CERIAS Tech Report 2000-11

Fighting the Wily Hacker: Modeling Information Security Issues for On-line Financial Institutions using the SEAS Environment

Alok Chaturvedi[1], Mukul Gupta[1], Shailendra Mehta[1], Lorenzo Valeri[2]
Center for Education and Research in
Information Assurance and Security
&
[1]Krannert School of Management, Purdue University
West Lafayette, IN 47907
[2]International Centre for Security Analysis,
Kings College London, United Kingdom

Paper To Be Presented at
I.NET 2000
The Annual Meeting of the Internet Society
July 18th-21st, 2000
Yokohama, Japan

Table of Contents

The Explosion of the Internet and the Rise of New Security Threats

The Internet is radically transforming the provision of services and goods because of its immediacy, openness, ubiquity and global reach. The financial and banking industry has not been aloof from the Internet but has fully embraced its new potentialities as demonstrated by a variegated set of new financial services offered to clients at competitive costs. This development, nevertheless, represents just the start an overall evolution which is expected to embrace the whole financial industry in the years to come as convergence between information and telecommunication services and new regulations and laws like the 1999 *US Financial Services Modification Act* deliver the expected benefits. However, leveraging the Internet to increase revenues and profits while lowering costs does not come without new threats and risks. The Internet, in fact, is also becoming the venue for a new set of illegal activities.

According to the Information Security Magazine, since 1998 about twenty percent of the surveyed financial institutions have suffered disruptions of their information and network systems.[1] Similar findings have been confirmed by the 1999 Computer Crime and Security Survey conducted by San Francisco-based Computer Security Institute and the Computer Intrusion Squad of the US Federal Bureau of Investigation. This initiative highlighted that more than 50 percent of the surveyed companies had their networks violated through their Internet connection.[2] Nonetheless, the most troublesome aspect of this rise on computer crime is its global reach, especially for an on-line financial institution that aims to offer its products and services to clients worldwide. In the final report of the Project Trawler, the National Criminal Intelligence Service, the central intelligence body of the various English regional police forces, has indicated an exponential growth of computer crime in the United Kingdom.[3]

The perpetrators of these security breaches may be classified in two categories: external agents and insiders. External actors refer to individuals or groups like hackers, terrorist organizations, business competitors and foreign intelligence organizations.[4] These agents perceive Internet ubiquity and anonymity as advantageous features for accomplishing their strategic and political objectives. The term "insiders" indicates those authorized users who take advantage of their authorized access to internal networks and the Internet in general to achieve personal objectives. According to the Information Security Magazine, more than half of the interviewed organizations have experienced abuses from their employee or authorized users. According to the consultancy firms Political Psychology Associates, this high number of misuses may be related to personal frustrations, computer dependency reduced loyalty to employers as well as perceived lack of financial entailment for supposed superior technical and managerial capabilities. [5]

These harmful activities would not cause any specific concern to on-line financial institutions if they were not to hamper one of the pivotal elements for the success of any on-line activity: the conquest and maintenance over the Internet of customers' trust. Users, in fact, develop trust on specific vendors and service providers, like on-line

financial institutions, when they have confidence on their overall reliability and integrity.[6] Therefore, countering these new threats represents a central strategic issue for business development, revenue increase and, where applicable, shareholder value because of the centrality of customer retention and management in an e-commerce environment. This aspect has been recently confirmed by the 1999 WWW User's Survey carried out by the Graphic Visualization and Usability Center of Georgia Technology University. It highlighted that more than 50 percent of Internet users are concerned with on-line security and reliability. The situation does not differ in case of on-line banking activities since the same survey indicates that more than two third of Internet users would no bank with financial institutions that do not provide a detailed security statement. It is important to stress that these data do not change if referred to a gender, age group, on-line individual experience and geographical origins. [7]

Information security, therefore, is a pivotal business and technical undertaking for any company involved on on-line financial activities. Because of the sensitivity of their activities, financial institutions have always focused on the overall security of their activities and operations. Moreover, government institutions have devised new regulations or updated previous ones. In an on-line financial environment, nevertheless, the notion of information security cannot be restricted to issues of availability, confidentiality and integrity of both networks and data transferred or held inside them. It involves also issues connected to authentication and non-repudiation in dealing with new and acquired customers in a digital environment. Actually, in an Internet environment, these five elements (availability, integrity, confidentiality, authentication and non-repudiation) have a dependency relationship among themselves. Thus, devising a managerial and technical policy to satisfy them and, as a direct consequence, acquire or maintain customers' trust may prove a complicated and financially cumbersome for any on-line financial institutions.

Objective of the Proposed Study

The purpose of this essay is to introduce the methodological undertakings of an on-going experimental study concerning possible offensive and defensive strategies to counter the multiple risks facing on-line financial institutions. These experiments are going carried out through the Synthetic Environment For Simulation and Analysis (SEAS) environment devised by the Krannert School of Management at Purdue University in the forthcoming months. This paper introduces the overall structure together with the initial assumptions, objectives and hypothesis.

SEAS emulates the US Department of Defense's "War Gaming" paradigm in business and economic settings. It is the application of computer generated modeling techniques, hero-to-fore use to create virtual realities to set up virtual economies. Specifically, SEAS allows for the creation of situation-specific economies through mathematical rule-sets derived from theoretical and empirical work. The goal is to permit scale controlled experiments where human and synthetic players can play together. In the context of the on-line financial businesses and information security, the experiment involves the

establishment of a specific synthetic environment involving three major players: financial institutions, offensive agents such as hackers and terrorists, and customers. These agents are expected to interact among themselves and aim to achieve specific objectives and roles. These interactions center on a set of rules of engagement and specific environmental variables regulating interactions among the agents. Therefore, in order to define these rules and variables, it is pivotal to understand the business and commercial environment, as well as risk scenarios, of on-line financial institutions.

The Internet and Financial Institutions: a business overview

In 1996, Morgan Stanley Dean Witter indicated financial services as the sector that would be most profoundly influenced by Internet since their service distribution does not require any physical exchange of goods. Nevertheless, the financial services industry is no stranger to developments such as dis-intermediation, product developments and strategic alliances.[8] The Internet, therefore, is not creating new solutions but rather accelerating established trends. Acquiring new customers, determining the correct products and services mix and distribution strategy while generating profits are still the main goals of any successful financial services company[9]. As the next statistics seem to indicate, on-line financial companies are rapidly moving away from a mere informative Internet presence while embracing a fully transactional approach where customers directly interact with the internal networks of financial institutions.

In their report Internet and Financial Services, Morgan Stanley Dean Witter has projected a compound annual growth of at least 34% for consumer financial services delivered over the Internet in the next four years. They have also estimated that U.S. consumer financial services business conducted over the Internet is expected to grow more than $435 billion in revenues by 2003 from a present $103 billion. This estimate includes consumer banking, brokerage services, auto insurance, term life insurance, and credit card interchange fees.[10] In terms of households penetration, Online Banking Report has affirmed that, while it took nearly fifteen years to achieve a mere 1% penetration rate of U.S. households in 1996, the figure now has rapidly climbed to 4% to 4.5% in last 18 months. Banking and bill payment usages is expected to increase by 4-5 million households yearly, reaching 22 million (+/- 4 million) by 2001. Afterwards, the growth will continue at a slower rate reaching 42 million (+/- 8 million) by 2010[11]. Morgan Stanley Dean Writer predicts that e-commerce will increase credit card industry charge volume from an annual 11% growth rate by 2004. Similar developments are predicted also for on-line stock brokering which is at the moment attracting most of the media and academic interests.

The statistics presented in the previous paragraphs refers mainly to established financial institutions, such as American Express, BankOne or Citigroup, which have branched over the Internet many of their operations to exploit the favorable customer demographics of the regular Internet users. Moreover, some of these institutions are using their on-line presence to also advertise and sell non-financial services like travel packages,

entertainment tickets, news and even Internet access. Nonetheless, the overall growth of the on-line financial industry is also connected to the appearance of innovative services such as *financial vertical portals, aggregators and specialty manufacturers*.

Vertical portals are websites that distribute information and multiple financial, while allowing to execute certain transactions such as bill payment. The success of these commercial ventures is mostly connected to their capacity to develop an open architecture while providing diverse services and establishing strong alliances and partnerships. Different from vertical portals, *aggregators* are destinations websites where it is possible to compare products like mortgages or insurance or even buying specific financial products. *Specialty manufacturers*, finally, are companies with best-of-breed suppliers to the main Internet distribution points such as aggregators or vertical portals.

On-line financial institutions are expected to face a growing set of risks due to their Internet reliance. The assessment of both risks and potential threats is a necessary step for the drafting of the rules of these experiments about information security techniques and management.

On-line Financial Institutions and Potential Risks: a Classification

The goal of this section is to provide a general overview of the potential risks faced by on-line financial institutions. This classification and definition is loosely extrapolated from the overall approach recently introduced by the Office of Comptroller of Currency Administrator of National Banks of the US Department of Treasury (OCC).[12] According to the OCC, risk is defined as "the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital". Overall, earnings and capital are directly related to the constant availability of advanced services and goods, and the simultaneous maintenance of a stable customer base while conquering new consumers. As mentioned before, the Internet provides new solutions to achieve these objectives but it creates a new set of vulnerabilities that may undermine the accomplishment of these goals.

These risks can be classified in two categories:

- *Overall risks*
- *Industry-related transactional risks.*

The first category includes those risks that any organization involved in Internet activities is expected to face. The second set, instead, indicates risks that are specifically related to the user' transactions with their on-line financial institutions. Between these two categories there is a direct correlation since the negative exploitation of each one of these risks by an external actors like an hacker or a disgruntled employee is expected to undermine the trust of legitimate users on that specific on-line financial institutions and, indirectly, the overall industry.

Overall Risks

This category refers to two equally important risks faced by on-line financial institutions:

- *Strategic risk*
- *Reputation risk.*

Strategic risk is the potential impact of adverse business decisions, improper implementation of decisions or lack of responsiveness to technological, commercial and legal changes involving the financial world. *Reputation risks* describe potential negative consequences originating from the disapproving customers or overall public opinion. It is possible to see a direct relationship between the two risks since a reputation loss may hamper a business plan that focuses on a high rate of customers' retention and trust. If network external intrusions and internal misuses continue, users may loose their trust in that particular on-line financial activity and moving to the competition because of the relatively low switching costs provided by the Internet.

Industry-related Transaction Risks

In the specific context of the on-line financial industry, the OCC indicates the following risks:

- *Credit Risks*
- *Liquidity Risks*
- *Interest Rate Risks*
- *Price Risks*
- *Foreign Exchange Risks*

Credit risks indicate the possibility of an obligator, either an individual or commercial clients, to fail to meet those contractual terms undertaken with a given financial institutions such as the repayment of a mortgage approved on-line. Therefore, in order to avoid this eventuality, it is necessary to develop specific procedures to authenticate users and collect the necessary information directly through the Internet. The *liquidity risk*, on the other hand, indicates the opposite situation since it refers to the inability of a given financial institution to meet its advertised or already undertaken obligations towards customers. An example in this case would be the case of an on-line financial institution that advertises 24X7X365 service operations that are undermined by malicious activities by hackers, business competitors or disgruntled employee. Changes in interest rates are also a possible source of risk (*interest rate risks*) since on-line financial institutions may fail to adjust to these changes accordingly and, therefore, suffer either additional costs or immediate dissatisfaction among present and potential customers. *Price risks* refer to potential losses of earnings and capitals originating from value changes involving traded portfolios of financial instruments like equities, foreign exchange or commodities. Finally, *foreign exchange risks* indicate the hazards of loans or other financial products that are directly managed on-line but are denominated in a foreign currency or funded

through borrowings in another currency. In last case, the main threats may originate from failure to adapt to rate fluctuations and as well as regulatory charges involving transactions with citizens from countries facing economic sanctions such as Iraq or the Republic of Serbia at this moment. The anonymity of the Internet may enhance the possibility of the violations of the strict regulations issues by the US Office of Foreign Asset Control or similar bodies in other countries. Therefore, there is a compelling need to develop specific authentication and non-repudiation procedures to avoid similar scenarios and, indirectly, hamper customers' trust on specific on-line financial institutions and the industry in general.

Technical and Managerial Information Security Policies: A Pivotal Requirements for On-line Financial Institutions

The previous paragraphs have provided a classification of potential risks faced by on-line financial institutions and the related need for an effective and efficient information security policy to maintain customers' trust. However, developing and maintain such a policy may prove extremely complex since it involves not only technical concerns but also managerial procedures that need to keep up with the constant evolution of Internet technologies and solutions. As mentioned at the beginning of this paper, the proposed experimental study based on the SEAS environment aims to aid in this "quest".

Technical information security may be defined as the combination of technical solutions that allow integrity, availability and confidentiality of data, information exchanges and Internet-based transactions. Although it is not an exhaustive lists, in the context of this experiment this non-exhaustive list of technical solutions has been taken into consideration: anti-virus software, firewalls, intrusion detection systems, user identification and authentication and public key infrastructure.

User identification and authentication represents the first line of defense against possible intrusions or internal violations. Technology in this domain has made significant improvements in the last years moving away from the username-and-password-only approach to encompass new solutions such as smart cards, tokens and biometrics. User identification systems, nevertheless, may be easily overcome by any skilled intruders or authorized disgruntled employee. Consequently, there is the need for solutions that control and monitor overall access to organizations' networks according to pre-defined security policies. In this context, firewalls and intrusion detection systems are two options. Firewalls delimit access to organizations' networks to authorized users while shunning off potential offenders. Moreover, they also restrict access to internal and external users to access specific portion of internal databases. Differently from firewalls, intrusion detection systems are information security tools that monitor network traffic to spot anomalies and misuses. There are two categories of intrusion detection systems: anomaly detection and misuse detection. The former monitors network traffic and flags possible anomalies in relation to the regular utilization behavior of a single or group of users. A competent example is the repeated access outside normal business hours of an organization's network that is usually accessed only during the day. Misuse intrusion

detection systems, instead, seek specific signs of internal or external misuses in the network traffic.

Information security policy is also expected to develop authentication and non-repudiation capabilities. Both issues can be tackled through the implementation of public key infrastructures (PKIs). They enable to achieve these objectives by establishing and managing the identities and trust relationships of parties during an electronic interchange. PKIs essentially create so called digital "handshake" through digital certificates. Encryption solutions, finally, allow for data and privacy protection by transforming any plain information in incomprehensible text. The recovery of the original text is accomplished by using an unscrambling key.

Although the market presents multiple technical solutions for information security, the protection of an organization's networks or data relies involves appropriate *management procedures*. One of the main managerial information security issues is the balance between openness and closeness. Managers need to weigh up how much information should be provided to users and the level of power the same user has to modify or change that same information. This last concern relates to problems of opting between a highly secure system and an insecure one but backed by disaster management and contingency planning procedures. Finally, whatever option is finally selected, management has to appreciate the fact that this choice is not definitive but needs to be dynamic enough to counter new threats and vulnerabilities. The PFIRES project suggests that managers consider information security management as a "lifecycle" which involves four repetitive stages:

- *Assessment*
- *Planning*
- *Delivery*
- *Operation*[13]

Assessment indicates possible changes or options against existing policies and technical environments to counter on-line related risks and threat. The outcome of this assessment should be a new management policy document in conjunction with an improved communication strategy and risk assessment procedure. Afterwards, the changes have to be implemented by updating policies and defining new requirements for these variations. This phase can be defined as *planning* and anticipate the *delivery* stage when the new security policy is actually put into action in relation to the overall security technical architecture. After the delivery of the new information security policy, management is expected to operate it while scrutinizing that every new control has been put into place to secure the organizations as well react to possible unexpected incidents or illegal intrusions. Nevertheless, the operative stage is not the final passage. In fact, any security policy needs to be constantly updated by going through the assessment stage again. The "life cycle" has to start again.

Information security requires the combination of technical resources and management procedures. The objective is to achieve a specific balance provide the necessary

protection against the various Internet-related risks. This experiment hopes to assist in this "information security maze".

Structure of the proposed experiment

The financial section of this paper introduces the artificial on-line financial institutions in the SEAS environment devised at Krannert School of Management at Purdue University. The strategy is to model the major players in the operation of on-line financial institutions into the synthetic environment, identify the relationships and transactions between these players, and build these interactions into the model. The experiments would be initially conducted using students from the business schools as subjects. The data and information collected would be utilized to analyze the impacts of the model parameters on the performance of the on-line financial institutions. Before tackling with an in-depth description of the game, it is necessary to introduce the assumption and specific objective of this game.

Assumptions, Objectives and Hypothesis

While devising this experimental game, the following assumptions have been taken into consideration while devising this experiment:

- Networks and information technologies are always vulnerable to intrusions;
- What it considered to be "secure" today won't be in tomorrow since a new vulnerability has been probably discovered and taken advantage of;
- New financial products and solutions required new functionalities and create new complexities in technical and management procedures to protect networks.

By taking into consideration these assumptions, this SEAS-empowered experimental game wants to achieve these four distinctive objectives while testing these hypotheses

- **First Objective**: the assessment of the optimal investment in security technologies and management to achieve or support business strategies and objective;
  First Hypothesis: maximum investment in security does not always result in maximum benefit for the on-line financial institutions.

- **Second Objective**: the testing of behavioral patterns in case of security breaches;
  Second Hypothesis: on-line financial institutions without properly defined information security policy have uncoordinated responses when facing security breaches while companies with well-defined technical and managerial security policies have more efficient and controlled reaction.

- **Third Objective**: the appraisal of the impact of government and industry-supported requirements for enhancing information security through controlled experiments;
  Third Hypothesis: New government and industry-sponsored security technology and management procedures (UK British Standard 7799, Common Criteria for the Security Evaluation of Information Systems, PriceWaterhouseCoopers's BetterWeb Initiative or the American Institute of Certified Public Accountants (AICPA) WebTrust™ Principles and Criteria for Business-to-Consumer Electronic Commerce.

Having defined the objectives and hypothesis of the experiment, it is possible to depict the proposed structure of the game.

The Agents

The synthetic environment for the game consists of three major agents:

- Financial institutions;
- Offense agents;
- Customers.

Each agent has a set of objectives and roles and the decisions are made based on these roles and objectives. They also interact with each other constantly based on certain rules of engagements. Apart from these agents, there are certain environmental variables that govern the interactions between agents.

The Financial Institutions

Human agents represent on-line financial institutions. Undergraduate and graduate business school students would form the pool of subjects. Subjects would receive cash incentives to perform well during the game. These agents are called upon to make business decisions to maximize the performance of the online financial institution they are representing. The structure of the online financial markets discussed in the previous sections guides the participants.

Strategy Layer

Human agents would be asked to devise a set of policies to draft security policies supporting their business strategy. Participants are encouraged to follow the four phases of the Policy Framework for Interpreting Risk in eCommerce Security (PFIRES) life cycle discussed previously.

Resource Layer

Resource layer performs the role of constraints for the financial institutions in the simulated economy. The agents have an initial endowment before the start of the game. In the later periods of the game, the level of the endowment is related to the performance in previous periods. This accounts for the financial constraints on the agents. Apart from the financial constraints, the agents also have human resource constraints. They are allotted certain amount of human resources that controls the level of operation of these institutions. The human resource level for an agent changes over periods depending upon the performance of the agents over the periods. The human resources would be classified as:

- On-site employees,
- Telecommuters,
- Contractors.

The other constraints include the physical location and the physical infrastructure size of the financial institution.

Operational Layer

Operational layer is where the agents have to make operational decisions concerning their business. These decisions are directly related to the policies defined by the agents in the strategy layer. The operational decisions that the agents make pertain to defining their level of operation, determining the level of investment in Information Technology Infrastructure and creating the information security infrastructure to safeguard the IT infrastructure.

The agents have to define their customers who can be for the purpose of the game:

- Individual consumers
- Business customers

Once the agents have defined their customers, they establish their operational level which determines the specific functionalities that agents may provide through their online business.

The services that could be provided by the agents are directly determined by the characteristics of the customers they are serving. We have defined few services for both individual consumers and the business customers that would be included in the game. The product profile for the individual customers could include:

- Consumer banking
- Security brokerage
- Insurance services
- Mortgages
- Credit cards
- Asset management
- Investment research and information

The product profiles for the corporate customers, instead, include:

- Online payments
- Payroll services (including employee benefits and perks)
- Authentication
- Electronic contracts

Once the agent has decided on its customers and services that the business is going to provide, it has to determine the investment level in the IT infrastructure. In the game, once the agent determines its customers and service profiles, he/she is provided with indicators on what is the minimum level of IT infrastructure required to achieve a determined service level. Agents would be restricted to create the required IT infrastructure if it has insufficient financial resources to update its existing IT infrastructure to the required level. The agent may choose to invest more in IT infrastructure to provide additional benefits to consumers. For example, an agent may choose to invest more in network layer to increase bandwidth thus providing faster and more simultaneous access to customers. But such decisions would be dependent on the IT policy and the marketing policy that the agent creates at the strategy layer. To provide simplicity for the game, the IT infrastructure has been classified into five layers:

- Network Layer
- Operating Systems Layer
- Database Layer
- Application Layer
- Business Process Layer

While determining the level of investment in the IT infrastructure agents also have to establish the investment in information security. Investment in information security would correspond to a certain percentage of IT budget. Few of the IT tools that could be used to provide information security have been discussed in the previous sections of this paper. Information security investment includes security tools and disaster recovery methodologies. The investment in Information Security is derived from the information security policies defined the strategy layer.

Consequence Layer

The determination of all the variables in the operational layer defines the profile of an agent during that period. The agent's success or failure is related to its own profile and that one of other agents. Based on the investment in IT infrastructure and information security technology and management, an agent's vulnerability profile is defined. Offense agents can exploit these vulnerabilities and undermine the level of customers' trust on the company's networks, brand image and financial strength.

The Offense Agents

The offense agents represent the sources of various external or internal threats that an organizations information system might face. An overview of their characteristics has been provided at an earlier stage of this paper. These agents are:

- Hackers
- Terrorists
- Organized crime
- Business competitors
- Foreign intelligence
- Internal threats.

For the purpose of this experiment, these offense agents are presently modeled as artificial agents.

The Structure of the Offense Agents

The offense agents have been classified along the following variables:

- Motivation to carry out intrusions against on-line financial institutions;
- Disposable financial resources;
- Collaboration level among agents;
- Risk acceptance
- Availability of technological resources.

The technology resources can be further classified according to the type of technology, its availability, complexity and cost. Technologies have been classified in correspondence to the IT infrastructure levels for the online financial institutions. Thus, these technologies could prove to be potential threats to one or more of the IT infrastructure layers, i.e. the network layer, the operating system layer, the database layer, the application layer, and the business process layer. The availability of technology characteristics corresponds to how a particular technology is available to the offense agents. The technology could be available for free, or it could be a modified version of freeware solutions or could be completely novel. Two other technology characteristics correspond to the complexity level of the technology, i.e. how sophisticated the technology is, and the cost of technology that depends on the other technology characteristics.

The Customers

The customers have been divided into two classes for the purpose of the game. They correspond to the individual consumers and the business customers. The classification has been made base on the types of services they demand from the online financial institutions. Similar to the offensive agents, consumers are being modeled as artificial agents.

The Environmental Variables

The environmental variables are those external elements that are present in the game and control certain parameters of the game. The administrators control these variables and the players are to adjust to them in case of on-the-fly changes. The environmental effectors include new government and legal requirements that may affect the strategy of the online financial institutions. Another environmental factor is the progress of the technology itself. The offense tool, IT infrastructure and the security tools depend upon the current state of the technology and its pace of change. Different values are given to these environmental parameters for separate sets of experiments.

Conclusion

The goal of this paper was to introduce an experiment presently carried out at the Krannert School of Management of Purdue University concerning the complexities associated with technical and managerial complexities associated with information security of on-line financial institutions. After a brief description of the overall on-line financial industry and its faced risks while conducting transactional activities of the Internet, the paper has presented a description of the game with its assumptions, objectives and hypothesis. This research effort is still at its infancy in terms of development and testing. Nevertheless, the research team aims to present initial results during this conference and to incorporate comments and suggestions in its future developments.

---

[1] "1999 Information Security Industry Survey" Information Security Magazine, July 1999 available at http://www.infosecuritymag.com/

[2] Computer Security Institute 1999 Computer Crime and Security Survey freely available at http://www.gocsi.com/

[3] Information taken from National Criminal Intelligence Service (NCIS) Project Trawler: Crime on the Information Highways May 1999 available at http://www.ncis.co.uk/newpage1.htm

[4] Most of the sources concerning the activities of these actors originate as part of the growing literature on information warfare, information operations and revolution of military affairs. For an initial classification of the activities of these offensive actors refers to Section 2-11 of the Report of the Defence Science Board-Task Force on Information Warfare-Defense (IW-D), prepared for the Office of Undersecretary of Defense for Acquisition and Technology, November 1996. A full text of the report is available in the Survey Section of the http://www.infowar.com

[5] Eric Shaw, Kevin Rubin and Jerrold Post "The Insider Threat to Information Systems" Security Awareness Bulletin n.2 (June 1998), pp.27-46 and Steven Harrington "Computer Crime and Abuse by IS Employee" Journal of System Management vol. 5, n.2, (Autumn 1995) pp.6-10

[6] For more information about the concept of trust in an on-line commercial environment see Robert Morgan and Shelby Hunt "The Commitment-Trust Theory of Relationship Marketing" Journal of Marketing vol. 58, n.3 (July September 1994) and Donna Hoffman, Thomas Novak and Marcos Peralta "Building Consumer Trust Online" Communications of the ACM vol. 42, n.2 (April 1999) pp.81-84

[7] "How Concerned About Security" and "Would You Bank Without a Security Statement" GVU's User Surveys, October 1999 available at http://www.gvu.gatech.edu/gvu/user_survey_/survey-1998-10/graphs/privacy/

[8] Morgan Stanley The Internet Banking Report September 1999 available at http://www.msdw.com

[9] Ernst and Young LLP E-commerce and Connecting the Customer-1998 Special Report Technology in Banking and Financial Services available at http://www.ey.com

[10] Morgan Stanley Dead Whittter The Internet Banking Report, September 1999 available at http://www.msdw.com

[11] "Strategic Online Banking Momentum Builds" Online Banking Report, January 1998 available at http://www.onlinebanikingreport.com/

[12] Comptroller of the Currency Administrator of National Banks Internet Banking-Comptroller's Handbook (Washington DC, USA: Office of the Comptroller of the Currency, October 1999) p.4. The Office of the Comptroller of the Currency regulates and supervises US national banks to ensure a safe, sound and competitive banking system. For more information see http://www.occ.treas.gov/

[13] Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University and Arthur Andersen Consulting Policy Framework for Interpreting Risk in Ecommerce Security (PFIRES) available at http://www.cerias.purdue.edu/ in the section Programs