed inconsistencies resulting in a reliable sample, but reduced the sample significantly and may have caused skews by potentially removing virulent malware that appeared in one encyclopaedia but not the other.

In the always evolving world of malware, creation and release of new strains of malware or variations of existing strains of malware is another identified limitation of the study. The gathering of the data for the study was completed at a particular point of time and not updated to ensure the completion of the study, including those pieces of malware that have been recently released. This limitation may be overcome with frequent studies, which include the new malware leading to a more thorough and up to date set of categories to determine the attributes and potential activities that a piece of malware may carry out. As malware evolves, the operating systems and programs they target also evolve. New versions of operating systems and applications may contain new vulnerabilities for the malware to exploit.

In the derivation of the categories from the malware, the study is somewhat limited. The researcher's decision to stop at a particular level of analysis and where each category starts and ends, particularly in the identification and selection of the Major Malware Attributes, can result in limiting the findings and conclusions made. While every attempt was made to be thorough and adopt robust methods, these methods are somewhat subjective in nature.

The final limitation of the study was limiting the sampled malware to worms, trojans and viruses. The sampling method omitted adware and spyware, which are also forms of malware. The length and time constraints for this study did not warrant the inclusion of the spyware and adware aspects of malware, as there is ample data and theoretical perspectives to warrant separate study of these types of malware.

FUTURE RESEARCH

There are many opportunities for further and ongoing research in this field of study. The methodology developed in this study has the potential to be used with other sources of data and may include the full sampling frame rather than a sample which could be repeated and updated on a regular basis, such as 6 months providing a dynamic list of malware attributes for computer users and administrators.

Adware and spyware excluded from this study may be considered as topics for further research. A specific study of adware and spyware is warranted due to the sheer amount and rate of infection of this type of malware found recently on the Internet. The purpose and motivations of adware and spyware is different to viruses, worms and trojans, one of their attributes is to track and record Internet and computer user's habits to aid marketing activities and consumer research on the Internet, the legitimacy of which is currently debated, in relation to privacy.

In the discussion it was suggested that computer users and administrators might be able to rename files and folders so that their system is unknown and unfamiliar to the potential hackers and malware writers. Further study is required to validate whether altering these file locations, filenames and folder names will allow the system to continue to operate effectively.

CONCLUSION

The purpose of this study was to identify common attributes of malware that result in the exploitation of vulnerabilities in computer and network systems. Several important attributes of malware that are common and constitute a malicious infection are revealed. Developing a better knowledge of which attributes commonly appear in virulent pieces of malware will lead to better measures for detection and subsequently proactive protection of computer systems. Such proactive measures should involve computer user training on how to detect malware and how to appropriately deal with it so as to protect their computer and network and other computers and networks.

ACKNOWLEDGEMENTS
Thanks are due to colleague Elizabeth Fryar, University of Ballarat, for help in initial data collection, methodology development and constructive criticism throughout the study.

REFERENCES

Babchuk, W.A. (1997). *Glaser or Strauss?: Grounded Theory and Adult Education*. Paper presented at the Midwest Research-To-Practice Conference in Adult, Continuing and Community Education.

Bakke, P., Beattie, S., Cowan, C., Grier, A., Hinton, H., Maier, D., Pu, C., Wagle, P., Walpole, J. & Zhang, Q. (1998). *Stack Guard: Automatic Adaptive Detection and Prevention of Buffer Overflow Attacks*. Paper presented at the 7th USENIX Security Conference.

Bowman, L.M. (2002). *Melissa virus creator gets 20 months*. Retrieved 02/08/04, from http://news.com.com/Melissa+virus+creator+gets+20+months/2100-1023_3-896464.html?tag=nl

Brown, J., Moore, D. & Shannon, C. (2002). *Code-Red: a case study on the spread and victims of an Internet worm*. Paper presented at the 2002 Internet Measurement Workshop (IMW).

Cunningham, R., Paxson, N., Staniford, S., & Weaver, N. (2003). *A Taxonomy of Computer Worms*. Paper presented at the ACM Workshop on Rapid Malcode (WORM).

Eichin, M.W. & Rochlis, J.A. (1989). *With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988*. Paper presented at the 1989 IEEE Symposium on Research in Security and Privacy.

Elder, M. C. & Kienzle, D. M. (2003). *Recent Worms: A Survey and Trends*. Paper presented at the ACM Workshop on Rapid Malcode (WORM).

Fryar, E. & Van Beveren, J. (2004). *Distribution methods and the effectiveness of malware*. Paper presented at the ASBBS 7th Annual International Conference.

Harrison, R. (2004). *The Antivirus Defence-in-Depth Guide*. Retrieved 19/7/04, from http://www.microsoft.com/technet/security/guidance/avdind_2.mspx

Jordan, T., & Taylor, P. (1998). *A Sociology of Hackers*. The Sociological Review, 46(4), 757 - 780.

McAfee. (2004). *Antivirus Software and Intrusion Prevention Solutions*. Retrieved 02/07/04, from http://www.mcafee.com

Microsoft. (2005). *Microsoft Security Glossary*. Retrieved 02/11/05, from http://www.microsoft.com/security/glossary.mspx

mIRC. (2005). mIRC Homepage. Retrieved 14/10/05, from http://www.mirc.com

Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S. & Weaver, N. (2003). *Slammer Worm Dissection: Inside the Slammer Worm*. IEEE Security and Privacy, 1(4), 33 - 39.

Moore, K. (2003). *MSN Messenger Outage Affects Millions.* Retrieved 17/10/05, from http://www.pcworld.com/news/article/0,aid,108451,00.asp

Network Associates. (2004). *Virus Information Library*. Retrieved 02/07/04, from http://vil.nai.com/vil/default.asp

OneStat.com. (2003). *Microsoft's Windows dominates the OS market on the web according to OneStat.com.* Retrieved 24/10/05, from http://www.onestat.com/html/aboutus_pressbox24.html

Strauss, A.L., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* Newbury Park, CA: Sage.

Symantec. (2004). *Symantec Security Response Glossary*. Retrieved 02/08/04, from http://securityresponse.symantec.com/avcenter/refa.html

Twycross, J. & Williamson, M.M. (2003). *Implementing and testing a virus throttle*. Paper presented at the 12th USENIX Security Symposium.

USInfo. (2003). *Microsoft Works with U.S. Law Enforcement to Catch Cyber criminals.* Retrieved 02/08/04, from http://usinfo.state.gov/xarchives/display.html?p=washfileenglish&y=2003&m=November&x=20031106153238retropc0.981167&t=usinfo/wf-latest.html

Wearden, G. (2004). *2004: A dreadful half-year for malware*. Retrieved 02/08/04, from http://news.zdnet.co.uk/0,39020330,39161677,00.htm

Webopedia. (2004). *Webopedia Glossary*. Retrieved 19/10/04, from http://www.webopedia.com

Whole Security. (2004). *Threat Centre: Cost of Worms***.** Retrieved 03/08/04, from http://www.wholesecurity.com/threat/cost_of_worms.html

Williamson, M.M. (2002). *Throttling Viruses: Restricting propagation to defeat malicious mobile code*. Paper presented at the 18th Annual Computer Security Applications Conference (ACSAC).

THE UTILIZATION OF INTERNET MARKETING BY EUROPEAN COMPANIES

João P. Couto, University of the Azores, Portugal
Flávio Borges-Tiago, University of the Azores, Portugal
Teresa Borges-Tiago, University of the Azores, Portugal
José C. Vieira, University of the Azores, Portugal

ABSTRACT

The ways that organizations exploit the Internet have been the focus of a substantial body of scientific studies. The main objective of this study is to compare practices of the major European companies. For this purpose, we attempt to determine the impact of contextual variables on the way in which companies establish. In order to achieve our objective, we examined a sample of 500 companies, based on the ranking published by the German business and economics newspaper, Handelsblatt. Taking into consideration the literature, we determine criteria to evaluate the performance of these on-line companies, based on their Internet websites.

Keywords: Internet Marketing, Marketing Strategy, Electronic Commerce, Web Site

Acknowledgements: FCT – CEEApla, Research Center for Applied Economics

INTRODUCTION

Globalization and the use of information and communication technologies are changing profoundly the way in which business is done and organizations evolve (Teo & Pian, 2003). The confluence of diverse factors over recent decades has transformed the technologies themselves. In particular, the Internet has affected the distribution channels and introduced new, sophisticated forms of commerce and marketing (Viswanathan, 2003).

As stated by Teo & Pian (2003), although 95% of the major companies now have a website, the Internet has not yet proven to be the magic solution that many organizations around the world had believed it would be when it first became available (Meall, 2002; Dubois & Vernette, 2001).

Since the advent of the so-called “dot.com” era, many authors have analyzed the boom in this type of enterprise (Mahajam, Srinivasan & Wind, 2002; Demers & Lev, 2000; Varianini & Vaturi, 2000; Tokic, 2002; Constantinides, 2002; Rohm & Milne, 2003).

Pollack (1999) suggested that the rapid adoption of this new communication vehicle and its growth potential would permit new forms of marketing. Today, however, organizations take a more balanced view of the opportunities and limitations of the Internet (Wu, 2002; Burke, 2002; Meall, 2002).

According to Sterne (1999), a company’s presence in the Internet is likely to be due to one of two reasons: (1) the perceived need to keep pace in terms of image and service provision with customers and/or competitors; (2) the consideration that the Internet is a vital tool in their sales and marketing operations.

With regard to the latter reason, we observe that Internet use has established a particularly strong position in the advertizing industry (Sheehan & Doherty, 2001; Hoffman & Novak, 1995; Briggs &

Hollis, 1997). The Internet represents a technological breakthrough, the effects of which extend from communication to interaction with customers. At the same time, its potential has not yet been fully explored (Avlonitis & Karayanni, 2003; Dubois & Vernette, 2001).

While the adoption of Internet marketing may imply a degree of adaptation of the business and requires minimal managerial experience (Engel et al., 1995; Holbrook & Hirshman, 1982), we can observe different levels of adaptation according to the type of business (Hoffman & Novak, 1996). The same can be observed with regard to new concepts and practices related to on-line commerce (Novak, Hoffman & Yung, 2000).

The importance of this fact is emphasized in many studies that examine Internet-related questions. In 1997, Alba et al. published the results of their research into different types of commerce, in which they compared the advantages and disadvantages of each alternative, in addition to their economic and social impacts. These authors highlighted the relevance of contextual factors, particularly the industry structure, the product characteristics and the level of competition, which were also identified and considered by other authors (Bakos, 1991; Benjamim & Wigand, 1995; Burke, 1996; Hoffman & Novak, 1996; Lynch & Ariely, 2000).

Hoffman & Novak (1996) and Peterson, Balasubramaniam & Bronnenber (1997) studied the Internet and stressed those characteristics which distinguish it from other marketing channels. In a similar study, Varadajam & Yadav (2002) underline the following distinctive elements: (1) a large information storage capacity that translates into a low-cost, personalized, efficient and satisfactory response to customer enquiries and requests; (2) the possibility of purchasing or selling by means of a cheap computerized process; (3) the creation of a multimedia experience; (4) a medium for digital product transactions; and (5) the low-cost acquisition of a full-time, 24/7 global presence.

A critical factor in the Internet's popularity as a marketing tool is the low cost associated with the development of an on-line presence (Kling, 1994; Cronin, 1996; Boyle & Alwitt, 1999). The benefits of the Internet have also been studied by other authors, such as Hanson, 2000; Turban et al., 2002; Turban et al., 2004; and Chaffey, 2004.

Among the more unfavorable aspects of Internet marketing, attention focuses on the difficulty in establishing a trustful relationship between seller and potential customer, due to the need to confirm identity and for clear transmission of messages to the consumer. The possibility of fraud (Neuman, 1991), the excess of information and the lack of personal contact are potential threats inherent in transactions, due to deceptive publicity, bad debt or the non-delivery of the purchased goods (Withmore, 1999).

LITERATURE REVIEW

In order to have a better understanding of the Internet marketing environment, we carried out a comprehensive review of the principal themes present in the literature (Kimiloğlu, 2004; Wagonfeld & Deighton, 2002; Hou & Rego, 2002; Dubois & Vernette, 2001; Ngai, 2003; Barwise, Elberse & Hammond, 2000). Taking these works as reference, we can define the concept of Internet marketing (IM) as the process of creating and maintaining a mutually satisfactory relationship between sellers and clients through on-line activities that facilitate the exchange of ideas, products and services (Imber & Toffler, 2000).

The growing interest in the Internet and in particular its marketing component, can be divided into five different categories in terms of corporate presence in the Web: commerce/distribution, promotional, diverse contents, institutional communication and information gathering (Hseih & Lin, 1998).

Quelch & Klein (1996), on analyzing the posture assumed by on-line companies, concluded that the way in which the Internet is utilized depends strongly on their previous activity. These authors suggest there are in existence two distinct models of operation: the first, developed by multinational corporations that use the Internet as a communication and information vehicle; the second, adopted by start-ups, which are more directly interested in exploiting the Internet's potential to the full. This latter group assumes, from the outset, a posture that is more accentuated to on-line transactions.

Considering this approach, in addition to the type of website and its target market, Cox & Koelzer (2004) propose the following classification of the websites: institutional sites; product and service information sites, transaction sites and customer relations marketing sites (CRM or e-CRM*)*.

One of the first proposals of website classification was presented in 1995 by Hoffman, Novak & Chatterjee and was based on commercial performance. In these authors' view, the site could be considered as one (or more) of the following: a on-line shop window; a web-presence; contents/information; a shopping center; a search engine; an incentive site. Further to this view, Ho (1997) presented a 3-category classification according to the purposes and business goals of the enterprises concerned: (1) product and service promotion; (2) data and information gathering; and (3) electronic transaction processing.

According to Strauss et al. (2003), a fundamental element in defining the strategic model to adopt for Internet marketing and e-business in general resides in determining the company's initial level of commitment. Thus, a company can start by simply developing an Internet brochure and later expand its commitment to a virtual store, or even concentrate all of its activity on the Internet.

Another aspect that has evolved is Web design. Initially, the contents were static with a few hyperlinks between elements, then evolving into dynamic multimedia, integrated with databases (Palmer & Griffith, 1998).

Two strategies can be found in website development according to the level of commitment: a communication strategy, focused on maximum information provision; and a transaction strategy, focused on online shopping, with budget simulations and information on availability and tracking of orders (Strauss et al., 2003; Palmer & Griffith, 1998). Lee, Katerattanakul & Hong (2005) suggest an additional strategy of entertainment. All design features should supporte an overall strategy (Chakraborty, Lala & Warren, 2002).

In the Internet's early years, the economic impact of web design was little known (Baty & Lee, 1995; Ridgon, 1996; Chatterjee, Hoffman & Novak, 2003), but more recently, its importance has attracted much attention from researchers in relation to: consumer behavior (Jarvenpaa & Todd, 1997; Eighmey, 1997; Chen & Wells, 1999); site traffic volume (Goodwin & Marquis, 2000; Lohse & Spiller, 1998; Drezè & Zufryden, 2004); the buying process (Liang & Lai, 2002); consumer loyalty (Koufaris, Kambil & LaBarbera, 2001); the level of interaction (Ghose & Dou, 1998; Olson & Widing, 2002); the personalization of contacts (Ansari, Essegaier & Kohli, 2000; Iacobucci, Arabie & Bodapati, 2000);

sales volume (Lohse & Spiller, 1998); security and privacy (Milne & Boza, 1999; Phelps, D'Souza & Nowak, 2001; Yoon, 2002); and the site background (Stevenson, Bruner & Kumar, 2000).

It is understandable that the importance of web design implies the need for permanent feedback, follow-up and updating processes, even if alterations to the site are only minimal. Companies will be anxious to inform their clients and the market quickly and efficiently of any changes, given how vital it is that the on-line 'store' remains both open and accessible. Corporate image is another factor to consider in relation to both the design and accessibility of the website.

HYPOTHESES

Considering the models proposed by Ainscough & Luckett (1996) and Cox & Koelzer (2004), which point to different ways of exploiting the potential of Internet marketing, reflected in the degrees of sophistication of the on-line applications, we define the following hypothesis.

A first aspect considered is the fact, mentioned in the literature, that sales initiatives tend to be more successful in the case of tangible goods, due to the possibility that consumers seek above all an homogeneous supply, with less risk attached to the buyer (Quelch & Klein, 1996; Alba et al., 1997; Poon & Joseph, 2001; Kimiloğlu, 2004). Selling services consitutes a greater challenge and thus, we consider that Internet marketing of services will tend to be more sophisticated.

Hypothesis 1: Internet marketing will be more developed in service industries.

A second aspect considers the idea of Bodkin & Perry (2004) that companies with higher sales volumes have a greater incentive to employ Internet marketing, providing financial information to stock holders or product and service information to consumers, have more resources to develop their strategies and can take better advantadge of emerging technologies (Li et al., 1999; Liu et al., 1997; Liu & Arnett, 2002).

Hypothesis 2: Internet marketing will be more developed in larger companies.

A third aspect relates to the company's national environment, namely, country-specific characteristics and infrastructure, in addition to inter-firm competition or cooperation that affects the diffusion of new technologies (Adam et al., 2002). Furthermore, cultural aspects may be relevant in terms of the behavior of firms and consumers (Hofstede, 1991; Grover et al., 1994; Aiex, 1995; Nath et al., 1998), which are manifested for example in the symbols and in the means of communication commonly used. In this paper we analyse the internet marketing development considering only internet usage in the country as a measure of technology diffusion.

Hypothesis 3: Internet marketing will be more developed in countries with more Internet usage.

METHODOLOGY AND RESULTS

The data used in this study was gathered from the websites of the 500 largest companies in Europe, according to the ranking list published by the German business and economics newspaper, Handelsblatt. This procedure is similar to the one adopted in other studies concentrating on the USA and Canada, that use Fortune 500 listtings, which therefore permits us to have some means of comparison to other works (See the sample data presented in the Appendix).

The base variable of our analysis is the level of sophistication of the websites according to a four-model classification of sales, service, communication and information, as shown in Figure 1 in the appendix. This procedure follows the methodologies of Young & Benamati (2000) and Houghton & Winklhofer (2004). These authors established a framework of classification that has been used in previous studies (see: Berthon, et al. 1996; Gow 1997; Griffith & Krampf, 1998; Gardner, 1998; Weston, 1999).

These variables were classified in an ordinal scale according to the existence or non-existence of the required element, ranging from 0 if none of the characteristics were present, to 5 if there was evidence of all of the characteristics. The sites were denominated as follows: interactive brochure; virtual storefront; information clearing house; and customer service tool (Ainscough & Luckett, 1996; Cox & Koelzer, 2004).

In order to verify the influence of organizational elements on the level of sophistication of the websites, we used as variables the sales volume and number of workers and the stock market capitalization.

A second group of variables is the industry type, since we considered that the activity of the firm would be relevant to the Internet usage, namely, product rather that service companies, or final consumers versus industrial goods company. We grouped the companies in main industry classifications.

Based on the literature, we also considered the country of origin as an element that influences the firm's Internet utilization. For this purpose, we considered as variables the number of hosts and Internet users.

In order to test this hypothesis, we used the classifications of the websites, ranging from 0 to 5 in the four major categories of the model and determined the overall level of sales, service communication and information of the sites, then employed this cluster analysis to group the companies. Consequently, we obtained three clusters, as shown in Table 1.

Table 1 – Cluster Analysis

		Clusters	
	1	2	3
	(n=122)	(n=129)	(n=249)
Level of Sales	0,98	4,29	1,18
Level of Service	0,97	3,04	1,62
Level of Communication	1,65	3,39	2,94
Level of Information	2,56	3,69	4,06

Scale: 0-5 (Max 5)

In relation to the clusters, we verify that Cluster 1 is characterized by high levels of information, Cluster 2, is related to sales and services and Cluster 3 as high levels of information and communication. According to these results we denominated the cluster as following: cluster 1, "Interactive Brochure"; cluster 2, "Virtual Storefront" and cluster 3, "Information Clearing House". The results of the ANOVA reveal that all variables are statistically significant in determining the clusters.

Table 2 – Cluster Analysis - ANOVA

	Cluster		Error		F	Sig.
	Mean Square	Df	Mean Square	df		
Level of Sales	483,00	2	0,36	497	1357,64	0,00
Level of Service	145,22	2	0,85	497	170,45	0,00
Level of Communication	104,82	2	0,80	497	130,71	0,00
Level of Information	93,67	2	0,69	497	136,65	0,00

The majority of elements from the banking and financial services sector are in Cluster 2. There is a tendency of agglomeration of the elements from the chemical and pharmaceutical industries as well as engineering and electronics in Cluster 3. The tourism companies appear in Cluster 2 and the petroleum, energy, construction and real estate industries are most strongly represented in Cluster 1.

Once we had established the classification of the companies by means of the cluster analysis, we tested hypotheses 1 and 3 using one-way ANOVA and the Duncan test to verify the existence of differences in the groups' averages regarding sales volume, number of workers, stock market capitalization and number of hosts per-inhabitant.

Table 3 – One-way ANOVA Analysis

			1	2	3	
	F	Sig.	(n=122)	(n=129)	(n=249)	Dif.m.
Sales Volume	10,35	0,00	7.304	17.461	13.939	1<3,2
Number of Workers	5,28	0,01	34.376	55.440	56.660	1<2,3
Stock Market Capital	7,30	0,00	4.826	12.435	9.075	1<3,2
Number of Hosts by Inhabitant	3,91	0,02	359	373	391	1<2,3

The results show that there is pattern in which the first cluster has a lower average than the second and third clusters in all four variables. This suggests that companies in these clusters are larger and are from countries with more Internet infrastructure.

We also performed a discriminatory analysis in order to verify the classification capability of these variables. The results are shown below in Table 4, in which it can be observed that two functions were extracted.

Table 4 – Discriminatory Function

Function	Coefficients	Variance %	Acumulative %	Cannonical Correlations
1	0,05	73,50%	73,50%	0,22
2	0,02	26,50%	100,00%	0,13

Table 5 - Lambda of Wilks Analysis

Functions Test	Lambda of Wilks	Chi-Square	df	Sig.
1 a 2	0,94	32,72	8	0,00
2	0,98	8,77	3	0,03

The first function explains 73.5% of the total variance, while the second function explains 26.5% and the Wilks test confirms both functions as significant. The correlations of the variables with the two functions are presented in Table 6. The first function relates to the dimension variables and the second the countries' Internet infrastructure measured by the number of hosts by inhabitant.

Table 6 – Structure Matrix

	Functions	
	1	2
Sales Volume	0,89 *	-0,32

Stock Market Capitalization	0,72 *	-0,43
Number of Workers	0,63 *	0,27
Number of Hosts by Inhabitant	0,36	0,65 *

* Larger absolute correlation

In order to test hypothesis 3, and because the industry is a qualitative variable, we used the chi-square to test for differences in cluster membership due to industry classifications. The results are shown in Tables 7 and 8. In Table 7 we divided the industry classification in terms of sophistication according to the model and the scoring criteria and in Table 8, we tested for significant differences between sophistication levels by industry. The results show significant differences, with the exception of tourism.

Table 7 – Comparison of Sophistication Scores by Industry

Industries	Percentage of Companies		
Sophistication Levels	0 to 7	8 to 14	15 to 20
Automobile and Aerospace	27	45	27
Chemical and Pharmaceutical	14	79	7
Banking and Financial Services	14	73	14
Tools and Utilities	19	69	13
Constructions	30	65	5
Petroleum and Energy	38	56	5
Engineering and Electronics	9	74	16
Retail and Logistics	25	65	11
Tourism	22	56	22
Others	32	65	3

Table 8 – Chi-Square Test Results - Industry/Sophistication

Industry	Chi-Square	P-value /Sig.	S/NS
Automobile and Aerospace	58,03	0,00	S
Chemical and Pharmaceutical	62,31	0,00	S
Banking and Financial Services	167,15	0,00	S
Tools and Utilities	52,74	0,00	S
Constructions	78,97	0,00	S
Petroleum and Energy	45,30	0,01	S
Engineering and Electronics	108,20	0,00	S
Retail and Logistics	128,65	0,00	S
Tourism	15,38	0,12	N
Others	43,83	0,00	S

Significance Level: S = 5% e NS = Non significant

DISCUSSION AND CONCLUSIONS

Considering these results, we can find evidence to confirm the hypotheses that we formulated that website sophistication will be greater in larger firms and in companies from countries with more developed Internet infrastructure and that Internet marketing will vary according to industry.

These results are in accordance with the literature that considers the influence of contextual variables in the adoption of Internet marketing. They also point to a pattern of differences in sophistication depending on the industry.

In relation to the more visible aspect of Internet marketing, namely the on-line sales, we observed that this activity is more in evidence in the tourism industry. This finding is according to theory, but the same was not observed regarding the retail and logistics industries, in which the level of activity is also commonly considered to be high.

These results imply that the Internet marketing activities pursued by companies should be defined by taking into account the specific contextual factors. The level of Internet usage in the country, we have measured in this study by the number of hosts per- inhabitant, is another aspect to consider. Companies should not simply emulate practices of companies from other countries without first analyzing the differences that might exist in terms of the local environment.

The same is true when companies consider the Internet marketing configuration that they will adopt with regard to the sales volume that might be achieved through this channel or the type of relations that can be fostered with agents or suppliers. The sophistication of Internet marketing has proven to be associated with larger companies that can invest with a certain return profit.

The level of sophistication of the websites of companies in the extraction and transformation industries is clearly different from the other industries analyzed, demonstrating evidence of the fact that companies which have a B2C strategy/ are very different from the companies involved in B2B activities.

To managers, these results suggest that they should take an active posture regarding the decision as to what type of website they should build. There should be an adaptation of Internet marketing adoption according to industry and dimension.

The limitations of this study are due to the fact that only some aspects of website design are addressed while the levels of quality, user-friendliness and appeal of the website are not considered. Further research should include these aspects, in addition to expanding the sample to include small and medium enterprises.

REFERENCES

Adam, S., Mulye, R., Deans, K. and Palihawadana, D. 2002. E-marketing in perspective: a three country comparison of business use of the Internet, *Marketing Intelligence & Planning*, 20 (4), 243-251.

Aiex, N. 1995. *Communication within organisational cultures*, (www document) http://www.indiana.edu/eric_rec/ieo/digests/d30.html.

Ainscough, T. and Luckett, M. 1996. The Internet for the rest of us: marketing on the World Wide Web, *Journal of Consumer Marketing*, 13 (2), 36-47.

Alba, J., Lynch, J., Weitz, B., Janiszewski, C., Lutz, R., Sawyer, A. and Wood, S. 1997. Interactive home shopping: consumer, retailer, and manufacturer incentives to participate in electronic marketplaces, *Journal of Marketing*, 61, 38-53.

Ansari, A., Essegaier, S. and Kohli, R. 2000. Internet recommendation systems*, Journal of Marketing Research*, 37 (August), 363–375.

Avlonitis, G. and Karayanni, D. 2003. The use of Internet in business to business marketing: some evidence from american and european companies, *Working Progress Paper*, Athens University of Economics and Business.

Bakos, J. 1991. A strategic analysis of electronic marketplaces, *MIS Quarterly*, 15, 295-310.

Barwise, P., Elberse, A., e Hammond, K. 2002. *Marketing and the Internet: A Research Review*. In B. Weitz & R. Wensley (Eds.), Handbook of Marketing, Thousand Oaks, CA: Sage.

Baty, J. and Lee, R. 1995. Intershop: Enhancing the vendor/customer dialectic in electronic shopping, *Journal of Management Information Systems*, 11(4), 9-31.

Benjamin, R. and Wigand, R. 1995. Electronic markets and virtual value chains on the information superhighway, *Sloan Management Review*, 36 (winter), 62-72.

Berthon, P., Pitt, L. and Watson, R. 1996. The World Wide Web as an advertising *medium, Journal of Advertising Research, 36(1), 43-55.*

Bodkin, C. and *Perry, M. 2004. Goods retailers and service providers: Comparative analysis of web site marketing communications, Journal of Retailing and Consumer Services, 11(1), 19-29.*

Boyle, B. and Alwitt, L. 1999. Internet use within the U.S. plastics industry, *Industrial Marketing Management*, 28, 327-341.

Briggs, R. and Hollis, N. 1997. Advertising on the Web: is there response before-through, *Journal of Advertising Research*, 37 (2), 33-45.

Burke, R. 1996. Virtual shopping: breakthrough in marketing research, *Harvard Business Review*, (March-April), 120-131.

Burke, R. 2002. Technology and the customer interface: what consumers want in the physical and virtual store, *Journal of the Academy of Marketing Science*, 30 (4), 411-432.

Chaffey, D. 2004. E-*Business and E-Commerce Management*, Second Edition, London: Prentice Hall.

Chakraborty, G., Lala, V. and Warren, D. 2002. An empirical investigation of antecedents of B2B websites' effectiveness, *Journal of Interactive Marketing*, 16 (4), 51-72.

Chatterjee, P., Hoffman, D. and Novak, T. 2003. Modeling the clickstream: implications for Web-Based advertising efforts, *Marketing Science*, 22 (4), 520-541.

Chen, Q. and Wells, W. 1999. Attitude toward the site, *Journal of Advertising Research*, 39 (5), 27–37.

Constantinides, E. 2002. From physical marketing to web marketing: the web-marketing mix, *In proceedings* of the 35th Anual Hawaii International Conference on System Sciences.

Cox, B. and Koelzer, W. 2004. *Internet Marketing*, Pearson Education Ltd: London.

Cronin, M. 1996. *The Internet strategy handbook: lessons from the new frontier of business*, Harvard Business School Press: Boston.

Demers, E. and Lev, B. 2000. A rude awakening: Internet shakeout in 2000, *In* proceedings EFA 0660, EFMA 2000 Athens Meetings, Simon Business School Working Paper No. FR 00-13.

Dreze, X. and Zufryden, F. 2004. Measurement of online visibility and its impact on Internet traffic, *Journal of Interactive Marketing,*18 (1), 20.

Dubois, P.-L. and Vernette, E. 2001. Contribution et pistes pour la recherche en e-marketing, *Recherche et Applications en Marketing*, 16 (3), 1-8.

Eighmey, J. 1997. Profiling user responses to commercial Websites, *Journal of Advertising Research*, 37(3), 59-66.

Engel, J., Blackwell, R. and Miniard, P. 1995. *Consumer Behaviour*, 8 Ed., Dryen Press.

Gardner, E. 1998. More work - more money, *Internet World*, October 5.

Ghose, S. and Dou, W. 1998. Interactive Functions and their impacts on the appeal of Internet presence sites*, Journal of Advertising Research*, 38(2), 29–43.

Goodwin, U. and Marquis, G. 2000. Effective web site design: an empirical study, *In proceedings* IEEE International Engineering Management Conference, Albuquerque, NM.

Gow, K. 1997. Risk versus opportunity, *Computerworld*, October 5.

Griffith, D. and Krampf, R. 1998. An examination of the Web-based strategies of the top 100 US retailers, *Journal of Marketing Theory and Practice*, 6 (3), 12-23.

Grover, V., Segars, A. and Durand, D. 1994. Organisational practise, information resource deployment and systems success: a cross-cultural survey, *Journal of Strategic Information Systems*, 3 (2), 85-105.

Hanson, W. 2000. *Principles of Internet Marketing*, Cincinnati, Ohio: South-Western College Publishing.

Ho, J.1997. Evaluation the World Wide Web: a global study of commercial sites, *Journal of computer mediated communication*, 3 (1), July.

Hoffman, D. and Novak, T. 1995. Marketing in hypermedia computer- mediated environments: conceptual foundations, (www document) http: //www2000.ogsm.vanderbilt. edu/cmepaper.revision.july11.1995/cmepaper.html (accessed 11 July 2004).

Hoffman, D. and Novak, T. 1996. Marketing in hypermedia computer-mediated environments: conceptual foundations, *Journal of Marketing*, 60, 50-68.

Hoffman, D., Novak, T. and Chatterjee, P. 1995. Commercial scenarios for the web: opportunities and challenges, *Journal of Computer Mediated Communication*, Special Issue on Electronic Commerce, 1(3).

Hofstede, G. 1991. *Cultures and organizations: Software of the mind*. London: McGraw-Hill.

Holbrook M. and Hirshman E. 1982. The experimential aspects of consumption: consumer fantasies, feelings and fun, *Journal of Consumer Research*, 9 (2), 132-140.

Hou, J. and C. Rego 2002. Internet marketing: An overview, *Working paper*. University of Mississippi, Mississippi, EUA.

Houghton, K. and Winklhofer, H.2004.The effect of website and e-commerce adoption on the relationship between SMEs and their export intermediaries, *International Small Business Journal*, 22 (4), 369-385

Hsieh, C. and Lin, B. 1998. Internet commerce for small businesses, *Industrial Management and Data Systems*, 3, 113-119.

Iacobucci, D., Arabie, P. and Bodapati, A. 2000. Recommendation agents on the Internet, *Journal of Interactive Marketing*, 14 (3), 2-11.

Imber, J. and Toffler, B. 2000. *Dictionary of Marketing Terms*, 3rd ed., Barrons Business Dictionaries, Hauppauge, NY.

Jarvenpaa, S. and Todd, P. 1997. Consumer reactions to electronic shopping on the World Wide Web, *Journal of Electronic Commerce*, 1 (2),59-88.

Kimiloğlu, H. 2004. The e-literature: a framework for understanding the accumulated knowledge about Internet marketing, *Academy of Marketing Science Review*, 6.

Kling, R. 1994. Reading 'all about' computerization: how genre conventions shape social analyses, *The Information Society*, 10, 147-172.

Koufaris, M., Kambil, A. and LaBarbera, P. 2001. Consumer behavior in web based commerce: an empirical study, *International Journal of Electronic Commerce*, Winter 2001.

Lee, S., Katerattanakul, P. and Hong, S. 2005. Framework for user perception of effective e-tail web sites, *Journal of Electronic Commerce in Organizations*, 3 (1),13-34.

Li, H., Kuo, C. and Russell, M. 1999. The impact of perceived channel utilities, shopping orientations, and demographics on the consumer’s online buying behaviour, *Journal of Computer-Mediated Communication*, 5 (2).

Liang, T-P. and Lai, H-J. 2002. Effect of store design on consumer purchases: Van empirical study of on-line bookstores, *Information and Management*, 39 (6), 431-444.

Liu, C., Arnett, K., Capella, L. and Beatty, R. 1997. Web sites of Fortune 500 companies: facing consumers through home pages, *Information and Management*, 31, 335-45.

Lohse, G. and Spiller, P. 1998. Electronic shopping: The effect of customer interfaces on traffic and sales, Communications of the ACM, 41(7), 81-87.

Lynch, J. and Ariely, D. 2000. Wine online: search costs affect competition on price, quality, and distribution, *Marketing Science*, 19 (Winter) (1), 83-103.

Mahajan, V., Srinivasan, R. and Wind, J. 2002. The Dot.com retail failures of 2000: were there any winners?, Journal of the Academy of Marketing Science, 30 (4), 474-486.

McLeod, R. and Rogers, J. 1982. Marketing information systems: uses in the Fortune 500, *California Management Review*, Fall, 25.

Meall, L. 2002. Business: SME’s and e-commerce-bubbles, bullets, and business. *Accountancy*, 130 (1311), November, 1.

Milne, G. and Boza, M. 1999. Trust and concern in consumers' perceptions of marketing, information management practices, *Journal of Interactive Marketing*, 13(1), 5–24.

Nath, R., Akmanligil, M., Hjelm, K., Sakaguchi, T. and Schultz, M. (1998). Electronic commerce and the Internet: issues, problems and perspectives, *International Journal of Information Management*, 18 (2), 91-101.

Neuman, R. 1991. *The future of the mass audience*. Cambridge, MA: Cambridge University Press.

Ngai, 2003. Internet marketing research (1987-2000): a literature review and classification, *European Journal of Marketing*, 37 (1/2), 24-49.

Novak, T. , Hoffman, D. and Yung, Y.-F. 2000. Measuring the customer experience in online environments: a structural modelling approach. *Marketing Science*, 19 (Winter)(1), 22-42.

Olson, E. and Widing, R. 2002. Are interactive decision aids better than passive decision aids? A comparison with implications for information providers on the Internet, *Journal of Interactive Marketing*, 16(2), 22–33.

Palmer, J. and Griffith, D. 1998. An emerging model of Web site design for marketing, *Communications of the ACM*, 44(3), 44-51.

Peterson, R., Balasubramanian, S. and Bronnenberg, B. 1997. Exploring the implication of the Internet for consumer marketing, *Academy of Marketing Science Journal*, Greenvale: Fall 2002, 30 (4), 348.

Phelps, J., D'Souza, G. and Nowak, G. 2001. Antecedents and consequences of consumer privacy concerns: an empirical investigation, *Journal of Interactive Marketing*, 15(4), 2–17.

Pollack, B. 1999. The state of Internet marketing, *Direct Marketing*, 61(9), January, 18.

Poon, S. and Joseph, M. 2001. A preliminary study of product nature and electronic commerce, Marketing Intelligence Research, 19 (7), 493-500.

Porter, M. 2001. Strategy and Internet, *Harvard Business Review*, March, 62-78.

Quelch, J. and Klein, L. 1996. The Internet and international marketing, *Sloan Management Review*, 38 (Spring), 60-75.

Ridgon, J. 1996. Caught in the Web, *Wall Street Journal*, July, R14.

Rohm, A. and Milne, G. 2003. Investigating Internet channel opportunities and challenges: managers' experiences across five industries, *Journal of Managerial Issues*, 15(4), 467-485.

Sheehan, K. and Doherty, C. 2001. Re-weaving the Web: integrating print and online communications, *Journal of Interactive Marketing*, 15 (2), 47.

Sterne, J. 1999. *World Wide Web Marketing*, John Wiley & Sons: New York.

Stevenson, J., Bruner, G. and Kumar, A. 2000. Webpage background and viewer attitudes, *Journal of Advertising Research*, 40 (1), 29–34.

Strauss, J., El-Ansary, A. and Frost, R. 2003. *E-Marketing*, 3rd edition, Prentice Hall: New York.

Teo, T. and Piam, Y. 2004. A model for web adoption, *Information and Management*, 41, 457-468.

Thompson, T. and Pian, Y. 2003. A contingency perspective of Internet adoption and competitive advantage, *European Journal of Information Systems*.

Tokic, D. 2002. What went wrong with the dot.coms, *The Journal of Investing*, 11(2), 52-56.

Turban, E., King, D., Lee, J. and Viehland, D. 2004*. Electronic Commerce a managerial Perspective*, Prentice Hall: New Jersey.

Turban, E., Lee, J., King, D. and Chung, H. 2002. *Electronic Commerce a Managerial Perspective*, Prentice Hall International Inc.: New Jersey.

Varadarajan, P. and Yadav, M. 2002. Marketing strategy and the Internet: an organizing framework, *Journal of the Academy of Marketing Science*, 30 (4), 296-312.

Varianini, V. and Vaturi, D. 2000. Marketing lessons from e-failures, *McKinsey Quarterly*, 4, 86-97.

Viswanathan, S. 2003. DotComs versus NotComs: Competing on Channel-Centric Value Propositions, *Working Paper*.

Wagonfeld, A. and Deigthon, J. 2002. Note on Marketing and Internet, *Harvard Business Review*, 1-16

Weston, R. 1999. Behind the numbers: who's minding the e-business store?, *Information Week On-Line*, 6/7.

Withmore, S. 1999. How not to get ripped-off while shopping, *Asiaweek*, 25 (11), 51.

Wu, S. 2002. Internet marketing involvement and consumer behavior, *Asia Pacific Journal of Marketing and Logistics*, 14 (4), 36-53.

Yoon, S. 2002. The antecedents and consequences of trust in online-purchase decisions, *Journal of Interactive Marketing*, 16(2), 47–63.

Young, D. and Benamati, J. 2000. Differences in public web sites: the current state of large U.S. firms, *Journal of Electronic Commerce Research*, 1 (3), 94-105.

Appendix

Figure a1 – Classification Model

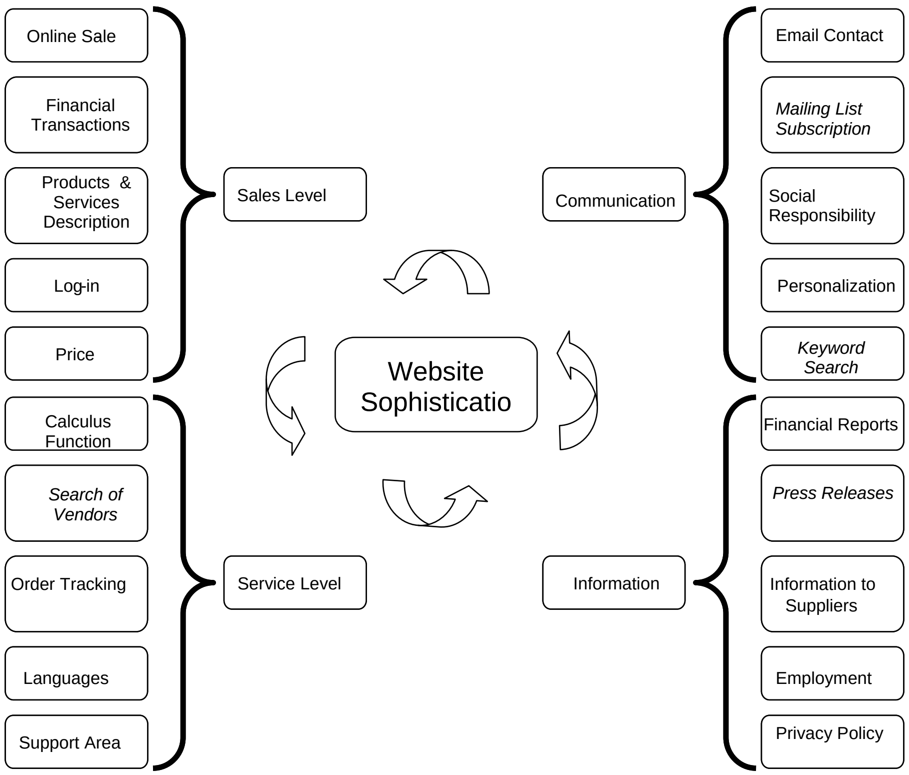


Table a1 – Companies Distribution Accordin to On-Line Sales

Industry	Number of Companies	Percentage (%)	Industry	Number of Companies	Percentage (%)
Automobilie and Aerospace	33	6,6	Petroleum and Energy	39	7,8
Chemical and Pharmaceutical	43	8,6	Electroniccs and Engeneering	74	14,8
Banking and finantial Services	111	22,2	Retail and Logistics	85	17
Utililities	32	6,4	Tourism	9	1,8
Constrution and Real State	43	8,6	Others	31	6,2

Table a2 – Comparion os Results between Europe and the EUA

Characteristics	Results Europa	Results EUA	Characteristics	Results Europa	Results EUA
Finantial Transactions	19	34,7	Social Responsability	46	2,9
Log-in	32	29,4	Products and Services Description	94	97,3
Search of Vendors	73	47,6	Finantial Reports	93	95,1
Calculus Function	15	14,7	Press releases	89	89
Order Tranking	10	4,3	Job Opportunities	67	88,4
Envio de emails	98	92	Keyword search	73	59,4
Mailing lists Sbscription	38	23,3	Secuirty Policy	88	52,7
Personalization	18	6,3	Information to Suppliers	20	34,1

A MODEL ON CONSUMER BEHAVIOR AND THE DEMAND FOR SECURED DIGITAL CONTENT

Marc Fetscherin, Rollins College, USA.

NEED FOR A MODEL

Most research dealing with digital content and piracy has focused on software rather than on music piracy (Sims/Cheng/Teegen (1996); Chen/Png (1999); Andres (2002); Chiang (2003); Katz (2003)). Those focusing on music have either looked at the implications of piracy for welfare or for the content industry (IFPI (2002); Papadopoulos (2003)), as well as the strategies that should be followed to fight piracy (Buhse (2001); Bhattacharjee et al. (2002)). The few papers known so far lack a model for the consumer's trade-off between purchasing and pirating content. None of them so far has looked at the implications of security technologies, such as Digital Rights Management Systems (DRMS), on the demand for digital content (Wijk (2002); Chiang (2003); Holm (2003)). The purpose of this paper is to fill that gap by presenting a mathematical model.

ASSUMPTIONS

The model should be as simple as possible in order to ensure its application, but sufficiently comprehensive for accurate modeling and prediction of consumer behavior and the demand for digital content. We distinguish three options for the consumers: Purchase of the original, use of an (illegal) copy, and no consumption at all. We assume that the original and the copy are initially perceived by consumers as substitutes with respect to their quality. This assumption enables us to keep our model linear, and hence simple. We present a model from the point of view of a single consumer and, later in this article, an aggregate model showing customers' demand for originals and copies. We also assume that the model is static in that we model the consumer's trade-off in one period of time by disregarding such dynamic aspects as the experience of downloading or copying over time and change in income, which are also aspects that should be studied further.

Other assumptions underlying the model are: Digital content has been developed and there are individuals who want to consume it. Each individual wants either zero or one unit of the content or does not want to consume the content. This decision is taken by consumers independently (Fetscherin (2003). Moreover, all consumers behave rationally and have similar preferences and they make their decision on the basis of their preferences. They always choose the product with the highest utility. We also assume that there is only one price for all downloads, as is the case with i-Tunes, and that there is no price discrimination among products and consumers. There are also no changes affecting the price of the legal download, such as taxes or subsidies. Finally, we omit risk factors that do not have a direct effect on the valuation of the product, such as a world crisis and demographic change.

BASIC MODEL

We define x_1 and x_2 as the number of purchases and the number of copies consumed, respectively. The parameter $i \in I$ where I represents the total number of consumers. Each consumer i has a budget constraint m_i that s/he is willing to spend on music, whether x_1, x_2, or a combination of the two. The consumer pays a price p_1 when purchasing music or p_2 when copying. The price p_1 is fixed by the music provider and is assumed to be fixed for all consumers and downloads. The price for the copy p_2 tends to be 0, $lim\ p_2 \rightarrow 0$, as the copy can be acquired for free in the digital age.

However, other costs are associated with the acquisition of digital music, such as access, search, and storage costs. Access costs, such as telecommunication or Internet access costs paid to telecom companies or Internet Service Providers (ISP), and storage costs, such as hard disk space, are assumed to be identical for both types of acquisition. The reasoning is that in both cases the consumer has to have access to the Internet and needs a combination of hardware and software to store and play music, regardless of whether s/he has copied or purchased it. Therefore, these costs can be omitted from further analyses. For simplicity we assume that the search costs, which are the monetary expression of the time and effort needed to search for music, are also identical for both types of acquisition modes and can therefore also be omitted in the model. We put v_{x1} as the utility or the value consumer i associates with the product x_1 which s/he is willing to pay for, and the same applies for v_{x2}. The effective utility or net benefit results from the difference between v_{xi} on one side and p_i on the other side, so that for the original x_1 it would be $v_{x1} - p_1$ and for the copy x_2 it would be $v_{x2} - p_2$.

The budget of consumer i is m_i, which is the amount of money spent by consumer i on the two products and can be no more than the total amount the consumer has to spend. Our model does not take into account any changes in income or in the customer's constraint budget. Therefore it can be expressed as:

$$m_i = p_1x_1 + p_2x_2$$

In this case, p_1x_1 is the amount of money the consumer is spending on purchasing and p_2x_2 is the amount of money s/he is spending on copying. The indifference curve or utility function for the two products can be expressed as:

$$U(x_1, x_2) = v_{x1}\, x_1 + v_{x2}\, x_2$$

In this context, when the consumer wants to purchase the content, s/he pays p_1. If we assume that $v_{x1}, p_1 \geq 0$, the net benefit of purchasing can be presented as follows:

$$Net\ benefit_1 = v_{x1} - p_1$$

If the products are substitutes ($v_{x1} = v_{x2}$), and if $v_{x2}, p_2 \geq 0$ the net benefit of copying will be:

$$Net\ benefit_2 = v_{x2} - p_2$$

As $p_2 \rightarrow 0$, taking into account that the products are substitutes ($v_{x1} = v_{x2}$), we obtain

$$v_{x2} > v_{x1} - p_1$$

meaning that the consumer would prefer the copy over the original. If this were the case, such companies as i-Tunes would not have generated any sales and could have closed down their businesses. There must be other factors involved in making consumers purchase music instead of copying it. What follows is an extension of the basic model by further parameters.

ECONOMICAL FACTORS

So far we have assumed that the copy and the original are substitutes with respect to quality. However, empirical data has shown that not all consumers perceive the quality of the copy as equal to the quality of the original. The differences in quality perception can have different reasons. On the one hand there are specialized companies (e.g., Overpeer) flooding, for example, P2P networks with fake, corrupt, or “spoof” files which contain little or no music in order to frustrate people's attempts of copying from such networks. On the other hand, copying from these networks also exposes consumers to the risk of getting viruses, which can either make the downloaded file unplayable or even damage the computer. In the case of music other reasons why a copy may not be as good as the original are the lack of other information (metadata) and poor file compression. All these factors have an impact on the quality perception by consumers. We express this possible quality degradation in our model by the parameter $q \in [0 : 1]$, which captures the quality degradation between the original and the copy. When $q = 0$, this indicates that there is a zero probability of deterioration in quality and hence the copy is perceived as a perfect substitute for the original. Higher values of q express a greater perceived difference in quality. The perceived value or utility of the copy can be expressed as the utility of the original (v_{x1}) multiplied by the factor (1 - q). Thus, the new utility function is

$U(x_{1,} x_2) = v_{x1} x_1 + v_{x1}(1 - q) x_2$

RISK FACTORS

DRMS make it possible to detect and track copyrighted content more easily, thanks to watermarking and fingerprinting technologies. Those systems therefore allow better identification of users who are copying and hence make it possible to prosecute them for copyright violations. We assume in our model that there is a certain probability u of being caught, depending on the law enforcement in the country where the violation takes place. Furthermore, we assume that when DRMS are used, this will also increase the probability of being caught, owing to watermarking or fingerprinting. This increase of the probability is expressed in our model with the parameter m. We assume that both parameters u and m are $\in [0 : 1]$.

When $u = 0$ there is no law enforcement in place in the country regarded, and we argue that no matter how robust DRMS are, even if $m = 1$ the overall probability of being caught would be equal to zero as the law is not enforced despite the detection of violations. On the other hand, when $u = 1$, even though there might be no DRMS in place, anybody violating the law by copying will be detected. Hence there would be a 100% probability of being caught because of the very strong law enforcement in the country concerned. Finally, if both values were equal to 0 the overall probability would also be 0, and if both values were 1 the overall probability would be 100%. Hence, when we respect the aforementioned rules we can express the following overall probability of being caught as $u^{(1-um)}$. Let z represent the overall monetary value, giving $z = u^{(1-um)} f$. As $p_2 \rightarrow 0$, we get the following new budget line:

$m_i = p_1 x_1 + z$

TECHNOLOGY FACTORS

When such DRMS are used, they also restrict consumers with the usage of the legal download. Either through specific technological requirements such as encryption or the requirement for specific software and hardware or through usability restrictions such as restrictions on playability. Those restrictions reduce the utility of the legally purchased download $v_{x1.}$ As DRM-protected content is economically less valuable than unprotected content, an additional parameter $d \in [0 : 1]$ is defined, which takes into account the degree to which the consumer is restricted in use of legal downloads. The value of d is dependent on the scope and severity of the DRMS in place. We arrive at the following new utility function for the legal download:

$U(x_1, x_2) = v_{x1}(1 - d)x_1 + v_{x1}(1 - q) x_2$

DEMAND FOR DIGITAL CONTENT

This section shows an aggregated model of consumers' demand for digital content. It specifically illustrates the implications of DRMS on the demand for digital content. For the sake of simplicity, we note the utility of the original by means of the parameter v instead of v_{xi}, which is reduced either by a value of q when it is a copy or by the value of d in the case of the original, as shown in the previous sections. As we assume that only the original has a price, we note it as p instead of p_{x1}. We assume that the valuation of the digital content is uniformly distributed over the interval of [0 : 1] and the size of the market is normalized to 1. Therefore, the distribution of consumers, and hence the demand for digital content, can be presented as shown in Figure 1.

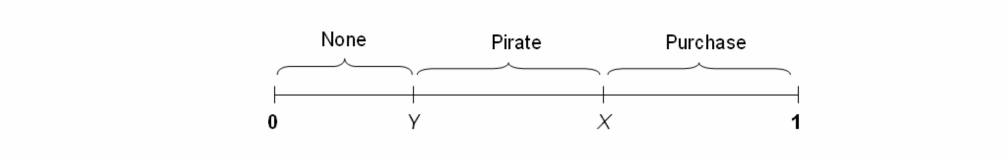


Figure 1: Demand for Digital Content

The consumer's utility function is given as:

$$U = \begin{cases} v(1 - d) - p & \text{when s/he purchases an original} \\ v(1 - q) - \mathrm{z} & \text{when s/he pirates/copies content} \\ 0 & \text{when s/he does not consumes digital content at all (none).} \end{cases}$$

We want to assess the impact of DRMS on consumer behavior, and especially on the demand for digital content. We discuss two cases: First, one in which no DRM is applied and, second, one in which DRM were applied, in order to show the effect of content control on the demand for originals and copies.

DEMAND WITHOUT DRM

If no DRM were in place there would be no restriction on use of the legal download, giving $d = 0$. Furthermore, in this case $m = 0$, meaning that the probability of being caught is $u^{(1-um)} f$ => uf. Assuming that $v, p \geq 0$, and by taking the marginal consumer X from Figure 1, who does not care whether s/he purchases the original or pirates the content, is facing the following:

$$v - p = v\ (1 - q) - uf$$

$$v = \frac{p - uf}{q}$$

The marginal consumer Y, who does not care whether s/he pirates or does not consume the product, is facing the following:

$$v\ (1 - q) - uf = 0$$

$$v = \frac{uf}{1 - q}$$

Hence, if the market is normalized to 1, the demand for originals D_o is

$$D_o = (1 - X)$$

$$D_o = 1 - \frac{p - uf}{q}$$

and the demand for copies or pirated content D_p is

$D_p = (X - Y)$

$$D_p = \frac{p - uf}{q} - \frac{uf}{1-q} = \frac{(1-q)(p-uf)}{(1-q)q} - \frac{quf}{q(1-q)} = \frac{p(1-q) - uf(1-q) - quf}{q(1-q)} = \frac{p(1-q) - uf + ufq - ufq}{(1-q)q} = \frac{(1-q)p - uf}{(1-q)q}$$

$$D_p = \frac{(1-q)p - uf}{(1-q)q}$$

Therefore, when the option of making a copy exists and no DRM is in place, consumers with low values of $v < uf / (1 - q)$ do not consume music. Those with intermediate values
$uf / (1 - q) \leq v < (p - uf) / q$ make copies. Only consumers with high value of $v > (p - uf) / q$ purchase the content, as Figure 2 shows.

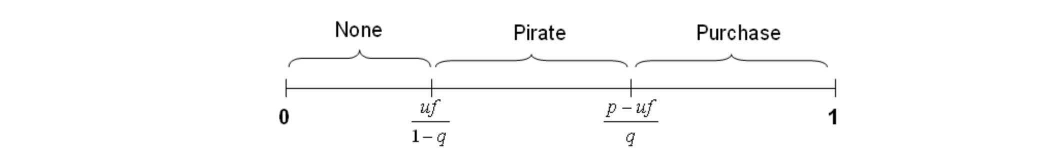


Figure 2: Demand without DRM

DEMAND WITH DRM

When there is DRM in place, hence $m > 0$, the probability of being caught is therefore $u^{(1-um)} f = z$. For notation we will also use z in this case. DRM has an impact on the utility of the original to the consumer, which is expressed by the parameter d. Assuming that $v, p \geq 0$, the marginal consumer X, who does not care whether s/he purchases the original or pirates the content, is facing the following:

$v(1 - d) - p = v(1 - q) - u^{(1-um)} f$

$$v = \frac{p - u^{(1-um)} f}{q - d}$$

The marginal consumer Y, who does not care whether s/he pirates the product or does not consume it at all, is facing the following:

$v(1 - q) - u^{(1-um)} f = 0$

$$v = \frac{u^{(1-um)} f}{1 - q}$$

Hence, if the market is normalized to 1, the demand for originals D_o is

$D_o = (1 - X)$

$$D_o = 1 - \frac{p - u^{(1-um)} f}{q - d}$$

and the demand for copies or pirated content D_p is

$$D_p = (X - Y)$$

$$D_p = \frac{p - u^{(1-um)}f}{q-d} - \frac{u^{(1-um)}f}{1-q} = we\,use\; z = u^{(1-um)}f \rightarrow \frac{(1-q)(p-z)}{(1-q)(q-d)} - \frac{(q-d)z}{(q-d)(1-q)} = \ldots = \frac{p(1-q) - z(1-d)}{(1-q)(q-d)}$$

$$D_p = \frac{(1-q)p - u^{(1-um)}f(1-d)}{(1-q)(q-d)}$$

Therefore, when they have the option of copying and DRM is in place, consumers with a low value for $v < u^{(1-um)}f\ /\ (1 - q)$ do not consume music. Those with intermediate values for $u^{(1-um)}f\ /(1 - q) \leq v < p - u^{(1-um)}f\ \ /\ (q - d)$ make copies. Consumers with high values for $v > p - u^{(1-um)}f\ \ /\ (q - d)$ purchase the product; as Figure 3 illustrates.

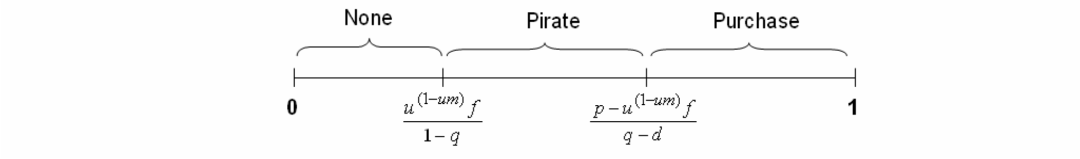


Figure 3: Demand with DRM

CONCLUSION

There are two main implications of DRM on the demand for digital content as can be seen from the model. First, thanks to DRM, detection of and prosecution for copyright violation become easier, which increases the probability of being caught expressed by the parameter *m* in our model. Our model shows that *m* has an impact on both intervals or regions, as illustrated in Figure 3. When *m* > 0, on the one hand it increases the purchase region, where consumers switch from pirating to purchasing, and on the other hand it reduces the demand for pirated content by switching some consumers from pirating to ceasing to consume. The key reason for this switch in both cases is the increased probability of being caught, which leads to increased copying costs for the consumer. The switch from one region to the other depends on the value the consumer places on the digital content.

In the case of consumer Y, the increase in the cost of copying due to the higher probability of being caught causes her/him not to consume the copy at all. In this case we could argue that piracy has not impacted on content providers' businesses, for the following reason. The consumer's initial valuation of the product was relatively low. Indeed, s/he did consume music, but only copies, and if the associated copying costs increase, in our case due to the increased probability of being caught, s/he prefers no longer to consume the product.

In the case of consumer X, the increase in copying costs makes her/him switch from pirating to purchasing. Hence, the resulting net benefit of the original is higher than that of the copy. In this case we could argue that the copy initially had a negative impact on content providers' businesses, as the consumer acquired the copy instead of purchasing the original. With the implementation of DRMS and the resulting increased copying costs to consumers, s/he switches from copying to purchasing. Thus, the extent to which piracy impacts on a content provider's business depends on the distribution of consumers' valuation or the utility they attribute to the digital content. In other words, individuals who put a low value on the original when copying is available are more prone to pirate than are individuals who put a higher value on the original.

The second implication of DRM is related to restrictions on the original. In our model we have expressed any restrictions on the original by the parameter *d*. These restrictions will not affect marginal consumer Y, who has no preference for not consuming over pirating. The restrictions only affect marginal consumer X. This reduction of the utility of the original also reduces the purchase region and causes consumers to switch from purchasing to pirating. In other words, if the market size stays the same there will be the same number of consumers not consuming any music, but there will be more consumers pirating than if no DRMS were in force.

The overall effect of security technologies on the demand of digital content depends heavily on the various parameters in the model and the type of distribution the consumer's estimate of utility of the original. However, what can be said is that, depending on the value the consumer puts on the digital content, not all copies should be regarded as lost sales. Some (marginal consumers Y) are copying for convenience, as copying costs are currently relatively low or nonexistent, where others (marginal consumers X) might buy the product but still prefer to copy because of the low or nonexistent copying costs. When security technologies such as DRMS are implemented, these consumers purchase the content due to the increase in copying costs. In this case it can be seen as a lost sale for the content industry. However, DRM might also have the effect of reducing the legal demand as a result of restrictions on the original, so that content providers make copying more attractive than purchasing. This is a problem with any protection technology, as it is primarily concerned with the illegal usage of material and has little consideration for consumers who purchase content, often even hampering such lawful consumers.

REFERENCES

Andres, R., The European Software Piracy: An Empirical Application, URL: http://www.serci.org/2002/Rodriguez.pdf [Accessed: 2005-07-01].

Bhattacharjee, S. et al., No more shadow boxing with online music piracy: Strategic Business Models to Enhance Revenues, Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), Hawaii 2002, 200-211.

Buhse, W., Digital Rights Management for Music Filesharing Communities, Proceedings of the Seventh Americas Conference on Information Systems (AMCIS 2001), Boston 2001, 1537-1543.

Chen, Y., Png, I., Software Pricing and Copyright Enforcement: Private Profit vis-a-vis Social Welfare, Proceedings of the 20th International Conference on Information Systems, Charlotte 1999, 119-123.

Chiang, E., Copyright Protection in U.S. Universities: An Overview of Copyright Piracy, Risk Attitudes towards Copyright Law, and Willingness-to-Pay, Manuscript 2003.

Fetscherin, M., Evaluating consumer acceptance for protected digital content, in: Becker, E., et al. (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Berlin: Springer 2003, 342-362.

Holm, H., Can Economic Theory Explain Piracy Behavior? in: Economic Analysis & Policy 3 (2003), 1.

IFPI, IFPI Music Piracy Report, URL: http://www.ifpi.org/site-content/library/piracy2002.pdf [Accessed: 2005-07-01].

Katz, A., A Network Effects Perspective on Software Piracy, URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=386141 [Accessed: 2005-07-01].

Papadopoulos, T., Determinants of International Sound Recording Piracy, in: Economics Bulletin 6 (2003) 10, 1-9.

Sims, R., Cheng, H. K., Teegen, H., Towards a profile of student software pirates, in: Journal of Business Ethics 15 (1996) 8, 839-849.

Wijk, J., Dealing With Piracy. Intellectual Asset Management in Music and Software, URL: https://ep.eur.nl/retrieve/229/erimrs20020930173203.pdf [Accessed: 2005-07-01].

TOWARDS AN E-MARKET MODEL

Reimer Ivang, Aalborg University, Denmark
Robert Hinson, Aalborg University, Denmark & University of Ghana Business School,
Ramanathan Somasundaram, National Institute for Smart Governmen India

ABSTRACT

Purpose: Seeks to argue that there are problems associated with e-market definitive efforts and consequently seeks proposes a new e-market model. Design/methodology/Approach: Paper based largely on literature survey and an assessment of the existing e-market conceptualizations. Findings: Based on the literature survey and identification of gaps in the present e-market definitive models, the authors postulate a preliminary e-market reference model. Originality/Value: Through synthesizing the e-market literature, and by taking into account contemporary e-market developments, key dimensions that define an e-market are identified and explained.

Key words: electronic, markets, model, review

INTRODUCTION TO E-MARKETS

Kambil and Van Heck (1998, 2002) have argued that online auctions and exchanges will soon be an essential part of business practice. They explain why companies must adopt electronic markets now if they hope to compete in the future. E-markets and their effects on market structures and business relationships have been subject for extensive research and date back to the late 1980s (see Malone, Yates et al. 1987 for some of the earliest work). B2B electronic marketplaces (e-markets) have in their short life been the subject of what might be described as contrary views of their perceived usefulness. Different organizational entities have different views on e-markets. On the one side, companies tell horrifying stories of whole industries that are suffering from auctions and other very transactional oriented applications. These applications bring price pressure and intense competition. In some industries the price pressure is so intense that the supplying companies cannot maintain margins for further research and development. As a result the old well-proven business models have to be altered. Those who manage the change will be the future winners. Conversely, companies tell stories of e-markets where the results are definitely not increased competition and extra price pressure. These e-markets bring suppliers and customers closer together support collaborative and long-term commitments, which could not have worked without today’s modern technology. These stories bring promises of upgrading the relationships to those suppliers whom manage the situation and provide the needed data in the agreed format. The suppliers, which manage this situation and adapt to these new customer needs, define the future winners. Elemica, GlobalSources and Alibaba are some of the best examples of successful e-markets.

Investors and participating companies have witnessed that e-market business models, which seemed to be guaranteed successes, in some cases were associated with so many problems that some e-markets have had to file for bankruptcy. At the turn of the new century (year 2000 onward) there was estimated to exist, over 2000 e-markets and today many of these have closed for business. An examination of the e-market database at emarketservices.com shows that there at present time exist less than 1000 e-markets (eMarketServices 2001-2004). Nowadays, governments, individual consumers and businesses are able to transact with one another either with their own types or with the other types over the Internet (Grieger 2003). Of the nine possibilities, we in this paper focus on the Business to Business (B2B) segment that has the most potential. Gartner consulting estimates B2B trade to hit as much as US$ 6 trillion by 2004 (Meehan 2001). Several intermediary organizations such as IBX and Gatetrade have arisen in the recent years hosting B2B trading infrastructure for a fee. Trading through e-market has become the norm in some industries such as the chemical and textile industries. It is expected that trading through e-market will be the norm in several other industries in the near future. Trading via e-markets is a massive development for businesses. The medium of transaction when shifted affects businesses for;

- the market structure is altered (Malone et al. 1987; Bakos 1991; Clemons et al. 1993; Wigand and Benjamin 1995; Bakos 1997; Bakos 1998; Daniel and Klimis 1999)
- disintermediation and cybermediation occurs (Sarkar et al. 1995; Bailey and Bakos 1997; Sarkar et al. 1998; Sinnecker and Christiaanse 2001)
- the supply chain relationships requires review (Anderson and Lee 2000; Essig and Arnold 2001; Grieger and Kotzab 2002; Skjøtt-Larsen et al. 2002)
- it requires organizational restructuring and new management practices (Archer and Gebauer 1999; James et al. 2000; James et al. 2000a; Brooks and Dik 2001; Boer et al. 2002)

THE RESEARCH GAP

As early as 1987, Malone et al. theorized the impact of information technology on governance structures. Theoretical research by Bakos (1991) and Clemons et al. (1993) also enriched our understanding of the subject. Researchers have used several theories such as transaction cost theory (Malone et al. 1987), information economics theory (Essig and Arnold 2001), game theory (Tomak and Xia 2002), channel evolution literature (Sarkar et al. 1998) and IOS adoption work (Piccinelli et al. 2001) for explaining e-market. Our understanding of the e-market concept has most certainly evolved since the early explanations by Malone et al. (1987) and Bakos (1991). Bakos (1991) terms e-market as *"an inter-organizational information system that allows the participating buyers and sellers in some market to exchange information about prices and product offerings"*. While this definition is still very valid, it does not adequately express the complexity of the entity. Recent explanations provided by such scholars as Lennstrand et al. (2001) recognize e-market as a thinking platform that intermediates between buyers and sellers. The recent definitions take into account dimensions such as ownership and transaction focus. There are other problems associated with e-market definitive efforts; see for example Choudhury et al. 1998; Segev et al. 1999; Sawy 2001; Barratt and Rosdahl 2002;and Mahadevan 2002. With a few exceptions, these efforts do not define e-market as their prime objective. The authors simply describe the concept as it is used in the context of their paper. While they usually cite explanations provided about e-market earlier, they identify some unique elements as well. During some instances, they use a different term for denoting the same aspect. It is thus our understanding of e-markets has evolved. Knowledge about e-market hence is distributed among a number of publications. Thus, there is clearly a need for unearthing this knowledge and making it easily available to those who embark on studying e-market.

Other efforts to objectively describe an e-market still have their drawbacks. Schmid and Lindemann (1998) for instance propose a reference model for explaining e-market. The objective of their model however is to guide the coherent development of e-market technical infrastructure. Several e-markets went bust not because they lacked technical infrastructure, bute instead because they were not breaking even due to inadequate participation. It seems to the authors of this paper therefore that thers has arisen a need to conceptualize not just the technical e-market attributes but also the attributes of the organization that is hosting it (the e-market) and the nature of goods and services traded over it. Kaplan and Sawhney's (2000) classification of e-market is a classic effort that defines an e-market. Their model despite it's objectivity however is found inadequate for relevant dimensions such as the transaction focus and ownership are not taken into account. Lennstrand et al.'s (2001) work has the explanatory power but it lacks clarity. Their objective is not to explain the key dimensions that define an e-market instead to study the impact of product and industry characteristics on value creation and business strategies. Their definition is more of a research framework that has dependencies than it is a model. We in this paper via a detailed literature review take on the task of attempting to develop a reference model for e-markets. Our effort serves two purposes. Firstly, it helps in synthesizing our knowledge about e-markets. Secondly, researchers can use the model for defining research possibilities and in the case of practitioners; they could use the model for evaluating an e-market.

RESEARCH METHODOLOGY

Literature reviews are useful for synthesizing what has been done so far and for identifying what needs to be done. Webster and Watson (2002) find two types of reviews. They are i) studying a mature area where the objective is to analyze and synthesize accumulated body of research and ii) studying an emerging area where the objective is to expose the study area to potential theoretical foundations. We find e-market area as having a tradition that is long enough to have a history. At the same time, it is in the cross roads for trading through e-market is increasingly becoming a norm. This implies that researchers by studying the challenges faced during the emergence of e-markets can advance science. It seems opportune then to synthesize a decade and a half long research tradition (e-markets) and to provide guidance for the future. To achieve our objective of comprehensively describing an e-market, we review literatures to find the various descriptions that have so far been provided. We combined the literature synthesis suggestions of Webster and Watson (2002) and augmented their ideology with the snow-balling technique described by Moriarty and Bateson (1982). We searched for the latest publications in the e-market area by searching for the term “electronic marketplaces” in both the title and in the abstract using DADS (Digital Article Database Service), ABI Inform and Emerald Library. We looked only into peer reviewed articles. From this we selected and read thoroughly a few recently published articles such as the work of Lennstrand et al. (2001) and Grieger (2003). From then on we relied upon the quoted literatures for finding relevant articles. At this point we were open to magazine articles, working papers, internet sites, consultant reports and other types of reports. In all, we identified, read thoroughly and once revised 69 papers[1]. From this we took notes on 24 papers as they had a claim on the description of electronic markets. These 24 papers were chronologically revised once again for better understanding the nature of their claim. In order to synthesize a comprehensive description of e-markets, we weeded out redundancies in their claims. Finally, we conceptualized electronic markets the best way we could think of by relying on the literatures and as well by relying on our experiences for arriving at our comprehensive description. In the section that follows, a critical summary of our findings is presented.

A REFERENCE MODEL FOR E-MARKETS

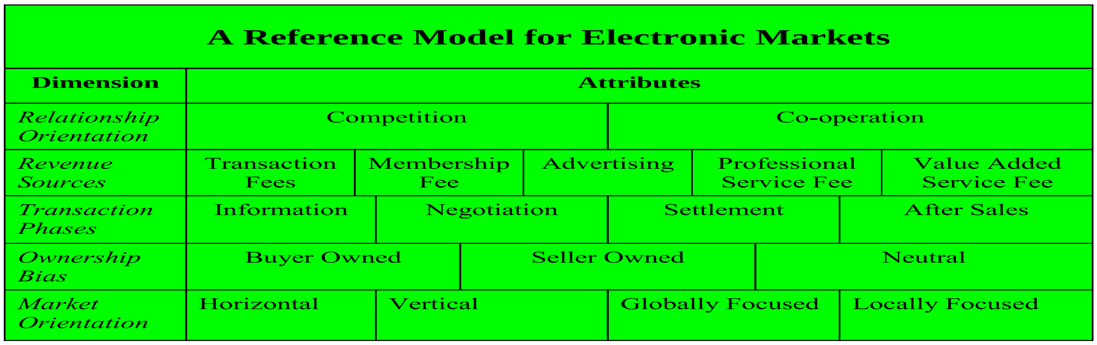
We relied on our synthesis of the e-markets literature for at our reference model for e-markets. The purpose of this model is to capture the widest latitudes of the e-market phenomenon. It is our fervent belief that practitioners and academics alike will be able to relate to the definitive aspects of our e-market model. It is pertinent to note however that the aspects defined within our e-markets model may be inter-related. We however do not discuss the nature of these relationships in detail. Hence in that sense it is not a conceptual framework in where propositions and predictions are made (Webster and Watson 2002). We hereby recognize e-market as not just an information system but also as an organizational entity that acts strategically.

[1] Please note that only the references mentioned in the paper are listed in the literature list. Please contact the authors for the full list

From our literature review we found 24 contributions that were unique either in terms of description details or in terms of terminologies. For instance, Choudhry et al.'s (1998) recognition of e-market as an organization that controls access to the information system is regarded a contribution for it then furthered our understanding of the concept by adding details. The suggestion of a different terminology for conceptualizing the same aspect is as well regarded as a contribution. For instance, representing the transaction process as under information, negotiation, settlement and after sales phases (Skjøtt-Larsen et al. 2002) just as pre-purchase determination, purchase consummation and post purchase interaction (Strader and Shaw 1997) is regarded a contribution. We however choose one that is the most suitable of the many for describing an aspect of e-market. Aiming for a model with clarity, we use as minimal a number of variables as possible. We combine two or more aspects of an e-market under one dimension when it is possible to do so. We take into account the recent developments in the e-market arena while arriving at the model. The resulting model thus has five dimensions which are i) transaction focus ii) market orientation iii) revenue sources iv) ownership bias and v) relationship orientation. A diagrammatic presentation of our reference model is presented in fig. 1.0. Our understanding of each of the five dimensions is hereby presented;

Transaction Focus

The value that an e-market adds depends on the extent to which it facilitates the carrying out of a transaction among buyers and sellers. As explained in the introduction to this section, Strader and Shaw (1997) just as Skjøtt-Larsen et al. (2002) propose different ways of conceptualizing a transaction. We choose the frequently quoted i) information ii) negotiation iii) settlement and iv) after sales phases classification to represent a transaction. A market can choose to focus on either one, two or even on all of the four phases. The Global Sources (www.globalsources.com) e-market focuses on presenting supplier information in a consistent and searchable manner. The Scan Market (www.scanmarket.com) e-market provides an auction infrastructure which buyers and sellers can lease for negotiation purposes. EC-Finance (www.ec-finance.com) develops information systems using which e-markets can electronically process letter of credits and thereby expedite carrying out settlement activities. In the after sales phase, logistics organizations such as Transcore (www.transcorexchange.com) have their own market in where they match logistics related requirements among carriers, agents and consumers. Kubus' TradeBuilder.net system (www.kubus.dk) provides the infrastructure for facilitating the sharing of experiences about products and services between end users in buying organizations and selling organizations. Chemconnect (www.chemconnect.com), an e-market in the chemical sector increasingly facilitates all phases of a transaction.



A Reference Model for Electronic Markets

Dimension	Attributes				
Relationship Orientation	Competition		Co-operation		
Revenue Sources	Transaction Fees	Membership Fee	Advertising	Professional Service Fee	Value Added Service Fee
Transaction Phases	Information	Negotiation	Settlement	After Sales	
Ownership Bias	Buyer Owned	Seller Owned	Neutral		
Market Orientation	Horizontal	Vertical	Globally Focused	Locally Focused	

Figure 1. A reference model for electronic markets

We categorize trading mechanism under the negotiation phase of a transaction. Earlier, prominent taxonomies such as that of Kaplan and Sawhney (2000) were made using trading mechanism as representing an axis. In the recent years however, just as Kambil et al. (1999) have posited, e-markets that provide several functions are becoming common place. Gatetrade (www.gatetrade.com), a Danish market for instance provides both aggregation and matching mechanisms. However, we still regard Mahadevan's (2002) classification of trading/market mechanism a valid contribution. It is just that trading mechanism is ranked as a second heading instead of the first. E-markets provide a vast range of products and services depending on the context in which they operate. These from an overall perspective can be categorized under any of the four phases.

Market Orientation

E-market, given its networked nature, requires participation of businesses (buyers and sellers) with synergetic requirements. Hence, it requires making its orientation explicit. A part of this orientation is captured by the frequently quoted classification horizontal vs. vertical (Kaplan and Sawhney 2000). The horizontal markets focus on the trading of operating supplies across industries (e.g. www.mro.com). In the vertical market, businesses usually belonging to a particular industry trade manufacturing inputs (e.g. www.elemica.com). Apart from the horizontal vs. vertical distinction, the market orientation term includes as well the geographical focus of the market. While some markets have a global orientation such as that of Global Supplies, others have a regional focus (www.byggehandel.dk). The term market orientation thus has two meanings. In one sense, it denotes the audience targeted as in the marketing sense. In the other sense, it says about the nature of goods and services traded in a market. It is the interaction of the targeted audience and the nature of trade dimensions that determines a market's orientation. This dimension explains a market's positioning efforts as in the strategy literature (Porter and Millar 1985). An e-market's transaction focus / product offerings are affected by its market orientation and vice versa. The *reach* dimension defined by the number of parties with whom a business can potentially trade and the *range* dimension that defines the types of good traded conceptualized by Sawy (2001) well expresses the market orientation dimension.

Revenue Sources

A market's ability to attract organization's for trading over its infrastructure is affected heavily by its service charges. At the same time, a market is able to self sustain only if it at least earns enough to meet its expenses. "Revenue sources" is a critical dimension for it pertains to a market's existence. Segev et al. (1999) recognize the revenue dimension during the early stages of describing e-markets. Barratt and Rosendahl (2002) cite a number of sources through which an e-market can earn. Lennstrand et al (2001) list five major sources of revenue for an e-market which are i) transaction fees ii) membership/licensing fees iii) advertising iv) professional service fees and v) value added service fees. E-markets rely on one or more or even all of the above revenue sources.

Ownership Bias

An e-market can be owned by a buyer, a seller or an independent party. Moreover, an e-market can either have a single owner or consortia of owners. Our description does not focus on a single buyer owned (e-procurement system) or a seller owned market (web shop). Owner when being a buyer or a seller is assumed to design the market with the objective of enhancing its' power in relation to the other group. A buyer owned market for instance would be designed such that the price transparency is high. A seller owned e-market in contrast would focus on the product qualities instead of the price. The market when owned by an independent is assumed to design the market in a neutral manner in order to entice adequate participation from both sides. The term "centricity" is often used to describe where the power lies between buyers and sellers of an e-market (Barratt and Rosdahl 2002). Covisint (www.covisint.com), an automobile exchange owned by the giants Ford, General Motors and Daimler – Chrysler, is an example of a buyer owned or a buyer centric e-market. Italian Moda (www.italianmoda.com) is owned by a consortium of Italian fashion and textile companies.

Relationship Orientation

An e-market can add value either by facilitating competition where its customers can find new trading partners on a spot basis or by facilitating co-operation where its customers can use the infrastructure for cementing ties. The term "market" is traditionally associated with competition, where price of a good determines the distribution of goods and services (Samuelson and Nordhaus 1992). However, empirical evidence shows collaborative activities on-going via e-market; incidence explained by the "move-to-the-middle hypothesis" propounded by Clemons et al. (1993). Christiaanse and Markus (2003) bring this development into light by discussing the case of Elemica marketplace. This dimension is a critical one for it affects the benefits that a business gains from participating in an e-market. This dimension can be regarded as a tactical one for a choice made here affects all of the other dimensions.

CONTRIBUTION TO E-MARKETS THEORY

The two central contributions of the paper are as follows; first, the notion of e-market as it has evolved since its inception is explained in details based on a thorough review of literatures. Second, through synthesizing the reviewed literatures and by taking into account the contemporary developments, key dimensions that define an e-market are identified and explained. The question addressed in this section is "how can research community make use of the propounded model for furthering knowledge about the e-market area?"

Firstly, our knowledge about e-markets would improve when each of the five dimensions and their sub divisions are better understood. Slabeva and Schmid (2000) for instance study in detail internet electronic product catalogs. Their work in relation to the proposed model can be termed as an effort for understanding the catalog trading mechanism within the transaction focus dimension. In such a sense, our model can be used as a reference model.

Secondly, the interrelationships between dimensions and among the five dimensions are to be explained. Based on empirical evidence, we can for instance foresee competition oriented markets focusing on the negotiation phase of a transaction. This hypothesis when tested can help us in understanding a small part of the puzzle. It however needs to be mentioned here that the puzzle that we are attempting to solve is a very complex one. We hereby calculate interaction possibilities that can be studied based on our classifications. The transaction focus dimension has *four* phases which are i) information ii) negotiation iii) settlement and iv) post sales. Under the negotiation phase there are *thirteen* trading mechanisms that Mahadevan (2002) describes. Market orientation as well is defined by *four* attributes which are i) verticial ii) horizontal iii) global focus and iv) local focus. We use Lennstrand's (2002) citation for listing *five* major sources of revenue which are i) i) transaction fees ii) membership/licensing fees iii) advertising iv) professional service fees and v) value added service fees. Ownership bias dimension has *three* attributes which are buyer, seller and independent owned e-market. Finally, the relationship dimension has *two* attributes; competition and collaboration. By multiplying 4 x 4 x 5 x 3 x 2 we get 480 relationships that require studying. If we multiple the number with third rung headings for instance the 13 trading mechanisms, we get 6240! That's a handful.

Thirdly, Soh and Markus (2002) recognizing the inadequacies of theory based and empirically grounded approach recommend the use of strategic archetypes approach. In which, frequently occurring configurations of e-markets are regarded as archetypes. The attributes that define an archetype are then holistically studied. Our model remains valid also in the context of this approach for the archetypes can be defined in terms of dimensions and attributes that we identify.

Finally, the research community is better off when there is a common understanding of the dimensions that define an e-market. We are of the opinion that knowledge can be accumulatively furthered when the proposed model or a revised version of it is used for referencing.

CONTRIBUTION TO E-MARKETS PRACTICE

We in this section explain as to how practitioners can make use of our model. Firstly, our model assists those hosting an e-market in positioning their services. The host as well can discuss their future plans using several dimensions that we identify in the model. For example, they can discuss about enhancing their transaction focus from just being an information provider to that of being a negotiation facilitator. While deciding upon a particular aspect of the model, they can indeed search the academic knowledge base for explanations. A common ontology among practitioners and the academia most certainly helps.

Secondly, trading via a particular type of e-market for a business is a strategic decision. Such a choice for sure affects its profitability and in some cases even its existence. Businesses can use our model for discussing the available options or possibilities and the consequences of trading via a particular type of e-market. Businesses using the dimensions of our model can as well analyze the likelihood of an e-market's success.

CONCLUSIONS

We realize that e-market is a complex phenomenon in this closing remark. To us, the different types of e-markets that can possibly exist and the very large number of interrelationships that require studying do not spring a surprise. It is a challenging task for we essentially attempt reorganizing our traditional ways of working over the Internet environment that has unique properties. Both academicians and practitioners have had a tough time in understanding what e-markets are and how we effectively make use of them. The challenge is further enhanced by the evolving nature of the subject. Despite which, we philosophize that conceptualizing the dimensions that define e-markets defines progression. To minimize the risk of misunderstanding, we explicitly state that the proposed model is the best that we could come up. We sincerely hope that the research community critically analyzes our reference model and further enhances it. Given the dynamic nature of the subject that we are trying to grapple with, there is a need for regrouping at regular time intervals for marching ahead.

REFERENCES

Anderson, D. and H. Lee (2000). The Internet-Enabled Supply Chain: From the First Click to the Last Mile. Mont, Montgomery Research Inc.

Archer, N. and J. Gebauer (1999). Managing in the Context of the New Electronic Marketplace. 1st World Congress on the Management of Electronic Commerce, Ontario, Canada.

Bailey, J. P. and J. Y. Bakos (1997). An Exploratory Study of the Emerging Role of Electronic Intermediaries. International Journal of Electronic Commerce, 1(3).

Bakos, J. Y. (1991). A Strategic Analysis of Electronic Marketplaces. MIS Quarterly, 15(3): 295-310.

Bakos, J. Y. (1997). Reducing Buyer Search Costs: Implications for Electronic Marketplaces. Management Science, 43(12).

Bakos, J. Y. (1998). The Emerging Role of Electronic Marketplaces on the Internet. Communication of the ACM, 41(8).

Barratt, M. and K. Rosdahl (2002). Exploring Business-to-Business Marketsites. European Journal of Purchase & Supply Management, 8.

Boer, L. D., J. Harink and G. JHeijboer (2002). A Conceptual Model for Assesing the Impact of Electronic Procurement. European Journal of Purchase & Supply Management, 8.

Brooks, J. and R. Dik (2001). B2B Markets: The Smart Path Forward, The Boston Consulting Group.

Chafey D. (2004), "E-business and E-commerce Management 2ed Prentice Hall, 10

Choudhury, V., K. S. Hartzel and B. R. Konsynski (1998). Uses and Consequences of Electronic Markets: An Empirical Investigation in the Aircraft Parts Industry. MIS Quarterly, December.

Christiaanse, E. and L. M. Markus (2003). Participation in Collaboration Marketplaces. Hawaii International Conference on System Sciences, Hawaii.

Clemons, E. K., S. P. Reddi and M. C. Row (1993). The Impact of Information Technology on the Organization of Economic Activity: The "Move to the Middle" Hypothesis. Journal of Management Information Systems, 10(2): 9-31.

Dai, Q. and R. J. Kaufmann (2002). Business Models for Internet-based B2B Electronic Markets: An Exploratory Assessment. International Journal of Electronic Commerce, 6(4).

Daniel, E. and G. M. Klimis (1999). The Impact of Electronic Commerce on Market Structure: An Evaluation of the Electronic Market Hypothesis. European Management Journal, 17(3).

Essig, M. and U. Arnold (2001). Electronic Procurement in Supply Chain Management: An Information Economics-Based Analysis of Electronic Markets. The Journal of Supply Chain Management, 37(4).

Giaglis, G. M., S. Klein and R. M. Keefe (2002). The Role of Intermediaries in Electronic Marketplaces: Developing a Contingency Model. Information Systems Journal, 12(3).

Grieger, M. (2003). Electronic Marketplaces: A Literature Review and a Call for Supply Chain Management Research. European Journal of Operational Research, 144: 280-294.

Grieger, M. and H. Kotzab (2002). Supply Chain Management Beyond Electronic Marketplaces - Insights from the Chemical Industry. Proceedings of the 14th Annual Conference for Nordic Researchers in Logistics (NoFoma), Trondheim, Norway.

James, A., B. Andy and S. Harold (2000). Electronic Marketplaces: Strategies for Sellers, The Boston Consulting Group.

James, A., B. Andy and S. Harold (2000a). Electronic Marketplaces: Surviving the Shakeout, The Boston Consulting Group.

Jelassi, T. Enders, A. (2005), "Strategies for e-business: Creating value through Electronic and Mobile Commerce: Concepts and Cases"; Prentice Hall; 4

Kambil, A., P. F. Nunes and D. Wilson (1999). Transforming the Marketspace with All-in-One Markets. International Journal of Electronic Commerce, 3(4).

Kambil, A. and Van Heck E. (1998), "Re-engineering the Dutch flower Auctions: A Framework for Analyzing Exchange Organizations" Information Systems Research, 9, No. 1, 1-19

Kambil, A. and Van Heck E. (2002), "Making Markets, How Firms design and profit from online auctions and Exchanges"; Harvard Business Press

Kaplan, S. and M. Sawhney (2000). E-Hubs: The New B2B Marketplaces. Harvard Business Review.

Lennstrand, B., M. Frey and M. Johansen (2001). Analyzing B2B eMarkets - the Impact of Product and Industry Characteristics on Value Creation and Business Strategies. ITS Asia-Indian Ocean Regional Conference.

Mahadevan, B. (2002). Emerging Market Mechanisms in Business-to-Business E-Commerce: A Framework. International Conference oon e-Business, e-Education, e-Science, and e-Medicine on the Internet (SSGRR 2002's), Rome, Italy.

Malone, T. W., J. Yates and R. I. Benjamin (1987). Electronic Markets and Electronic Hierarchies. Communication of the ACM, 30(6).

Meehan, M. (2001). Gartner Scales Back B2B projections. ComputerWorld.

Moriarty, R. and J. Bateson (1982). Exploring Complex Decision Units: A New Approach. Journal of Marketing Research, 19(May).

Piccinelli, G., G. Vitantonio and L. Mokrushin (2001). Dynamic Service Aggregation in Electronic Marketplaces. Computer Networks, 37: 95 - 109.

Porter, M. E. and V. E. Millar (1985). How Information Gives you Competitive Advantage. Harvard Business Review: 149-160.

Samuelson, P. and W. D. Nordhaus (1992). Economics, McGraw Hill.

Sarkar, M., B. Butler and C. Steinfield (1998). Cybermediaries in Electronic Marketspace: Toward Theory Building. Journal of Business Research, 41: 215-221.

Sarkar, M., B. S. Butler and C. Steinfield (1995). Intermediaries and Cybermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace. Journal of Computer-Mediated Communication, 1(3).

Sawy, O. E. (2001). Identifying Structural Models of B2B Procurement Exchanges, Marshall School of Business.

Schmid, B. and M. Lindemann (1998). Elements of a Reference Model for Electronic Markets. 38th Hawaii International Conference on Social Sciences.

Segev, A., J. Gebauer and F. Farber (1999). Internet-Based Electronic Markets. International Journal of Electronic Markets, 9(3).

Sinnecker, R. and E. Christiaanse (2001). Impacts of Electronic Marketplaces on Brick and Mortar: The Elemica Case. European Conference on Information Systems.

Skjøtt-Larsen, T., H. Kotzab and M. Grieger (2002). Electronic Marketplaces and Supply Chain Relationships. Industrial Marketing Management.

Soh, C. and L. M. Markus (2002). Business-to-Business Electronic Marketplaces: A Strategic Archetypes Approach. Twenty Third International Conference on Information Systems.

Stanoevska-Slabeva, K. and B. Schmid (2000). Internet Electronic Product Catalogs: An Approach Beying Simple Keywords and Multimedia. Computer Networks, 32.

Stockdale, R. and C. Standing (2002). A Framework for the Selection of Electronic Marketplaces: A Content Analysis Approach. Internet Research: Electronic Networking Applications and Policy, 12(3).

Strader, T. J. and M. J. Shaw (1997). Characteristics of Electronic Markets. Decision Support Systems, 21.

Timmers P., (2000), "Strategies and Models for business-to-business trading electronic commerce", John Wiley and Sons Limited; Paperback edition; 4

Tomak, K. and M. Xia (2002). Evolution of B2B Marketplaces. Electronic Markets, 12(2).

Turban, E. King, D. Viehland D. and Lee, J., (2006), "Electronic Commerce 2006: A Managerial Perspective; Prentice Hall; 4

Webster, J. and R. T. Watson (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26(2): xiii-xxiii.

Wigand, R. T. and R. I. Benjamin (1995). Electronic Commerce: Effects on Electronic Markets. Journal of Computer Mediated Communication, 1(3).

http://www.ncl.ac.uk/nubs/research/news.htm (accessed 1st September, 2005)

ICT, NEW WORKING ELITE, AND SOCIAL IMPLICATIONS

Faruk Karaman, Okan University, Istanbul-Turkey
Gonca Telli Yamamoto, Okan University, Istanbul-Turkey

ABSTRACT

The advances in the Information and Communication Technologies (ICT) are frequently compared with the Industrial Revolution (IR). Similar to IR, the ICT Revolution (ICTR) caused an upheaval in the social fabric. The prestigious occupations of the recent past lose value while ICT occupations climb the ranks. Purpose of this paper is to increase awareness of the unemployment threat from technology among academicians, industry practitioners and urge them formulate solutions for this problem. In this paper we first define a new category of IA Jobs besides the traditional agricultural & services jobs. Then we developed job sophistication Index (JSI).

Key Words: IA Jobs, job satisfaction index, technological change, unemployment

INTRODUCTION

Unemployment became a major problem despite the economic and technological developments in the post-industrial era. In his book Reich (2001), discusses how the workplace became insecure as companies adopt strategies like lean organization, outsourcing, etc and he give a picture of bleak future for the employees. He also introduces “fast-track” and “slow-track” concepts which are very useful in modeling the new workplace which we greatly benefited from. According to Reich, new technologies cause unemployment and governments are unable to reach a solution. To tackle this new type of structural unemployment classical classification of jobs should be altered and the problem should be viewed from a different angle. The problem is that the current job categories of agricultural, industrial, service jobs in use are not sufficient to analyze the unemployment patterns in the new economy.

For that purpose, we introduced a new category of jobs called intellectual and artwork (IA) jobs and defined a Job Sophistication Index (JSI). These two new concepts give us a new path to see the source of the post industrial era unemployment. Also, with such tools it is easier to predict the future of the professions and challenges it will face.

During the course of the industrial revolution, the share of the manufacturing and agriculture sectors in the total employment consistently declined and that of the services sector increased (Ochoa and Corey, 2004). In other words, the services sector compensated the job losses stemming from industrialization.

In the information age, the services sector is a source of unemployment itself and the middle class is shrinking. Developments about the software industry and the Internet technologies coerce the services industry. For example, the number of employees in the banking industry shrinks globally via mergers and acquisitions. New jobs arise mainly in technical fields such as software, hardware, biotechnology and genetics. These jobs naturally do not offer a solution to the people with non-technical orientation. Therefore a novel approach is needed for them.

For “non-technical” people the key question is: What the tasks that the human being has superiority over the computers were. Obviously, in creativity, artwork and intellectual work, human beings still have a definite advantage and will keep this advantage for a predictable future. At least, apart from technical jobs, these intellectual studies and artwork offers a solution for the compensation of the jobs lost to the technology. Hereupon, we will call these jobs as “Intellectual and Artwork-Type Jobs” or IA-Jobs.

HISTORICAL DEVELOPMENT

Before the industrial revolution agricultural jobs and craftsmanship was the main source of jobs, as seen on the “Figure 1”. In fact, military and church can also be added but the main idea is the same. In the 19th century, factories become the source of employment and peasants became factory workers. During the course of the 20th century new machinery and equipment decreased the need for muscle force and aroused services sector requirements. People were now using partly their intellectual and relationship capital depending on the nature of the job.

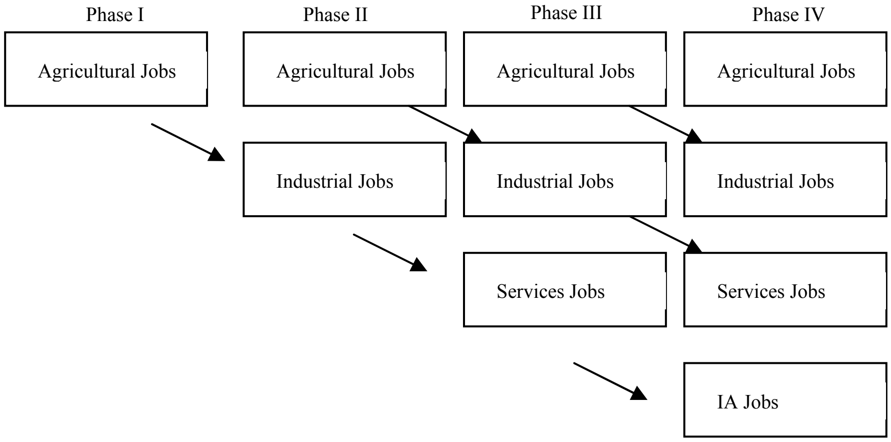


Figure I. Migration of jobs from agriculturel jobs to IA-jobs

Currently, we are again in the midst of a major transformation and rapid technological change makes services sector workers unemployed. Although, industrial and agricultural sectors also continues to lose jobs to the services sector, those who has lost jobs in the services sector are highly qualified and have no other place to go than the IA sector.

One reason to choose the acronym “IA” for the IA-Jobs and IA sector is to refer that these are the jobs that can best resist against the destructive powers of the technology. AI is used as the acronym for the Artificial Intelligence which is a field that can be seen as the most direct threat to the human capabilities. AI discipline tries to mimic the human brain and even surpass it. The IA jobs in this context can be seen the jobs that can resist the threat from the AI. We hold the view that, technology will not be able to replicate all of the human capabilities but will enhance them. Those capabilities that can not be replicated are IA capabilities.

One of the well-known *five forces* of Michael Porter is “entry barriers” (Porter, 1998). These barriers are very low for the internet companies and this causes low profits. For the IA jobs the biggest problem is the protection of the work done by the IA workers. The content business could not be made a profitable business itself and depends on the advertisement revenues. The illegal copying over the Internet poses a threat against the music, film-making industries. Music, pictures, videos, text and software are copied via Internet. This is not only an infringement of the copyright laws but also increases the *bargaining power of the customers* albeit illegally. This is another force of the Michael Porter. In Porter’s framework the classical services jobs are in danger due to the weakening industry structure. Content Protecting Technologies (CPT) present a solution against the threat of the technology content and intellectual work should be protected more strictly for IA-jobs. (Yamamoto & Karaman, 2005).

In other words, the illegal copying over the Internet prevents the take-off of the IA sector which postpones the solution of the structural unemployment problem. In a way, by copying content and intellectual property illegally people eventually harm themselves. The concepts IA-jobs, technology-driven unemployment are important to increase awareness about the problem and to fasten the process to adopt better and more effective measures to protect content. For IA sector to provide enough new high-paying jobs to replace the lost services and industrial jobs the products of the IA workers should be protected much stricter than ever. This need seems to be only felt more widely as new waves of the technology come into scene.

DETAILS OF THE TYPE OF THE TASKS

AGRICULTURAL TASKS:

These are mostly physical tasks. Examples are basic irrigation, planting, harvesting, and storing tasks. These should not be confused with modern agricultural techniques and these tasks are not confined to agriculture. The name “agricultural tasks” points to the fact that these are unsophisticated tasks belonging to the pre-industrial era and people do not use industrial-age level or more advanced technology in performing these tasks.

INDUSTRIAL TASKS:

In performing these tasks people use industrial-age level technology. Using such machinery, maintenance, working in the production line are examples. However, even in the industrial age, services and IA-tasks and jobs occur. As a result, “industrial tasks” too must be seen as an average sophistication level seen in the industrial age in the industrial sector. Industrial tasks are also tasks that can be performed by machinery and technology alone. The decision to use human labor (HL) instead of technology or machinery labor (TML) is mostly a political and economic issue. If HL is cheaper HL is used, if not TML is used provided that its usage is not limited to safeguard the employees. The key point is that an industrial task can be completely automated if the cost of doing so is not an issue.

SERVICES TASKS:

Services tasks can be defined as activities involving at least another person. All activities which involve the use of machinery or technology are excluded. Within the framework of this definition, a computer programmer’s job is not a services job but rather a mixture of industrial and IA-job. Commonly such technical jobs are included in the services sector which is a misleading classification. Salespeople, customer representatives are excellent examples of the nearly pure services jobs. Technical help and call center workers’ jobs involve both industrial and services components with very limited IA components. Expansion of the services sector is being presented as a solution to the unemployment but the pitfalls of that idea are examined before. If there is a commercially available technology that can replace human being that particular task can not be services or IA tasks. Examples of services workers under threat include “simultaneous translators” and “call center agents.”

IA TASKS:

The distinction with a services task/job or IA task/job is not easy. In the current practice the latter is included in the services sector. The terms “information society” “information sector” are inadequate for our purposes. Therefore we defined a new category named “intellectual and artwork” jobs.

To distinguish IA tasks from services and industrial tasks, the following criteria can be helpful:

a) An IA task is characterized by innovativeness and high level of intellectual activity,
b) An IA task can not be performed solely by technology without the involvement of human being. If a technology enables a task to be performed by technology alone without human intervention then it is no longer an IA task but rather an industrial task. In other words, the line of distinction is not static but rather dynamic,
c) An IA task can be performed by just one person in contrast with a services task necessitating the involvement of at least two people.

JOB SOPHISTICATION INDEX (JSI)

In order to make a more quantitative discussion we need a quantitative means of measurement about the four categories a particular job belongs to. Such a quantitative measure will also enable practitioners and researchers to test develop and test the ideas presented above. For this purpose we developed the Job Sophistication Index (JSI Index) which is explained below.

JSI is an index that measures the sophistication level of a job enabling to asses the job security in the face of technology. In other words JSI index measures the difficulty for the technology to replace human being in a particular job. It is apparent that a job can not be pure industrial job or services job etc…

To calculate the JSI index,

1. Decompose the job in question into agricultural, industrial, services, and IA components,
2. Give each component weights from 1 to 4 “taken in Table I”, 1 representing least sophistication and 4 representing most sophistication,
3. Calculate the weighted average of the sophistication levels to reach the Job Sophistication Index (JSI Index).

Table I. JSI Index Calculation Table

Type of the Tasks	% Weight	Sophistication Level
Agricultural Tasks	WA	1
Industrial Tasks	WI	2
Services Tasks	WS	3
IA Tasks	WIA	4

JSI FORMULA:

Job Sophistication Index (JSI) = (WA) x (1) + (WI) x (2) + (WS) x (3) + (WIA) x (4)

WA: weight of agricultural tasks in the job definition
WI: weight of industrial tasks in the job definition
WS: weight of services tasks in the job definition
WIA: weight of intellectual and artwork (IA) tasks in the job definition

THE INTERPRETATION OF THE JSI INDEX:

The JSI index can range from 1 to 4. One represents a purely agricultural job, four represents a purely IA-job. Of course the JSI index is a proxy for sophistication and an index of 2 may not belong to an industrial job and may belong instead a services job.

The significance of the index is that, the higher the index the harder for the advances in technology to replace the human capability. That translates into better job security in front of the destructive forces of the technology. A low index means the job is not adding so much value. These kinds of jobs involve mostly routine tasks and can be easily automated at low cost. A job having a high JSI Index of 3.5 for example requires highly skilled and educated labor and innovativeness.

The JSI Index has implications for the education sector and human resources departments of the companies in that innovative capabilities and skill should be developed for each individual for them to survive in a world of rapid technological change.

LIMITATIONS OF THE IA-JOBS AND JSI INDEX CONCEPTS:

The JSI Index presented in this study, although original and a revolutionary new concept was not tested in the day-to-day workplace and its value and usefulness is yet to be seen. Also, both the concepts IA-jobs and JSI-index may be hard to visualize and apply by the Human Resources (HR) practitioners.

Dividing a job into its tasks as defined in this paper requires an in-depth analysis and knowledge of the job. The traditional distinction of the industrial and services jobs are also misleading. However, the traditional view is being used for many years and achieved an almost axiomatic status which can not be challenged.

It can be asked that why we try to divide the jobs into new categories. This is because we think that the recent unemployment and underemployment problem faced is the result of the technological changes which frequently referred as “the new economy” (Hartman, Sifonis & Kador 2000). Hartman and Sifonis use “e-conomy” almost as equivalent of “the new economy”. According to a broad view “the new economy” includes technologies such as biotechnology, genetics, nanotechnology, robotics, advanced materials besides the frequently quoted Information and Communication Technologies (ICT). For the purposes of this study, we prefer this latter broader definition since it helps visualizing how the unemployment problem will get worse in the near future as the genetics and robotics take off.

The destructive effects of the technology is well-known and widely accepted however there is no effort to quantitatively measure the effect of technology on persons’ losing their jobs.

We accept that, JSI index, even though may be hard to compute for the HR practitioner for hundreds of jobs he or she deal with, can be seen only a simple model of the actual phenomenon. Since it is new and it was not practically tested it is hard to assess its practical value. However, one thing is certain. Technology causes unemployment and this could have influences in people's lives. Defining a problem can be seen as a first step to solving it. IA-Jobs and JSI-Index can be seen as first such step for the measurement of the effects of the technological revolutions in the workplace. With the contributions from the academicians and practitioners they can be revised and improved. Also, new and more powerful measurement tools may be developed.

CONCLUSION

Technological revolutions do not stop but rather accelerate. Each new technology makes old types of doing business out of the date leaving many people unemployed and unskilled. During the 20th century, the services sector including the financial services compensated the adverse affects of the technology.

However, the new breeds of technology including Information and Communication Technologies (ICT), genetics and biotechnology, and robotics among others began to threaten even the services sector. Technological capabilities compete with the human capabilities and this is a major reason for the globally rising unemployment levels. We should find ways to survive as human being against such advanced technologies. This will be an even more important issue 15-20 years later when the revolutionary new technologies offer cheap alternatives to human labor.

We are human being. Our superiority over the machines is that we can produce innovative ideas; we can record movies and music. We should concentrate in those areas that can not be performed by technology alone. To better capture our superior capabilities we defined the new category called IA Jobs. We also developed a job satisfaction index (JSI) which measures the vulnerability of a particular job in the face of technological developments.

IA-work is the distinguishing aspect of humanity. In the future most of us will work in either technology-production and implementation or IA or IA-related fields. Of course, agriculture, industry and services sectors will not totally disappear but they will not be major source of jobs. For IA sector to provide jobs for the laid-off workers from the services and industrial sectors, legal and technological progress is needed.

Both IA-job and JSI index concepts are new and needs further development. We expect contributions from both HR practitioners and academic researchers. Therefore we would highly appreciate your comments. In the future, we plan to further develop these concepts and try to find solutions to the practical problems that may arise.

REFERENCES:

Hartman, A., Sifonis J., Kador J. 2000. *Net Ready: Strategies for the Success in the e-conomy*. McGraw-Hill.

Ochoa, G. and Corey M. 2004. *The 100 Best Trends 2005: Emerging Developments You Can't Afford to Ignore!.* Avon: Adams Media,

Porter, M. 1998. *On Competition*. Harvard Business School Press.

Reich, R. B. 2001. *The Future of Success*. New York: Alfred A. Knope.

Yamamoto, G. T. and Karaman F. 2005. A Road-Map for the Development of the Content Protecting Technologies (CPT) For The Content Based E-Business Models. *The E-Business Review*, 5, 226.

INVESTIGATING A THEORETICAL FOUNDATION OF E-GOVERNMENT PERFORMANCE: AN EXPLORATORY STUDY

Assion Lawson-Body, University of North Dakota, USA
Glenn Miller, University of North Dakota, USA

ABSTRACT

MIS literature has not adequately addressed the theoretical foundation of electronic government performance. Theories from Information Systems (IS) reference disciplines are yet to be proposed to examine the theoretical foundation of electronic government performance. In this paper, we develop a theoretical framework that is a first effort toward this end. Two of these IS reference disciplines are: organizational economics and marketing. We draw upon transaction cost theory (TCT) and role theory (RT) to explore and understand the theoretical foundation of electronic government performance which is categorized into two groups, either web portal based performance or the e-government service delivery performance. In fact, we suggest the government web portal-based performance as an enhancement to TCT because using web portals may impact electronic government performance in terms of reducing service-processing costs, increasing citizen online participation, reducing in errors and amount of time saved. We build on foundational advances in RT in examining via service encounter e-government service delivery performance. A research model drawn from the theoretical framework and its implications in IS research are discussed.

1. INTRODUCTION

E-government services refers to the emerging area of information systems (IS) and information technology (IT) services that are delivered electronically (Ramesh and Tiwana, 2001). The way that government agencies design and deliver services and configure and deploy underlying information and communications technologies, is central to the performance of e-government service delivery (Wang, 2002). The Council for Excellence in Government (2001) points out that the ideas of a more knowledgeable citizenry and a government more accountable to the people have become central to U.S. citizens' current vision of e-government (Cetiner and Ryan, 2004). Clearly, this vision involves more than just delivering superior electronic government services to citizens.

To better understand how IT affects government activities, transaction cost theory (TCT) and role theory (RT) are adopted to analyze the theoretical foundation of e-government performance. TCT is probably the most widely applied theory for analyzing electronic commerce framework, ranging from conceptual to analytical and empirical studies.

Indeed, many authors like O'Looney (2003), Neef (2001; cited in Moon, 2002), Damsgaard (2002), and Chen and Perry (2003) have developed models or frameworks for analyzing e-government. Most of those electronic government frameworks are based on the representation of the government service processes. Rare is the existing research that has developed a framework dedicated to the theoretical foundation of electronic government performance. In addition, there is a lack or shortage of research based on a theoretical framework for electronic government performance in which TCT and RT play an important role.

The purpose of this paper is to examine a framework dealing with the theoretical foundation of electronic government performance that should be used in future research. We draw upon TCT and RT to explore and understand the theoretical foundation of e-government performance. In fact, we suggest the government web portal-based performance as an enhancement to TCT because using web portals may impact electronic government performance in terms of reducing service-processing costs, increasing citizen online participation, reducing in errors and amount of time saved. We build on foundational advances in RT in examining via service encounter e-government service delivery performance. We suggest a research model from the theoretical framework perspective.

This article is organized as follows: In Section 2, we present a literature review. In Section 3, we present the theoretical framework development. In Section 4, we draw a research model from the theoretical framework. In Section 5, we present conclusions and outline research implications

2. LITERATURE REVIEW

2.1. MODELS AND FRAMEWORKS OF E-GOVERNMENT

O'Looney (2003) describes the major trends and factors that are likely to lead to increase the use of the computer models, simulations, and decision support technologies (MSDST) for citizen understanding of government and citizen engagement in government.

Neef (2001; cited in Moon, 2002) developed various models of e-government procurement including the sell-side one-to-many model, buy-side one-to-many model, independent portal model, and auction model. Overall, models of e-government procurement differ based on who is the focus of the procurement system (sell-side or buy-side), who manages the electronic catalog (suppliers, buyers, or third parties), and the types of portal sites (one-to-many model or many-to-many model), among others (Neef, 2001; cited in Moon, 2002).

Damsgaard (2002) presented a model for government Internet portal management. The model is a lifecycle that contains four stages. Four competitive strategies are used as effective for steering the portal through each of the stages.

Chen and Perry (2003) outlined the process model for managing government IT outsourcing. Their project is based on five phases: determining a sourcing strategy, analyzing sourcing needs and the operational relationship, selecting a vendor and negotiating contracts, making the transition to the service provider and managing the performance of the service provider.

2.2. E-GOVERNMENT PERFORMANCE AND BUSINESS ORGANIZATION PERFORMANCE

Each year large and small businesses invest in IT to improve their business performance (Huang and Hu, 2004). The relationship between IT investments and business performance is complex and multifaceted (Huang and Hu, 2004).

In recent years, many studies have written about the resource-based view (RBV) theory to examine the IT-firm performance relationship (Ravichandran and Lertwongsatien, 2002). Many past studies in Information Systems (IS) have implicitly assumed that IS assets could have direct effects on firm performance (Ravichandran and Lertwongsatien, 2002). (Barney (1991) proposed that the RBV of a firm could help obtain competitive advantage and enhance firm performance (Santhanam and Hartono, 2003). The conventional wisdom is that IT is necessary for business survival and that the appropriate use of IT resources and capabilities leads to enhance firm performance (Lu and Ramamurthy, 2004). Widely publicized IT programs in firms such as American Airlines, Merrill-Lynch, and Frito-Lay have been associated with superior business performance (Bharadwaj, 2000). In fact, this theory based framework commonly referred to as the RBV has been adopted to address the productivity paradox, the controversy over the business value of IT investments.

While these studies posit a direct positive impact of the use of IT resource on firm performance, others have found opposing effect of the IT-performance relationship. Powell and Dent-Micallef (1997; cited in Ravichandran and Lertwongsatien, 2002) found that IT resources did not have a direct impact on firm performance. Carr (2003) found that firm financial performance rarely improves with IT spending (Lu and Ramamurthy, 2004). There is evidence that many firms, concerned about falling behind on the technology curve, engage in high IT investments without deriving any benefits from IT (Bharadwaj, 2000).

IS researchers argue that competitors may easily duplicate investments in IT resources by purchasing the same hardware, software and network, and hence resources per se do not provide sustained firm performance (Santhanam and Hartono, 2003). This also occurs because many IT investments are easily duplicated by competitors resulting in the same industry competitive situation but at an increased level of cost (Kettinger et al., 1994). Rather, it is the manner in which firms leverage their IT investment to create unique capabilities that impact a firm's overall performance (Santhanam and Hartono, 2003). Bharadwaj (2000) proposed that if firms can combine IT resources to create a unique IT capability, it can result in superior firm performance. Santhanam and Hartono, (2003) found that firms with superior IT capability indeed exhibit superior current and sustained firm performance when compared to average industry performance, even after adjusting for effects of prior firm performance. Ravichandran and Lertwongsatien, (2002) posit that variations in firm performance can be explained by how effective it is in using IT to support and enhance its core competencies. Santhanam and Hartono (2003) state that resources can be easily duplicated, but a unique set of capabilities mobilized by a firm cannot be easily duplicated and will result in increased firm performance.

According to the RBV theory, the benefits of superior IT capability must be sustainable over time (Santhanam and Hartono, 2003). Chatterjee et al., (2001) found that the impact of IT spending may not be immediately reflected in firm performance because it takes time for firms to assimilate IT and realize related performance benefits. Researchers state that IT investments are made with long-term goals and there is a time lag in obtaining benefits (Santhanam and Hartono, 2003). Anderson et al., (2003) found that to validate the link between IT spending and future firm performance, a direct analysis of the association between IT spending and future earnings must be performed. Using cross-sectional archival data, Lu and Ramamurthy (2004) found that under low environmental dynamism condition, the performance advantages of high IT capability are found to sustain over time. Demirhan et al., (2002) mentioned that the declining cost of IT over time provides improved performance.

Certain authors refer to the term "IT business value" as the "impact of IT on firm performance" and introduce mediating or moderating variables to impact the relation between IT and firm performance (Melville et al., 2004). In fact, a third variable plays the role of moderator when it partitions a focal independent variable into subgroups that establish its domains of maximal effectiveness in regard to a given dependent variable (Baron and Kenny, 1986). In general terms, a moderator is a qualitative or quantitative variable that affects the direction and/or strength of the relation between an independent or predictor variable (IT resources) and a dependent or criterion variable (firm performance) (Baron and Kenny, 1986; Chin et al., 1996). Barua et al. (1995) developed a model of IT business value in which intermediate processes play a mediating role between IT and firm performance (Melville et al., 2004). Weill (1992) identified that the impact of IT on firm performance is mediated by several conversion effectiveness factors (Melville et al., 2004). Soh and Markus (1995) mentioned that IT assets (IT conversion process) and IT impacts (IT use process) may moderate the relation between IT investment and firm performance (Melville et al., 2004). Francalanci and Galal (1998) stated that managerial choices regarding the mix of clerical, managerial, and professional employees mediate the link between IT and organizational performance (Melville et al., 2004). Melville et al., (2004) used the RBV of the firm as a theoretical foundation of an integrative model of IT business value. They tested that model and found that IT is valuable, but the extent and dimensions are dependent upon internal and external factors, including complementary organizational resources of the firm and its trading partners, as well as the macro and competitive environment. Melville et al., (2004) model showed that IT impacts firm performance through intermediate business processes. Also the model reveals that other organizational resources such as work-place practices interact with IT, whether as mediator or moderator, in the attainment of firm performance impacts.

2.3, E-GOVERNMENT SERVICE DELIVERY PERFORMANCE

Performance measurement is important to assess e-governments efforts because, in government, IT and information are public property not a proprietary resource to be protected and exploited for competitive advantage (Dufner et al., 2002). In the public sector, goals and objectives of government organizations are expressed as laws or ordinances, and government success consists of program delivery and organization performance (Dufner et al., 2003). As in the private sector, achievement of success in government organizations is dependent on IT. Research on IT in the public sector, however, indicates management and planning for IT are performed lower in the hierarchies of public organizations because performance is measured by the “bottom line” (Dufner et al., 2003). Performance measurement allows governments to track what is working and what is not and assure citizens that government’s time and funds are being well spent (Stowers, 2004). Public sector performance measures are quantitative ways of determining the resources that go into providing services, the immediate results of those services, and the longer-term results of providing those services (Stowers, 2004).

Jain (2003) found that IT investments in 1999 had a negative relationship with performance of the states in 1999 in each of the performance dimension, such as financial management, human resource management, information technology management, capital management, and managing for results. The same author also found a positive relationship between IT investments and projected state budget deficits in 2003 and 2004. Finally, Jain (2003) found that the more U.S. state governments invest in IT, the worse they perform. However there are also indications that as time goes on, the relationship between IT investment and performance shows improvements in the public sector.

Many authors have also examined how governments can invest in e-commerce to improve their service delivery performance (Dufner et al., 2002; Jain, 2004). After conducting six case studies and contacting over 50 government organizations, Cohen and Eimicke, (2001) found that e-government service delivery could change human resource deployment patterns and improve organizational performance. Another source of e-government service delivery performance is savings generated from reduced costs. When costs were assessed in the cases presented in their study, Cohen and Eimicke (2001) found that typically services delivered over the Internet were less expensive to deliver than those delivered in person. The resulting cost savings in electronic service delivery can be significant. Many valuable internal services may be made available to citizens, thus creating new revenue streams. Allowing and facilitating customer access to crucial service information using web portal would be an important draw to attract customers, while the linkage itself can serve as a switching cost to prevent customers from moving to competitors services.

Although some important work has been undertaken, the IT (Internet)-government service delivery performance relations are not adequately represented in current IS research. This study is a first effort toward this end.

3. THEORETICAL FRAMEWORK DEVELOPMENT

Several theoretical perspectives from IS reference disciplines are relevant for this study. Two of these perspectives are organization economics and marketing. We draw upon TCT to explore the theoretical foundation of government web portals and RT to understand the theoretical foundation of e-government service delivery. E-government performance is well balanced between government web portals and e-government service delivery.

3.1. TRANSACTION COST THEORY (TCT)

The TCT, pioneered by Coase (1937) and developed principally by Williamson (1975, 1985a, 1996a), posits that there are costs in using a market (Wang, 2002). These costs include operational costs and contractual costs (Wang, 2002). Although the organization of economic activities depends on balancing production economics against the costs of transacting, the paradigmatic question of the theory is the use of electronic media (Internet) to decrease the transaction costs. This eases the decision making process, in which economizing of transaction cost is central (Wang, 2002).

3.2. E-GOVERNMENT WEB PORTAL AND TCT

For the past decade, organizational economics has been an important reference discipline for IS research (Aubert et al., 1994). Indeed, TCT has been used extensively in interpreting inter-organizational systems (IOS) (Malone et al., 1987; Grover et al., 2002). These various applications of organization economics demonstrate the explanatory power of the theory (Aubert et al., 1994) and are particularly relevant for this study. Malone et al., (1987) used the TCT to study the impact of IT on the choice between the firm and the market. They found that IT reduces communication costs and encourages the migration of economic activities from the firm to the market (Aubert et al., 1994). Therefore, Malone et al, (1987) were among the first to link TCT to IOS, illustrating how electronic networks can lower the costs of transactions (Sarkar et al., 1995).

Following Malone et al., (1987) in the way they looked at IOS and Internet through TCT, one of our goals was to understand the use of a web portal in government performance through TCT. The foregoing analysis suggests the need to augment TCT for IS research on e-government. Therefore we used government web portals to enhance TCT. The government is finding that the web portals can provide considerable value at a lower cost and with more efficiency than traditional methods. Delivery via web portals gives government agencies the ability to control the consistency and quality of information and services. As web portals continue their rapid cost performance improvement, government agencies will continue to find incentives to coordinate their activities electronically.

When transaction costs, service-processing costs, error made costs and time costs reach a certain level, the transaction is not profitable to the government agencies. According to TCT, web portals may be used to decrease these costs and specifically transaction costs between government agencies and their constituents.

3.3. AN OVERVIEW OF ROLE THEORY

In exploring e-government service delivery, we adopt RT from marketing. This theory has been adopted by MIS and marketing researchers for examining service encounters. A service encounter is a form of social exchange in which participants normally seek to maximize the rewards and minimize the costs of the transaction (Solomon et al., 1985).

RT is based on a dramaturgical metaphor (Solomon et al., 1985). It is the study of the conduct associated with certain socially defined positions rather than of the particular individuals who occupy these positions (Solomon et al., 1985). A role theoretic approach emphasizes the nature of people as social actors who learn behaviors appropriate to the positions they occupy in society (Solomon et al., 1985). A role is the behavior associated with a socially defined position and role expectations are the standards for role behavior. Each role that one plays is learned (Solomon et al., 1985).

In many routine service encounters, the roles are well defined and both the customer and employee know what to expect from each other (Bitner, 1995). The recipient of the service also plays a role. The recipient role is composed of a set of learned behaviors and a repertoire of roles (Solomon et al., 1985).

3.3.1. ROLE THEORY, SERVICE ENCOUNTER AND E-GOVERNMENT SERVICE DELIVERY PERFORMANCE

Following Bitner (1995) and Solomon et al., (1985), we draw upon RT and service encounter to theoretically explain e-government service delivery.

According to RT, each participant in government service delivery has a role to play. A role theoretic approach in the setting of e-government is based upon the nature of government employees who play the role of actors and learn behaviors appropriate to the positions they occupy in the government structure. Successful relations and interactions between government employees and citizens or businesses are critical to government service delivery effectiveness. Internet-enabled communication technologies have the potential to enable significant improvements in the quality of government service delivery. Through the lens of role theory, government employee and citizens' or businesses' role in these relations are well defined and both know what to expect from each other. The Role theory also helps understand that each role that one plays is learned.

3.4. PRESENTATION OF THE FRAMEWORK

In figure 1, the IS reference disciplines are comprised of the organizational economic theory and marketing theory. TCT and RT are elements of the organizational economic theory and marketing theory, respectively. RT has been used to explain the service encounter. The framework proceeds to explain the link between RT and the service encounter and concludes that in many routine service encounters, the roles of both the customer and service provider are well defined and each of them knows and learns how to behave in order to reciprocally benefit from the encounter.

Since the service encounter is influenced by dyadic interactions in the marketplace and many pure service situations are characterized by interactions between service provider and customer, it plays via RT the role of a theoretical foundation for government service performance. E-government is a means to improve the quality of the interactions during service delivery and pure service exchange between government agencies and citizens or businesses. E-government service delivery performance is measured by the amount of time saved. E-government service delivery relieves government employees of having to perform many repetitive, yet critical time-sensitive tasks, thereby freeing them to support other strategic activities.

TCT is a theoretical foundation of inter-organizational information systems (IOS), which in turn are a theoretical foundation of electronic commerce and the government web portal. The least costly form of e-government is at one hand to put existing services online; at the other to create a mega-portal. E-government typically reduces costs and conveniences for citizens and businesses. According to TCT, the use of web portals may decrease transactions costs of government procurement. E-government may cut procurement expenditures by aggregating procurement and putting it on-line. If e-government uses web portals it can achieve commensurate economies. Those saving strategies explain why e-government efforts have focused first on procurement and only later on interactions with the public.

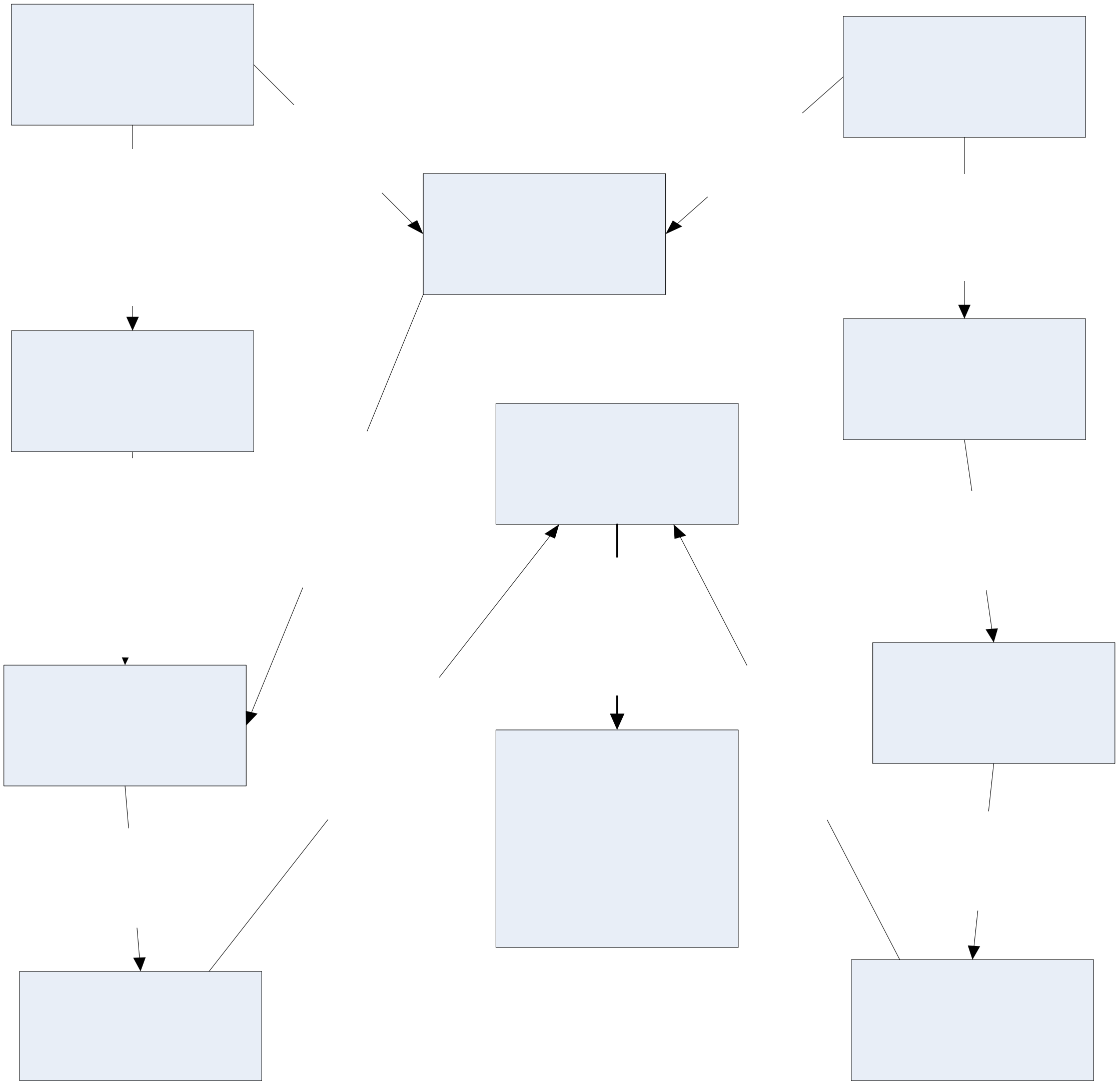


Figure 1: Theoretical framework for understanding e-government performance

4. RESEARCH MODEL AND PROPOSITIONS DRAWN FROM THE THEORETICAL FRAMEWORK

The key constructs of the proposed research model, identified through the objective and the theoretical framework for understanding e-government performance are as follows: the dependent variable will be drawn from e-government service delivery performance construct and the independent variables will be drawn from the government service management (GSM).

4.1 GSM CONSTRUCT COMPONENTS

In this study, a GSM is defined as the process whereby citizen service representatives understand citizen expectations, teach citizens ways to secure services for themselves, develops partnerships of service, and cooperation with government agencies in order to serve citizens (Moon, 2002). The extent of GSM is split in two in this research: eGSM from G2G perspective (G2GSM) and eGSM from G2C perspective (G2CSM). The two major G2GSM components identified are: cooperation and partnerships of service. The two major G2CSM components identified are: empowerment of citizen and understanding citizen expectations. We hope to investigate into eGSM factors influencing e-government service delivery performance.

4.1.1 ONLINE COOPERATION

Cooperation is defined in this study as coordinated actions taken by government agencies, citizen service providers, and citizen service representatives to achieve mutual outcomes. Cooperation promotes effective working relationship success. A government agency committed to the relationship will cooperate with citizen service representatives because of a desire to make the relationship work. The interaction of cooperation results in cooperative behavior, allowing the relationship to work by ensuring that both parties receive the benefits of the relationship. Citizen service representatives know that coordinated efforts will lead to outcomes that exceed what the citizen service representatives would achieve if it acted solely in its own best interests. Wilson (1995) presented a cooperative model in which both parties achieve lower costs by working together to lower both buyer's and seller's operating costs. This enduring desire to maintain a valued cooperative relationship should, in turn, impact e-government service delivery performance. Performance management is the central theme of the working relationship between citizen service provider and citizen service representatives. Both need to cooperate so they can update each other in an ongoing effort to improve services delivery performance or jointly resolve service delivery concerns (Moon, 2002). Thus we propose the proposition below:

Proposition 1: Online cooperation will have a positive effect on government service delivery performance

4.2.2. ONLINE PARTNERSHIP OF SERVICE

Partnerships are created when citizen service representatives communicate and share information closely with citizen service providers or government agencies. This means refurnishing of information to citizen service provider and government agency's services by citizen service representatives. It also means joint development of services with citizen service providers or government agencies. To get effective partnership with citizen service providers, some citizen service representatives refer to other citizen's services when they offer service to citizens.

In the management of service delivery, frequent quality communication needs to be in place to foster partnerships and cope with changing services needs (Moon, 2002). Partnering with the government agencies is among the broad spectrum of citizen retention tactics and government service delivery performance. Tight collaboration and sharing of information with government agencies enhance e-government service delivery performance.

A partnership helps both parties stay on the course of mutual interests (Moon, 2002). Given the possible disparity between citizen service providers and citizen service representatives regarding specific knowledge about e-service delivery, citizen service provider organizations need to rely on citizen service representatives to be forthcoming about potential problems or better service deliveries. In this case, an online partnership can go a long way and impacts on e-government service delivery performance. Accordingly, it is proposed that:

Proposition 2: Online partnerships of service will have a positive effect on government service delivery performance.

4.2.3. ONLINE EMPOWERMENT OF CITIZENS

Empowerment of citizen generally refers to the process government agencies adopt to educate, teach, encourage and reward citizens who exercise initiative and make valuable creative contributions or do everything that is possible to help themselves solving their problems. Most citizen service representatives prefer to deal with empowered citizens because they are easy to serve, because they understand the government's preoccupations, and because they make only a few requests to citizen service representatives. So, it is proposed that:

Proposition 3: Online empowerment of citizens will have a positive effect on government service delivery performance.

4.2.4. UNDERSTANDING CITIZEN EXPECTATIONS

This concept stresses the importance of citizen service representatives' having the ability to identify their citizens' desires and to deliver to those citizens services which meet their expectation. Understanding citizen expectations is a strategy adopted by citizen service representatives to generate more knowledge of citizen expectations and needs and to provide citizens with the best services.

Governments must continually improve citizen service representative skills for better understanding citizen expectations. E-government emphasizes delivering information and services in ways that better reflect what people need or want from government, and are less constrained by how government agencies are structured. citizen service representatives need to be able to satisfy citizen' specific requirements in order to increase the perceived value that citizen receive from the transactions in order to increase e-government service delivery performance. Therefore we posit:

Proposition 4: Online understanding citizen expectations will have a positive effect on government service delivery performance.

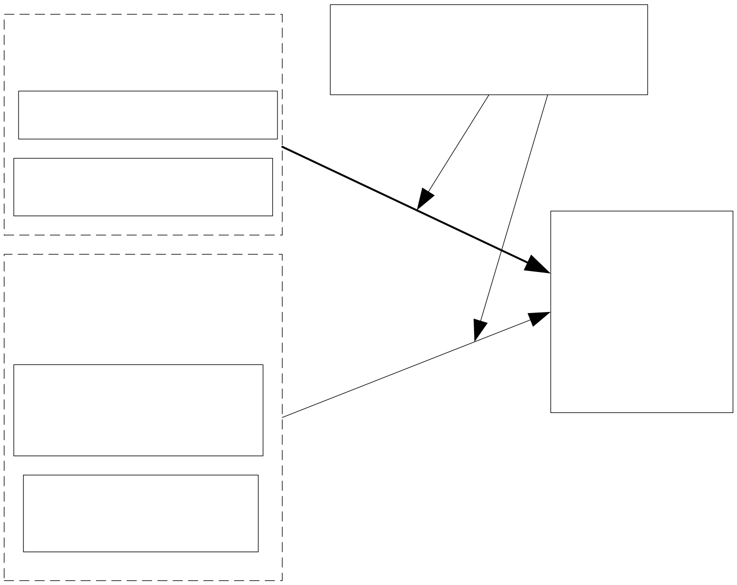


Figure 2. Research Model

5. CONCLUSION

The paper presents a theoretical discussion of how experts in the IS field and e-government should inform governments and researchers about the theoretical foundation of e-government performance. These experts have to show governments reliable methods of fixing e-government service delivery performance that involve increasing the level of cooperation, partnership, empowerment and understanding citizen expectations when using web site dedicated to citizens. Its objective is to examine a framework dealing with two dimensions of e-government performance, such as web portal-based performance and e-government service delivery performance.

In fact, we used the Internet's web portal-based performance to enhance TCT. Government web portals allow government agencies, citizens, businesses and other government constituents to access all government services and activities from a single interface. Such a portal may offer government greater convenience and give invaluable saving cost opportunities. Governments may save cost on every transaction completed on the portal.

Regarding the theoretical contribution of this study, it is important to point out its originality because it facilitates the development of a new research model, which will help future research.

The use of the RBV of the firm theory to explain the IT-firm performance relationship and to build the theoretical foundation of e-government service delivery performance is another distinctive element of this research. The combination of RT and service encounter theory to explain GSM, and to demonstrate how those theories can be applied to a research project in the public sector constitutes a further contribution of this study.

We built on advances in RT to establish e-government service delivery and discuss its theoretical impact on e-government performance. The successful e-government service delivery depends on the contribution of its participants in terms of role, learning and behavior. When participants to e-government service delivery know very well their role, e-government performance will benefit from that.

5.1. RESEARCH IMPLICATIONS

A multitude of research questions exist about the theoretical foundation of electronic government performance. The framework and the research model presented here give one way to organize thoughts about such questions.

Another way of identifying and characterizing potential research is to consider the implications and problems that the e-government performance present to each of the traditional fields of business and IS.

Clearly, there is much uncertainty in the emerging world of electronic government. This uncertainty spans a variety of areas: marketing, political science, public administration, organizational economics, and technology. All participants in the IS research community need to wake up to, understand, and adapt to the theoretical foundation of electronic government performance. They need to redefine their research philosophies and approaches.

Many exciting research issues are being addressed and some are yet to be addressed and we hope that this paper inspires others to do future research by drawing concepts or variables from this framework. Researchers should need this framework to categorize electronic government dimensions so that hypotheses and theories can be tested meaningfully.

Finally, this research facilitates the development of a new framework of electronic government and a new research model. Further research is needed because this theoretical and conceptual study needs to be tested. In fact, empirical research based upon this study is necessary. Future research will also be important because Internet technology evolves so rapidly. Topics that deserve further exploration are: longitudinal studies with government agency panels, comparative studies on the effectiveness of the Internet's web portals and electronic government applications across various categories of citizens, customers, businesses, products, and industries.

REFERENCES

Adelaar, T. (2000). Electronic commerce and the implications for market structure: The example of the art and antiques trade. Journal of Computer-Mediated Communication [On-line], 5 (3). http://www.ascusc.org/jcmc/vol5/issue3/adelaar.htm

Anderson, M, Banker, R. D., and Hu Nan (2003) The impact of IT spending on future performance, Twenty-Fourth International Conference on Information Systems. pp. 563-575.

Aubert, B., S. Rivard and M. Patry (1994) "Development of Measures to Assess Dimensions of IS Operation Transactions ", ICIS, Vancouver, December 14-17, pp.13-26.

Baron, R. M. and D. A. Kenny (1986) "The moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic and Statistical Considerations", Journal of Personality and Social Psychology, (51)6, pp.1173-1182.

Bharadwaj, A, S, (2000) A Resource-Based Perspective on IT Capability and Firm Performance: An Empirical Investigation, MIS Quarterly, Vol 24, No 1, pp. 169-196.

Bitner, J. M. (1995). Building Service Relationships: It's All About Promises. Journal of Academy of Marketing Science. (23)4, 246-251.

Chatterjee, D., Richardson, V., and Zmud, R. (2001) Examining the shareholder wealth effects of new CIO position announcements, MIS Quarterly, (25:1) pp. 43-70.

Cetiner, M. and Ryan, T. 2004. How to improve the usability of government web sites. Proceedings of the Seventh Conference of the Southern Association for Information Systems. 1(1), 65-68.

Chen, Y-C and Perry, J., (2003). IT Outsourcing: A primer for public managers. E-Government Series, 1-36. Grant Report, The PricewaterhouseCoopers Endowment for The Business of Government. http://www.businessofgovernment.org/main/winners/area/index.asp

Cohen, S., & Eimicke, W., (2001). The Use of the Internet in Government Service Delivery. E-Government Series, 1-36.

Damsgaard, J. 2002. Managing an Internet Portal. Communications of the Association for Information Systems, 8(9), 408-420.

Demirhan, D., Jacob, V. S. and Raghunathan, S. (2002), Strategic IT investments: Impacts of Switching Cost and Declining Technology Cost. Twenty-Third International Conference on Information Systems. pp. 469-480.

Dufner, D., Holley, L., & Reed, B. (2002). Can private sector strategic information systems planning techniques work for the public sector? Communications of the Association for Information Systems, 8(27), 413-431.

Grover, V., J. T. C. Teng and K. D. Fiedler (2002) "Investigating the Role of Information Technology in Building Buyer-Supplier Relationships", Journal of the Association for Information Systems, (3)1, pp.217-245.

Huang, D. C, & Hu, Q. (2004). Integrating web services with competitive strategies : The balanced Scorecard approach. Communications of the Association for Information Systems, 1(13), 57-80.

Jain, A., (2003) Performance Paradox: IT investments and Administrative Performance in the case of the 50 US state governments, Twenty-Fourth International Conference on Information Systems. pp. 389-400.

Kettinger, W. J., Grover, V., Guha, S. and Segars, A. H. (1994), Strategic Information Systems Revisited: A study in sustainability and performance, MIS Quarterly, (March) pp. 31-58.

Lu, Ying and Ramamurthy, K. (2004), Does IT always lead to better firm performance? The role of environmental dynamism. Twenty-Fifth International Conference on Information Systems. pp. 249-262.

Malone R. W., J. Yates and R. I. Benjamin (1987) “Electronic Markets and Electronic Hierarchies”, Communications of the ACM, (June 1987), pp. 484-497.

Melville, N., Kraemer, K., and Gurbaxani, V., (2004), Review: IT and organizational performance: An integrative model of IT business value. MIS Quaterly, Vol. 28, No. 2, pp. 283-322.

Moon, M. J. (2002). State Government E-Procurement in the Information Age: Issues, Practices, and Trends. E-Government Series, 1-65. Grant Report, The PricewaterhouseCoopers Endowment for The Business of Government. http://www.businessofgovernment.org/main/winners/area/index.asp

O’Looney, J. (2003). Using technology to increase citizen participation in government : the Use of models and simulation, E-Government Series, 1-59. Grant Report, The PricewaterhouseCoopers Endowment for The Business of Government. http://www.businessofgovernment.org/main/winners/area/index.asp

Ramesh, B. and Tiwana A. (2001) “e-Services: Models and Methods for Design, Implementation, and Delivery” Proceedings of the 34th Hawaii International Conference on System Sciences, 1 page.

Ravichandran, T. and Lertwongsatien, C. (2002). Impact of IS resources and capabilities on firm performance: a resource-based perspective, Twenty-Third International Conference on Information Systems. pp. 577-582.

Santhanam, R. and Hartono, E. (2003) Issues in Linking Information Technology Capability to Firm Performance, MIS Quaterly, Vol. 27, No. 1, pp. 125-153.

Sarkar, M.B., B. Butler, and C. Steinfield (1995) “Intermediaries and cybermediaries: A continuing role for mediating players in the electronic marketplace,“ Journal of Computer-Mediated Communication [On-line], (3)1. Available: http://www.ascusc.org/jcmc/vol1/issue3/sarkar.html

Stowers, G. N. (2004). Measuring the Performance of E-Government. E-Government Series, 1-52.

Solomon, M. R., Carol, F., Surprenant, J. A., Evelyn G. G., (1985). A role theory perspective on dyadic Interactions : the service encounter, Journal of marketing, 49(1), 99-111.

Wang, E. T. G. (2002). Transaction attributes and software outsourcing success: an empirical investigation of transaction cost theory. Information Systems Journal, 12, 153-181.

Wilson, T. D. (1995). An Integrated Model of Buyer-Seller. Journal of Academy of Marketing Science, 23(4), 335-345.