Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2000 Proceedings

International Conference on Information Systems (ICIS)

December 2000

The Experimental Analysis of Information Security Management Issues for Online Financial Services

Mukul Gupta
Purdue University

Alok Chaturvedi
Purdue University

Shailendra Mehta
Purdue University

Lorenzo Valeri
King's College London

THE EXPERIMENTAL ANALYSIS OF INFORMATION SECURITY MANAGEMENT ISSUES FOR ONLINE FINANCIAL SERVICES[1]

Mukul Gupta
Alok R. Chaturvedi
Shailendra Mehta
Krannert Graduate School of Management
Purdue University
U.S.A.

Lorenzo Valeri[2]
International Center for Security Analysis
King's College London
United Kingdom

Abstract

E-commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective financial activities over the Internet. Still, its definition is a complex endeavor due to the constant technological and business change and requires a coordinated match of managerial and technical solutions. This research intends to provide an instrument to test and evaluate the strategies to counter threats facing online financial institutions through an artificial economic setup at the Synthetic Environments for Simulation and Analysis (SEAS) laboratory at the Krannert Graduate School of Management, Purdue University. The research also intends to provide guidelines for forming information security policies and strategies for survival and success in the dynamic and hostile business environment. Initial results indicate that online banks that were proactive in recognizing the threats and devising policies to counter them generated greater revenue and were able to focus on the core activities. Public disclosure of security breaches by the victim banks resulted in better overall health of the simulated economy. The simulation is still in its development and testing phase and the research team intends to present the findings at the conference.

1. INTRODUCTION

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 rates. This development, nevertheless, represents just the start of 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

[1]This research is partially funded by the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University.

[2]Lorenzo Valeri's participation in this research was supported by the European Union's Marie Curie Research Fellowship.

illegal activities. Information security, thus, is becoming a pivotal business and technical undertaking for any company involved in online financial activities. Because of the sensitivity of their activities, financial institutions have to focus on the overall security of their activities and operations.

The purpose of this research is to compare and test the success and failure of the possible strategies to counter the multiple risks facing online financial institutions in the experimental set up of Synthetic Environments for Simulation and Analysis (SEAS) laboratory devised by the Krannert School of Management at Purdue University. This research intends to provide guidelines to the existing and future businesses for forming the information security policies and strategies to survive in a dynamic and hostile environment. The existing security research either focuses on technical research devising specific security solutions to threats or anecdotes the existing success and failure stories. There is a lack of experimental studies in security research that can evaluate the managerial and policy issues. Our research attempts to fill this void. The simulated economy developed for the study could also be used to demonstrate and train the organizations in countering the threats faced by online financial institutions. The experiments could also be expanded to include into their scope businesses other than the financial institutions.

2. ONLINE BANKS

In 1996, Morgan Stanley Dean Witter (1999, p. 3) indicated that the Internet would most profoundly influence the financial industry as a sector since its service distribution does not require the physical exchange of goods. Nevertheless, the financial industry is not new to Internet-related trends like dis-intermediation, product developments, and strategic alliances that were normal business developments even in the pre-Internet era. The Net, nonetheless, has accelerated these changes and created new opportunities. *The Online Banking Report* (1999) has assessed that, while is took nearly 15 years to achieve a mere 1% penetration rate of U.S. households in 1996 for online financial services, that figure has increased to 4% by 1999. By 2001, more than 22 millions U.S. customers are expected to have online banking accounts. This number will rise to 42 millions by 2010. Morgan Stanley Dean Witter has also predicted credit card charges will increase by 11% by 2004 due to e-commerce transactions. Similar developments are predicted for online share trading and electronic loans and mortgages (Morgan Stanley Dean Witter 1999, p. 5).

These statistics are not circumscribed to so-called "brick and mortar" financial institutions like American Express, BankOne, or Citigroup that have espoused the Internet to provide new services and products in order to exploit rapid growth of online users. The growing success of the online financial industry is also connected to new financial services like thematic vertical portals, aggregators and specialty manufacturers (Morgan Stanley Dean Witter 1999, pp. 9-25; see Table 1).

Table 1. Business Model for Online Banks

Business Model	Features	Example
Vertical Portal	• Distribute information and financial solutions • Customers can access information and execute transactions (e.g., online bill payment)	Bank One Citibank American Express
Aggregator	• Visitors can compare products such as mortgages or insurance policies • Sell product prices and information, sometimes acting as intermediaries between online agents or brokers	InsWeb E-Loan QuickenMortgage InsureMarket
Specialty Manufacturer	• Provide a diverse array of ready-made services for Internet distribution points such as aggregators or vertical portals • Web presence is less important to these companies than producing a superior, low-cost, well-recognized brand name product	Capitol One MBNA Janus

Whatever their business strategy and target might be, online financial institutions need management and technical measures to counter the growing set of risks related to their increasing reliance on the Internet. The proposed simulation focuses on existing banks that have branched over the Internet, such as BankOne's WingspanBank.com or Citicorp's Eciti.com, or new Internet-only banks, such as Aerobank, NextBank, CompuBank, or Telebank. Nevertheless, the experiment has been structured with the full understanding that this market will evolve rapidly following the 1999 Financial Services Modification Act (ABA Banking 1999).

3. THREAT OF COMPUTER CRIME

Although these risks are part of the overall activities of any financial institution operating in any environment, the Internet has made it more complex to manage them, especially in relation to the rise in computer crimes and misuse. According to the *Information Security Magazine* (1999), since 1998 about 20% of the surveyed financial institutions have experienced disruptions of their information and network systems. The 2000 Computer Crime and Security Survey by the Computer Security Institute (CSI) has confirmed similar findings: 70% of the surveyed corporations have reported security breaches beyond the usual computer viruses, laptop theft or employee "netabuse." The rise of computer crime, moreover, does not know geographical boundaries and instances of computer crime can be found across the globe.[3]

The perpetrators of these security breaches may be classified in two groups: external agents and insiders. According to the 2000 CSI Computer Security Survey, almost three-quarters of the corporate respondents have suffered abuses from insiders. Motivations for these misuses vary from personal frustrations related to perceived lack of financial entailment for professional skills, computer dependency, and reduced loyalty to employers.

Table 2. Classification of Perpetrators

Perpetrators	Threat	Examples
External	Exploit Internet ubiquity and anonymity as advantageous feature to accomplish their objectives	• Hackers • Terrorist organizations • Business competitors • Organized crime • Foreign intelligence
Internal	Authorized users who exploit their system access to achieve specific objectives	• Employee • Contractor • Teleworker

4. RESEARCH OBJECTIVES

The objective of this research is to assist managers in devising the optimal investment level in information security management and technology in order to enable specific business strategies and goals. In particular, the experiment hopes to shed some light on the hypotheses that maximum investment in information security does not result in maximum benefits for the online banks and it may have a non-positive effect on the bank's internal and external functionalities and activities.

The research also aims at testing the behavioral patterns of the online banking organizations when confronted with actual security breaches or potential security threats. We expect to gain some insights into firm behavior, whether the banks have immediate reaction to security breaches or they are proactive in building up a security infrastructure. We hypthothesize that the companies with well-defined technical and managerial security policies demonstrate much more controlled reaction to major security breaches.

Through the experimental framework of the research, we also intend to test, compare, and analyze various risk management methodologies on the performance of the agents. Finally, the research aims at evaluating the impact and efficiency of some of the many information security policy initiatives devised by the U.S. federal government as part of its effort to protect elements of the critical national information infrastructure, which includes the online financial industry, to preserve national political stability and maintain economic competitiveness.

[3]The British National Criminal Intelligence Service, for example, has recently registered an exponential growth of computer crime throughout the United Kingdom (National Criminal Intelligence Service 1999). The rise of computer crime, moreover, does not know geographical boundaries. Recent data released by KPMG at the 2000 European Information Security conference have confirmed this trend even in Europe. Moreover, the recent spread of the "I Love you" virus, which originated in Philippines, confirms how the threat for malicious activities can originate even in countries that do not have a strong Internet and e-commerce infrastructure.

5. RESEARCH METHODOLOGY

We propose to develop a synthetic economy to evaluate and test our hypothesis. The simulated economy for the online financial institutions and the threat environments are being created at the Synthetic Environments for Analysis and Simulation (SEAS) at Krannert School of Management at Purdue University. SEAS is a distributed, interactive, real-time synthetic economy populated with human and artificial agents. It allows realistic representations of markets and economies at any level of detail. A crucial feature of SEAS is that it incorporates human agents and their attendant decision support systems in an effective way. The artificial agents represent decision-makers who engage in relatively non-strategic decision making, such as consumers in large markets. Human agents, on the other hand, represent decision-makers such as firms and governments that engage in strategic interaction.

The synthetic economies have distinct advantage over traditional simulations in capturing human behavior. Simulations focus on determining the rational behaviors of humans and modeling them into the simulations, but the rationality assumptions don't hold very well for our environment. Complex human behaviors have traditionally given trouble to scientists and have stimulated theories about cognition and creativity (Epstein 1996). The most perplexing of these have been the novel behavior where humans do things that they have not done before. The mystery of novelty underlines most theories of productivity in problem solving (Wertheimer 1945). Also the behavior is affected by events that have occurred in past (Köhler 1925).

In synthetic economies, human players are involved to capture the decision-making process of humans. Simulations tend to analyze the performance of a process or human decisions in a bounded search space. But irrationality is unbounded, thereby making the search space for our environment unbounded. One of the objectives of the synthetic economy is to create search spaces themselves under which the behavior of human agents can be monitored, analyzed, and interpreted.

This experiment includes a synthetic economy in which three classes of players interact: online financial institutions (played by humans), potential attackers, and customers (the latter two played by artificial agents). These interactions are centered on a set of rules of engagement and specific environmental variables regulating the relations among agents. We plan to conduct a series of experiments with different sets of human agents and capture their behavior. In the experiment, the human agents are given incentives to make their best decisions. In addition, we systematically collect data on costs, demands, market shares, demographics, and technological trends and calibrate SEAS to replicate the economic or management situations under consideration. The data collected from these experiments would be analyzed to achieve our research objectives.

6. RESEARCH DESIGN

In light of the complexity of information security, the following design and data modeling assumptions have been made. First, network and information technologies have intrinsic vulnerabilities as confirmed by the constant stream of news provided by specialized mailing lists and websites. This situation is explained by the fact that developers often rush products and services to the market that have not undergone proper testing and quality control procedures. Moreover, e-commerce ventures such as online banks constantly strive to provide their customer base with new services and products as well as security solutions. Their integration often creates new and dangerous vulnerabilities that facilitate the work of hackers and business competitors.

This simulation involves two classes of agents: online banks and malicious actors. Each of them is conceived to be a rational actor who expects to achieve a specific set of objectives. In addition, the simulation includes independent environmental variables such new legal and regulatory settings directly involving online banking activities. The inclusion of these variables is essential to maintain the practical relevance of this simulation in light of the expected changes brought out by the 1999 Financial Services Modifications Act and initiatives concerning the protection of the critical national information infrastructure (ABA Banking 1999; see Figure 1).

6.1 Human Agents as Online Banks

In this simulation, these agents play the role of financial institutions. During the trial, period MBA students from the Krannert School of Management played the role of the first set of agents. The research team expects positive feedback from initial trials since these students have undertaken intensive academic training in IT management and operations as well as strategy and e-commerce. Still, the objective in the medium and long term is to engage senior managers with business and IT responsibilities to raise their awareness about the complexities of information security management and planning. Whatever their professional and academic status, these agents are required to form and justify their decisions to improve the overall performance of their online bank, while devising calibrated technological and managerial information security policies. In this context, players are invited to follow the information security policy lifecycles proposed by Rees (2000) (see Figure 2).

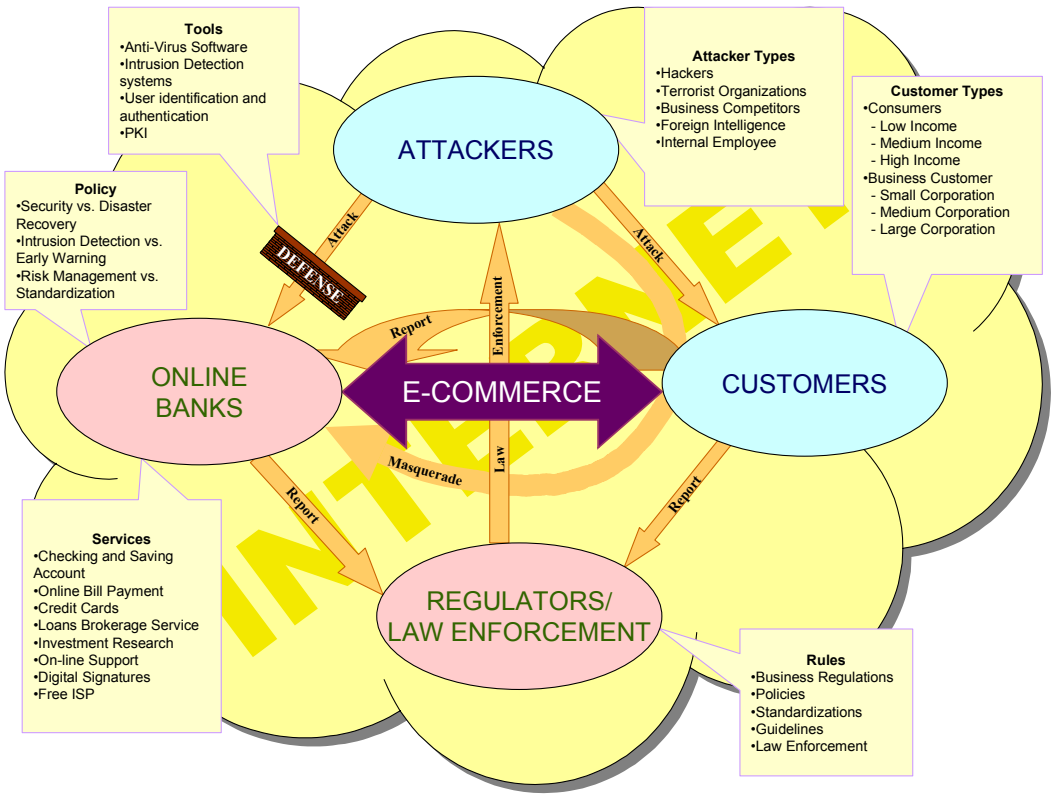

Figure 1. Experimental Design

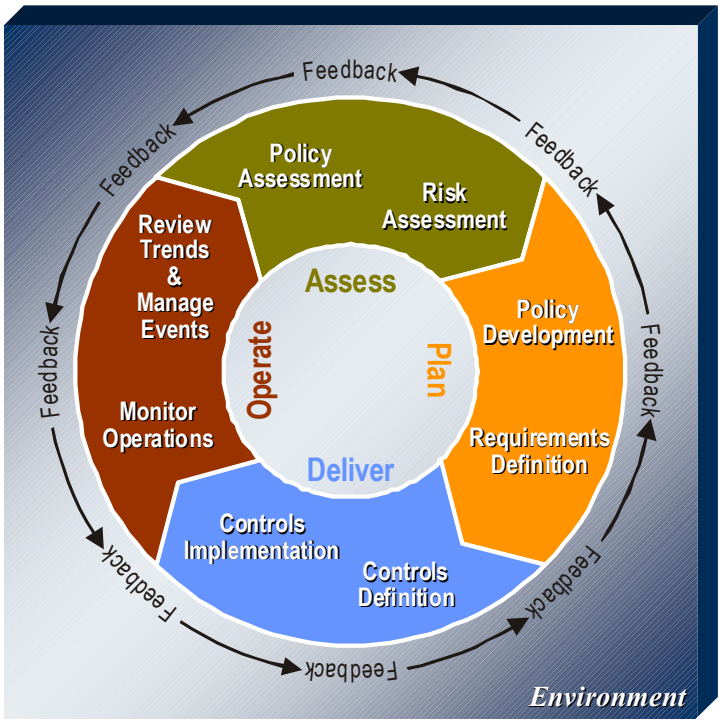

Figure 2. Policy Framework for Interpreting Risk in E-Commerce Security

Agents are assigned to represent two different classes of banks. The first class includes Internet-only banks that have been approved by federal or state regulators such as the Office of the Chief Controller at the Department of Treasury or the Federal Deposit Insurance Council (FDIC). The other set of financial institutions refers to online banks that are related to a brick and mortar banks. This differentiation is critical since it indicates distinction of financial, marketing, and commercial objectives. Online banks are expected to offer services and products as well as multiple valued-added services to individual and business clients. Initially this simulation focuses on the provision of banking services mainly to individual customers. Nevertheless, the underlying technical infrastructure of this simulation is conceived to be flexible enough to include new business services at a later stage. The agents have the objective to determine the bundle of services offered and the level of investment in IT infrastructure and security. For the purpose of this simulation, it is assumed that agents offer only significant bundling of products and services. In significant bundling, agents are expected to generate more information and data to determine the right bundle that is expected to general the highest level of revenues (Altinkemer 2000).[4]

Table 3. Human Agent Objectives

	Decision Category	Solutions	Choices	Key Performance Indicators
Business Decisions	Primary Services (Online Banking Report 1999)	• Checking and savings account • Online Bill Payment • Credit Cards • Loans • Brokerage Services	• Product Bundle • Price • Quantity • Channel • Investments	• Revenues • Profits • Market Share
	Value Added Services	• Investment Research • Online Support/Call Centers • Service Customization • Digital Signatures • Free ISP		
IT Decisions	IT Infrastructure	• Network • Operating System • Database • Application • Business Process	Infrastructure Investment Level	• Total cost of ownership • Quality of Service • Return on Investments
	Security Management (Financial Services Security Laboratory 2000)	• Identification • Authentication • Authorization • Data Integrity • Audit • Data Disposal • System Integrity • Security Administration • Guidance • Non-Repudiation	• Security Feature • Investment level	• Security Index • Cost • Vulnerability

[4]The level of the quality of service is the parameter that differentiates each significant bundling of financial products provided to customers. For instance, if an online bank provides checking and savings accounts, the quality of service guarantee may correspond to specific interest rates for savings accounts or a minimum balance for free checking services or ATM transactions. Moreover, agents may decide to specify the level of quality for each product and value added service. For example, it is possible to provide customers with extensive investment research by combining the contents of the main information sources available. The agent may also choose not to offer one product or service such as digital signatures in light of a specific strategic business objective. The interesting aspect of this single-bundle approach is that it surrogates tine-bundling of certain services. For large volume online stock purchases, quality of service requirements for the execution of the transaction may be one tenth of a second, one hundredth of a second, and so forth.

6.2 The Offense Agents

The effectiveness of the previous business and operation decisions of the human agents acting as online banks is tested by their capacity to mitigate malicious activities of these following offense agents: hackers, terrorists, organized crime, business competitors, foreign intelligence, and internal threat. In the context of this simulation, these offense agents are classified according to motivation and capability (RSA 1999; see Table 4). High combinations of motivations and capabilities indicate elevated levels of threat associated with a specific threat agent (see Figure 3). Therefore, through a detailed analysis of these factors, it is possible to establish a specific profile that may indicate the tendency of an individual or group to engage in offense activities against online banks, with regard to their perception of risks connected to the undertaking of these online operations.

Table 4. Criteria for Classification of Offense Agents

Criteria	Characteristics
Motivation	• Indicates the actors' commitment to carry out malicious activities against online banks • Related to individual and collective psychology of the agents and their political and ideological background
Capability	• Indicates the actors' capability to effectively use available offense tools, modify them or create new ones in order to achieve specific strategic and political objectives • Related to actors' access to financial resources that determine their capacity to acquire the sophisticated technical and human resources to conduct malicious activities

Figure 3. SEAS Classification of Offense Agents

For the purpose of this simulation, the offense agents have been modeled using genetic algorithms. The advantage of using the genetic algorithm in modeling the offense agents is the capability to dynamically change the composition of the offense agents. During each period of the experiment, successful agents are retained and recombined to generate new offense agents while the unsuccessful agents are eliminated. This reproduction of the new set of offense agents in the next generation is carried out using the selection, crossover, and mutation operations of the genetic algorithms (Goldberg 1995).

To an extent, the initial mix of offense agents determines the mix of agents in later stages. To avoid this bias, the experiments will be conducted with several initial mixes of offense agents. Also the crossover and mutation probabilities for the genetic algorithms will be altered in each run of the experiment.

7. PRELIMINARY RESULTS OF AGENTS BEHAVIOR

The results of the preliminary experiments gave some interesting insights into the behaviors of the agents: the firms, the governments, and the perpetrators. The banks could be classified as conservative, speculative, or belligerent on the basis of their behaviors. These agent behaviors are described in Table 5. It has to be noted that these results are preliminary and may be viewed as trends. They still need to be analyzed and verified more thoroughly. Nevertheless, these results do provide directions toward modifying and improving the synthetic economy.

Table 5. Agent Behaviors

Agent	Behavior
Banks	**Conservative Banks** • invested in information security early and often and achieved higher revenue, profits, and customer satisfaction • banks were protected against attempted attack and were able to focus on core business activities **Speculative Banks** • with little investments in information security did well early on, but once they suffered losses due to cyber attacks, they could not fully recover to compete effectively for several experiment periods • lost their customers trust and it was very difficult to win them back **Belligerent Banks** • invested in offensive capabilities and resorted to espionage against their competitors • attracted the attention of the government and other competitive organizations and exposed them to retaliation from other banks and law enforcement
Perpetrators	• anti-social organizations that invested heavily in intelligence gathering capabilities showed a higher rate of successful attacks • those who did not gather intelligence often ended up wasting their offensive resources on banks that already had sufficient defensive resources • it was evident that artificial agents were better at terrorist activities than human agents
Law Enforcement	• when the law enforcement agents were very active and aggressive, the economy functioned very smoothly, and the cost of information security for the firms were much lower • when the government agents cooperated with firm agents on security and law enforcement, it benefitted both the governments and the firms • although there was a tendency to not to disclose attacks, but when the victim banks made the attacks knowledge public, they generally performed better on the long run

8. CONCLUSIONS

Operating over the Internet provides online banks with new potentialities, but also creates a set of new risks that many malicious actors are expected to use for their illegal activities. Information security, therefore, is an essential management and technical requirement for any efficient and effective financial activities over the Internet. The purpose of this research is to analyze the success and failure of the possible strategies to counter the multiple risks facing the online financial institutions in the experimental set up of Synthetic Environments for Simulation and Analysis (SEAS) laboratory devised by the Krannert School of Management. This research intends to provide guidelines to existing and future businesses to formulate the information security policies and strategies to survive in a dynamic and hostile environment. The limitation of the research is that the strength of the results obtained lies in the design of the synthetic economy and the performance of the human agents. The results obtained can only be viewed as indications to possible security policies that the management can employ in an environment similar to the one generated by the synthetic economy. This research project is still in the development and testing phase. The research team aims to present the experiment design and the some results at the conference. The research team is willing to incorporate comments and suggestions in its future developments.

References[5]

ABA Banking. "Cover Report: Banking in the New Millennium-Financial Modernization Arrives: The Financial Services Modification Act," *ABA Banking* (41:12), 1999, pp. 6-24.

Altinkemer, K. "Pricing E-Banking Service," Working Paper, Krannert Graduate School of Management, Purdue University. March 2000.

Computer Security Institute. *2000 Computer Crime and Security Survey*, 2000 (available from http://www.gocsi.com; accessed March 2000)

Epstein, R. *Cognition, Creativity and Behavior: Selected Essays*, Westport, CT: Praeger Publishers, 1996.

Financial Services Security Laboratory. *Master Security Criteria*, February 2000.

Goldberg, D. E. *Genetic Algorithms: In Search, Optimization and Machine Learning*, Reading, MA: Addison-Wesley Publishing Company, 1995.

Information Security Industry Survey. *Information Security Magazine,* July 1999 (available at http://www.infosecuritymag.com; accessed September 1999).

Köhler, W. *The Mentality of Apes,* London: Routledge & Kegan Paul, 1925.

Morgan Stanley Dean Witter. *The Internet and Financial Services,* Equity Research-North America, August 1999.

National Criminal Intelligence Service. *Project Trawler: Crime on the Information Highways*, May 1999 (available from http://www.ncis.co.uk/newpage1.htm; accessed January 2000).

Online Banking Report. *The Online Banking Report,* 1999 (aailable from http://www.onlinebankingreport.com; accessed September 1999).

Rees, J. "Policy Framework for Interpreting Risk in eCommerce Security," joint research project by Anderson Consulting and The Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University,. Technical Report, January 2000 (vailable from http://www.cerias.purdue.edu/techreports/public/PFIRES.pdf; accessed January 2000).

RSA. "Industry/Government Partnerships: The Key to Information Assurance," *The 1999 RSA Data Security Conference and Expo,* San Jose, CA, January 17-21, 1999.

Wertheimer, M. *Productive Thinking,* New York: Holt, Reinhart, 1945.

[5]The following reference list contains URLs for World Wide Web pages. These links existed as of the date of submission but are not guaranteed to be working thereafter. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced. The author(s) of the Web pages, not ICIS, is (are) responsible for the accuracy of their content. The author(s) of this article, not ICIS, is (are) responsible for the accuracy of the URL and version information.