Electronic Security: Risk Mitigation in Financial Transactions

Public Policy Issues

Thomas Glaessner, Tom Kellermann, Valerie McNevin*

World Bank Policy Research Working Paper 2870, July 2002

* Thomas Glaessner is Lead Financial Economist in the Financial Sector Strategy and Policy Department of the World Bank, Tom Kellermann is a Data Risk Management Specialist, and Valerie McNevin is Security Information Officer and the Privacy Officer for the State of Colorado. A far more in depth version of this paper can be found at http://www1.worldbank.org/finance/ which includes the four annexes cited in this paper and the executive summary.

Abstract

This paper builds on a previous series of papers (see Claessens, Glaessner, and Klingebiel, 2001, 2002) that identified electronic security as a key component to the delivery of e-finance benefits. This paper and its technical annexes identify and discuss seven key pillars necessary to the fostering of a secure electronic environment. Hence, it is intended for those formulating broad policies in the area of electronic security and those working with financial services providers (e.g., executives and management). The detailed annexes of this paper are especially relevant for chief information and security officers responsible for establishing layered security.

First, the paper provides definitions of electronic finance and electronic security and explains why these issues deserve attention. Next, it presents a picture of the burgeoning global electronic security industry. Then, it develops a risk-management framework for understanding the trade-offs and risks inherent in the electronic security infrastructure. It also provides examples of trade-offs that may arise with respect to technological innovation, privacy, quality of service, and security in the design of an electronic security policy framework. Finally, it outlines issues in seven interrelated areas that often need attention in the building of an adequate electronic security infrastructure. These are (i) the legal framework and enforcement; (ii) electronic security of payment systems; (iii) supervision and prevention challenges; (iv) the role of private insurance as an essential monitoring mechanism; (v) certification, standards, and the roles of the public and private sectors; (vi) improving the accuracy of information about electronic security incidents and creating better arrangements for sharing this information; and (vii) improving overall education about these issues as a key to enhancing prevention.

Acknowledgments

The authors would like to thank the following individuals who have shared their time and background material. In addition, we thank them for their valuable written and oral input. They are Forrester Allison, Chris Bateman, Joseph Cooper, Tony Chew, Dr. Dorothy Denning, John Farber, Jonathan Fiechter, Karen Furst, Rick Fleming, John Frazzini, Edward Gilbride, Joi Grieg, Hugh Kelly, James H. Lau, Stephanie Lanz, Toby Levin, Peter MacDoran, Simon Martinez, Linda McCarthy, Joe McLeod, Raj Nanavati, Brian Palma, Dr. Joseph Pelton, Peter Penfiel, Bill Rogers, James Savage, Leonardo Scudere, Don Skillman, Kurt Suhs, Gary Sullivan, Cornelius Tate, Dave Thomas, Bob Weaver, and Bob Wice. In addition to these individuals, many private organizations and public agencies took time to share their ideas with the authors, both in person and in a Global Dialogue held via the World Bank video conference facilities that included a discussion of e-security issues with officials from 20 countries in Latin America, Asia, and Africa.

Introduction

> *Is it a fact…that, by means of electricity, the world of matter has become a great nerve, vibrating thousands of miles in a breathless point of time? Rather, the globe is a vast head, a brain, instinct with intelligence! Or shall we say it is itself a thought, nothing but a thought…. —Nathaniel Hawthorne, 1851.*

Even before the events of September 11, electronic security was a growing area of concern for banks and other financial services providers in managing daily operational risk. Now, because of the rapid growth of wireless technology and its increasing use in providing financial services in emerging markets, either in coordination with the Internet or on a freestanding basis, there is even more demand for a careful look at issues related to electronic security.

This paper has three central objectives. The first is to define electronic security, discuss why this issue is becoming important worldwide, and characterize the players in the burgeoning worldwide electronic security industry. The second is to offer an economic incentive framework to use in addressing the problems posed by electronic security, with particular attention to financial services provided by banks. The third is to identify seven distinct pillars of reform that every country should construct and maintain to develop a secure electronic environment.

In meeting these objectives, the paper addresses the following public policy questions relevant to the future security of the global financial system:

- Are financial services providers given proper incentives to fully share timely and accurate information with law enforcement on security breaches? If not, is there a form of market failure taking place in this area within the financial services industry? What actions might be taken to facilitate public-private cooperation to remedy the situation? (See Sections II, III, and X.)
- What kinds of changes or additions to the legal and regulatory framework will be consistent with proper law enforcement within and across country boundaries? (See Sections V and VI and Annex IV.)
- What role should government play in setting policies, standards, and guidelines for e-security? How can it strike the proper balance between fostering technological innovation and establishing e-security standards? (See Sections IV and V and Annex IV.)
- What role should government play in regulating and supervising not only financial services providers but also third-party providers, such as money transmitters, hosting companies, ISP providers, and electronic security vendors? (See Sections VI and VII.)
- How should electronic records or transactions be verified or authenticated? What role should the government and the private sector play in certification? (See Section IX and Annex II.)
- What role can the private insurance industry play, especially in emerging markets, which often lack extensive human capital and capacity in regulatory agencies? Can it offer incentives to guide business toward a risk-management and risk-mitigation approach? How can layered security help in monitoring the operational and other risks created by electronic security breaches? (See Section VIII.)
- What roles can the government, private market participants, and the electronic security industry play in accurately measuring the extent of electronic security risk within and across countries? How can institutions improve their information and databases from which to measure this risk? (See Section X.)

- How can complementary and reinforcing actions be taken to ensure better electronic security in emerging market countries where regulatory, supervisory, and enforcement institutions are not strong? (See Sections IX, X, and XI.)

The answers to many of these questions are interrelated, and this paper approaches them in a systemic manner. The annexes offer a more detailed and technical analysis of the issues. Included also is a glossary of terms. Hence, the paper is intended for those formulating broad policies in the area of electronic security, those working with financial services providers (e.g., systems administrators in these entities), vendors of electronic security or other products (i.e., front-end Internet platforms provided by a hosting or portal company) that outsource to such financial services providers, and other participants in what is becoming a global electronic security industry.

The paper is divided into 11 sections. Each of sections II through XI addresses one set of the questions raised above. Section II defines electronic finance and security as used in the context of this paper; it explains why these issues will increase in importance as dependence on new technologies spreads into emerging markets and leapfrogging becomes a reality. Section III characterizes the functional categories of the global electronic security industry and describes its links to e-finance. Section IV delineates a risk-management framework for thinking about electronic security and outlines the elements necessary for policy development to ensure adequate electronic security. Section V outlines legal and enforcement issues. Section VI examines the complexities of electronic security with respect to payment systems and money transmitters. Section VII examines supervision and prevention of security breaches, including new approaches to oversight and inspection of security systems at financial services providers or nondepository institutions that act as money transmitters. Section VIII explores the opportunities for private insurance to participate in creating a risk-sharing approach to electronic security. Section IX examines certification issues within the electronic security industry, as well as the specific topic of electronic messages or signatures and the appropriate role of the government. Section X suggests possibilities for developing public-private partnership to improve the accuracy and availability of information about electronic security incidents. Section XI examines education as a key to improving protection against e-security incidents.

This paper treats the rapidly evolving are of electronic security from a perspective of technology. Too little is known about this subject in emerging markets. The paper focuses more attention on the United States, because the Internet originated there and because the defense and law enforcement agencies there have more experience in ensuring electronic security. It also focuses on some of the more advanced economies in Europe, as well as on Singapore and Hong Kong, to examine how electronic security issues have been addressed in those areas. Clearly, more research is needed to understand the specific problems of emerging markets as well as to identify critical areas of legislation and relevant institutional arrangements needed to improve electronic security standards worldwide. Unless it protects its information assets, the great potential electronic commerce offers can be significantly compromised.

I. What Is Electronic Security and Why Is It Needed?

Definitions of E-Finance and E-Security

To understand the need for electronic security, one must first precisely define what is meant by electronic finance. For purposes of this paper, e-finance is the use of electronic means

to exchange information, to transfer signs and representations of value, and to execute transactions in a commercial environment. E-finance comprises four primary channels: electronic funds transfers (EFTs); electronic data interchange (EDI); electronic benefits transfers (EBTs); and electronic trade confirmations (ETCs).

EFT, which began in the early 1960s, is the oldest form of electronic money transmittal. The amount of money moving by EFT is $2 trillion per day and growing. The volume of EFT usage worldwide is 677,411,204 transactions.[1] The second oldest form of electronic money movement is EDI. EDI is used to effect money payment orders and bar coding. Bar coding is operational in more than 70 countries worldwide. Its use has doubled in the past five years and is equal to 50 to 75 percent of purchases worldwide. The third oldest channel is EBT. Benefits have been transferred electronically for a decade in more than 37 countries worldwide, including many emerging economies. In the United States alone, EBT moves $500 billion in cash entitlements, such as food stamps, Social Security payments, and child assistance benefits. The total volume of EBT transactions in the United States is 568,981,051 annually.[2]

E-security can be described on the one hand as those policies, guidelines, processes, and actions needed to enable electronic transactions to be carried out with a minimum risk of breach, intrusion, or theft. On the other hand, e-security is any tool, technique, or process used to protect a system's information assets. Information is a valuable strategic asset that must be managed and protected accordingly. The degree of e-security used for any activity should be proportional to the activity's underlying value. Thus, security is a risk-management or risk-mitigation tool, and appropriate security means mitigation of the risk for the underlying transaction in proportion to its value.

The need for security is a constant of doing business over the Internet because, in essence, the Internet is a broadcast medium. E-security enhances or adds value to a naked network and is composed of both a "soft" and a "hard" infrastructure. Soft infrastructure components are those policies, processes, protocols, and guidelines that create the protective environment to keep the system and the data from compromise. The hard infrastructure consists of the actual hardware and software needed to protect the system and its data from external and internal threats to security.

The Potential Growth of Electronic Transactions

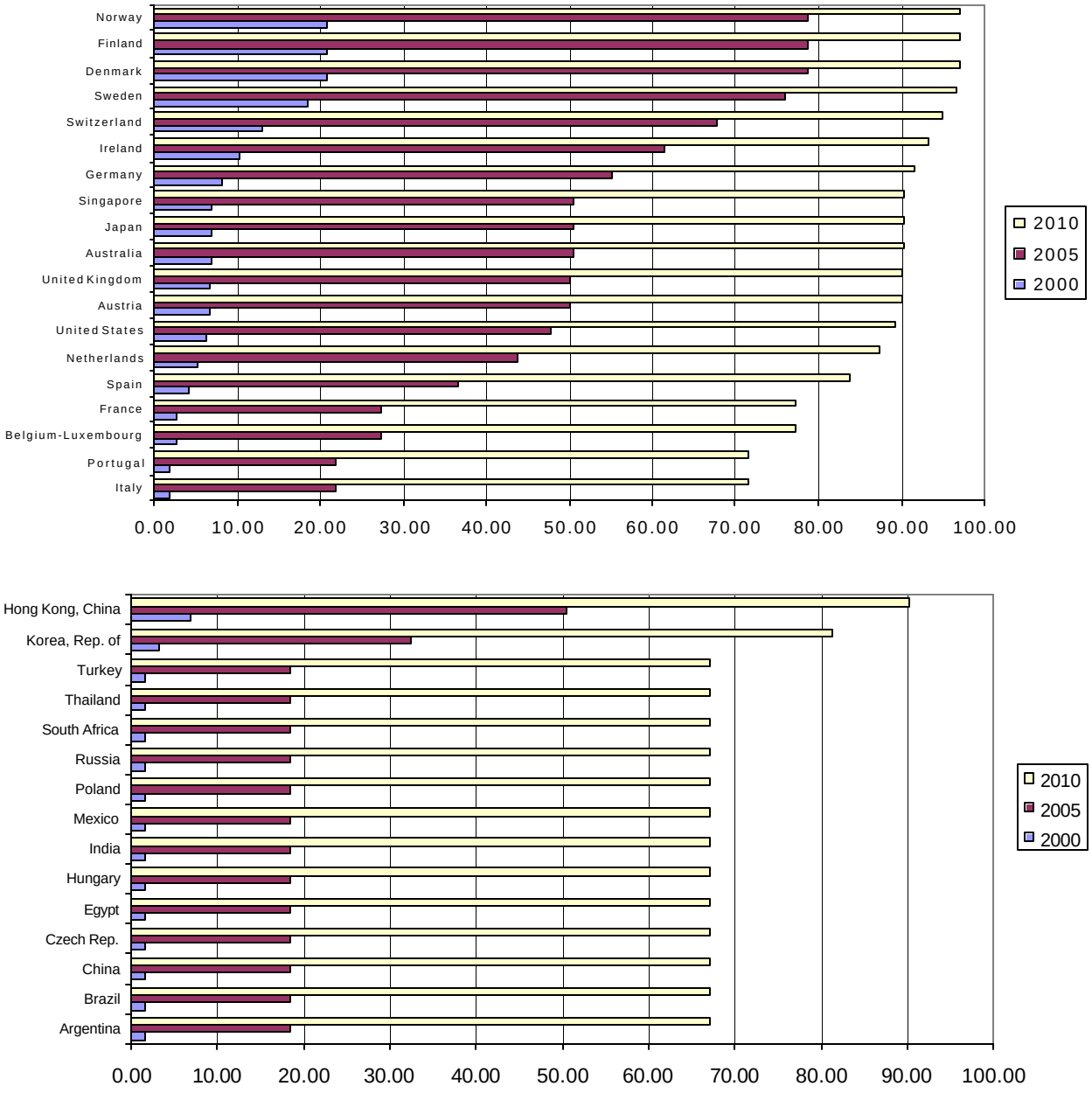
The volume and variety of electronic financial services have increased significantly, and use of the electronic medium to do business, whether online or through remote mechanisms, has spread rapidly over the past decade. Countries, not just consumers, are increasingly getting connected. As is evident in Figure 1, "these new technologies not only allow countries to leapfrog in connectivity, they also open new channels for delivering e-financial services" (Claessens, Glaessner, and Klingebiel, 2001). Since the mid-1990s, investment in banking technology has focused on online banking and brokerage services to increase convenience and also to reduce costs.

Concurrent with these realities, four new technology-related financial services industry trends have occurred: outsourcing, open architecture, integrated strategies, and new methods of e-payment. The new trends have been driven by considerations of cost reduction and need for improvement in quality of service, yet in the process of putting them in place, security issues have

[1] U.S. Department of the Treasury 2001.
[2] U.S. Department of the Treasury 2001 statistics.

too often been presumed to be less important or sometimes taken for granted. Figure 1 illustrates the projected rates of e-finance penetration worldwide.

Figure 1. E-Finance Penetration: 2000 and Projected Rates for 2005 and 2010



Note: The figures show projections based on takeoff years with better connectivity. The projections assume that all emerging markets have the same connectivity rating as in today's lowest-ranked industrial country, 6 (or better if their current rating is already higher); thus, the projections lead to the same minimum level of penetration in each emerging market.
Source: Authors' calculations.

By 2005, the share of banking that is done online could rise from 8.5 percent to 50 percent in industrial countries, and from 1 percent to 10 percent in emerging markets. With better

connectivity, online banking transactions in emerging markets could rise even further to 20 percent by 2005 (Glaessner, Claessens, and Klingebiel, 2001). Some estimate that $6.3 trillion of bank-to-bank transactions will be online by 2005.[3]

A parallel trend to the global use of e-finance is the adoption of new technologies that can act to expand the scope for electronic finance and access to financial services. Emerging markets increasingly find it more advantageous to use "new" technologies, such as wireless cellular technology, for e-finance as opposed to the Internet. Table 1 indicates that in a variety of emerging markets, wireless technology, as measured by cell phone penetration, is rapidly outstripping Internet penetration.

Table 1. Global Connectivity Trends

Country	*Number of mobile phone subscribers (Millions)*	*Percentage of population who are mobile or cellular subscribers*	*Percentage of population who are Internet users*
Developed Countries [a]	**30.0**	**56**	**32**
Australia	8.6	**45**	**35**
Finland	3.7	**72**	**38**
France	29.1	**49**	**14**
United States	109.0	**40**	**35**
United Kingdom	43.5	**73**	**30**
Developing Countries [a]	**6.9**	**7**	**2**
Brazil	23.2	**14**	**3**
Bulgaria	.6	**7**	**5**
Cambodia	.1	**1**	**<1**
China	84.5	**7**	**2**
Egypt	1.4	**2**	**1**
Guatemala	.7	**6**	**<1**
India	3.6	**< 1**	**<1**
Indonesia	3.7	**2**	**<1**
Mexico	14.1	**14**	**3**
Philippines	6.5	**8**	**3**
Republic of Korea	26.8	**57**	**40**
South Africa	8.3	**19**	**5**

Source: International Telecommunications Union, *World Telecommunications Indicators Database 2000*.
a/ These are averages for developed and developing countries respectively.

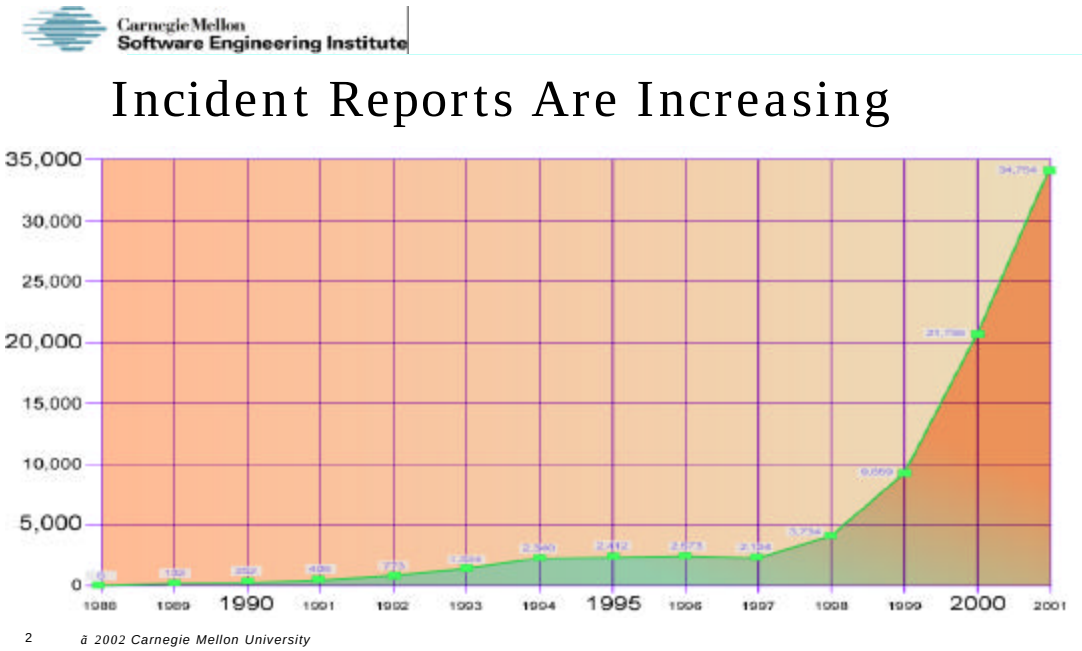
The Risks of New Technologies

With the benefits of new technology also come new and potentially virulent risks (see Figure 2). Table 2 shows that since 1995, incident reports increased 61 percent between 2000 and 2001 in the United States alone. Technology facilitates more efficient and quicker ways to commit old crimes such as fraud and theft. Remote access, high-quality graphics and printing, and new multipurpose tools and platforms provide greater means to commit such crimes as theft and impersonation online.[4] Disturbingly, as the technology becomes more complex, a perpetrator needs fewer skills to commit these crimes. For example, the art of online penetrations (i.e., hacking) was once a highly sophisticated skill. The information age, however, has permitted a

[3] Jupiter Communications 2001.
[4] Ibid.

breeding ground for underground hacker Web sites that now supply dubious individuals with the multifaceted tools necessary to break into financial platforms. Such Web sites as www.astalavista.box.sk and www.attrition.org supply complex malicious codes and viruses that enable novice users to penetrate banking systems.

Figure 2. Increase in Incident Reports



The most frightening aspect of the convergence of technology and crime is the magnitude of the crimes that can be carried out quite speedily. For instance, in the past it would have taken months or perhaps even years for highly organized criminals to steal 50,000 credit card numbers. Today, one criminal using tools that are freely available on the Web can hack into a database and steal that number of identities in seconds. Or a perpetrator can steal a laptop containing a database of 400,000 names and their associated credit card information. These are the reasons e-security must be taken very seriously.

Although e-finance offers an opportunity for developing market economies to leapfrog, it is not a panacea. The Internet Data Corporation (www.idc.com) recently reported that more than 57 percent of all hack attacks last year were initiated in the financial sector. Traditional risks have thus been reshaped. In the physical environment, frauds traditionally were paper-based or people-based, whereas the following are the means most often used to commit crimes online:

- Message interception and alteration
- Unauthorized account access
- Identity theft
- Manipulation of stocks and bonds
- Extortion
- Unauthorized system access (e.g., system damage, degradation, or denial of service)
- Industrial espionage
- Manipulation of e-payment systems

Table 2. Reported E-Security Intrusions

Date of Attack	*Compromised financial and e-commerce entities*	*Name of hacker, group, or malicious tool*	*Various losses sustained because of the intrusion into the financial entity's networks*
Sept. 18, 1995	Citibank [1]	Vladimir Levin	$ 10,000,000[2]
Mar. 1, 2000	U.K., U.S., Thailand, and Canada's e-finance and e-commerce sites	Alias "CURADOR"	28,000 accounts compromised, with total losses exceeding $3.5 million.[3]
Mar. 15, 2000	Internet Trading Technologies	Abelkader Smires	Denial-of-service attacks that caused major disruption of trading on the NASDAQ.
Aug. 10, 2000	Bloomberg[4]	Oleg Zesev and Igor Yarimaka	Broke into the Bloomberg computer system in Manhattan in an attempt to extort $200,000.
Dec. 22, 2000	EggHead [5]	Eastern European groups	Hackers compromise database of thousands of credit cards; on Christmas Eve, many of the cards were then "salami sliced." [6]
2001	Hong Kong	Various Hackers	Eight cases of e-banking theft were recorded in the year involving the loss of over $4.4M.[7]
Mar. 8, 2001	40 domestic e-banking and e-commerce sites	Eastern European criminal syndicate	Intruders stole credit card account information and other data by exploiting a Windows NT security flaw; the National Infrastructure Protection Center labeled this attack the "largest Internet attack to date." [8]
Apr. 12, 2001	VISA	Eastern European groups	Intruders gained access to its computer network in the U.K. and later demanded ransom for data obtained in the virtual break-in; company received a ransom demand of £10 million.
Jun. 5, 2001	Central Texas Bank[9]	Vasilly Gorshov and Alexey Ivanov	They had access to the bank's system for six months before they were detected.
Jul. 6, 2001	S1 (a host company)[10]	Investigation ongoing	The compromise of more than 300 banks and credit unions whose systems were hosted by S1.[11]
Jul. 14, 2001	Australia's Online Trading Systems	Black Orifice—Trojan Horse	Account data of more than 40,000 of their clients was compromised.
Aug. 21, 2001	Riggs Bank, First Virginia Banks, SunTrust, and Visa	Investigation ongoing	The account information of more than 4,000 account holders from these banks who used Visa debit cards was compromised; banks were forced to cancel all debit cards. [12]
Sept. 3, 2001	Intrusions into banking and e-commerce sites	Eastern European groups	Various extortions.[13]
Sept. 20, 2001	Deutsche Bank[14]	Nimda worm	Unknown—costs of breaches indeterminable.
Feb. 7, 2002	U.S. Treasury Direct[15]	Louis Lebaga	$158 million—Lebaga was apprehended only after attempting to steal $1.3 billion more five days later.
Mar. 1, 2002	Prudential Insurance Company	Donald McNeese	McNeese was arrested for the theft and credit card scam stemming from the hack of Prudential's database, compromising 60,000 personal records of employees there.[16]
Apr. 5, 2002	State of California, Payroll database	Investigation Ongoing	The hacker copied 265,000 state employee account names and social security numbers, thus making them vulnerable to ID theft.
Apr. 12, 2002	Republic Bank	Investigation Ongoing	The hacker copied 3,600 bank customer account names and files, thus making them vulnerable to ID theft; by exploiting S1's (the hosting company's) servers, he was able to compromise the accounts of these customers.[17]

Notes:

1. "Bank's Security Chains Rattled." *Financial Times*. Sept. 20, 1995. www.ft.com
2. Of the $10 million lost, all but $400,000 was recovered.
3. National Infrastructure Protection Center Major Investigations Web site: www.nipc.gov/investigations/curador.htm.
4. National Infrastructure Protection Center Major Investigations Web site: www.nipc.gov/investigations/bloomberg.htm.
5. Sullivan, 2001.
6. National Infrastructure Protection Center briefing, August 2001.
7. http://www.info.gov.hk/police/aahome/english/statistics/download/200201/crimebrief_eng.doc
8. SANS Institute Alert, March 8, 2001.
9. Predictive Systems "Global E-review," August 2001. www.chron.com/cs/cda/story.hts/metropolitan/929311 .
10. First reported by www.securityfocus.com
11. A compromise is defined as access to a person's computer systems and databases without his or her explicit knowledge and consent. S1 had an impressive client list, from E*Trade to FleetBoston Financial Corp.
12. Sara Goo of the *Washington Post* first broke this story. www.idg.net.
13. National Infrastructure Protection Center. www.nipc.gov. These intrusions were perpetrated to steal proprietary databases, which were then sent to the heads of these banks with extortion demands.
14. The National Infrastructure Protection Center reported that the worm was distributed from unknown sources and is said to have disrupted and infiltrated networks worldwide. www.zdnet.com
15. U.S. District Court Arrest Warrant Case # 02-841.
16. U.S. Department of Justice, 2002.
17. www.newsbytes.com/news/02/175977.html.

The tremendous growth in open networks has created a penetrable electronic environment akin to a circle of Swiss cheese pieces. Financial institutions are increasingly relying on technology to process, store, and retrieve data, but advances in computer hardware, software, and communications technology increase the financial industry's vulnerability to internal and external attacks. Without strong security controls, banks risk the possibility of financial loss, legal liability, and reputation harm.

The insecurity of the Internet further exposes financial institutions to undetected, global, and virtually instantaneous attacks on internal systems and proprietary information. This includes attacks by foreign governments and terrorists, as well as attacks by criminals or hackers originating domestically. Banks and vendors with weak security controls are susceptible to business disruptions, theft of data, sabotage, corruption of key records, and fraud. The development of wireless Internet access will further compound the problem (see Annex III) by enabling foreign governments, terrorists, criminals, and hackers, singly or in concert, to operate in countries that do not have the advanced communications infrastructure or adequate security protocols in place. Hence, building awareness now of the criticality of the risks associated with e-finance and promoting industry use of aggressive mitigation is crucial.

Despite the relative lack of accurate information about actual intrusions and associated losses, Table 2 highlights some the most pervasive venues for electronic attacks in the area of e-financial services that have been publicly documented. The most frequent problems in this arena are (i) insider abuse, (ii) identity theft, (iii) fraud, and (iv) breaking and entering, often conducted by hackers.

Just as legitimate use is increasing at a phenomenal rate, nefarious activity is also growing rapidly. Identity theft is the number one crime in the United States. Reported incidents of identity theft are projected to more than double, from 700,000[5] in 2001 to 1.7 million in 2005, and the costs to U.S. financial institutions alone will increase 30 percent each year, to more than $8 billion in 2005.[6] These numbers do not take into account the wide range of social costs associated with this crime, such as litigation expenses, or the lost hours to redeem one's name or credit information. In fact, these calculations do not include the very substantial losses for financial services providers generated by denial-of-service attacks. Table 3 suggests that denial of service can cost an average-size brokerage firm $6.5 million an hour or a credit card authorization company $2.6 million an hour. And these estimates do not include the costs of damage to reputation. Box 1 provides a graphic example of how pervasive a problem identity theft has become.

Table 3. Potential Losses from a Denial-of-Service Attack[7]

Business type	*Brokerage firm*	*Credit card authorization company*	*Automated teller machines*	*Major online auction site*
Exposure/Hour	$6.5 million/hr	$2.6 million/hr	$14,500/hr in fees	$70,000/hr

Source: Red Herring, December 2000.

Hacking, too, is endemic. Law enforcement agencies have documented that Eastern European organized hacker groups have penetrated hundreds of banks worldwide. The FBI's

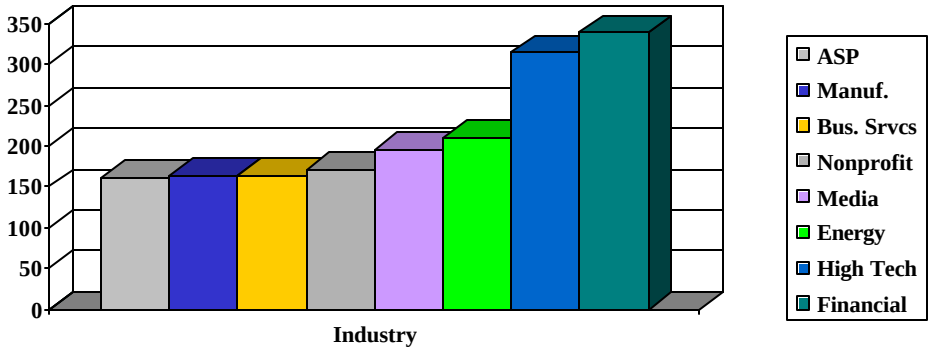
[5] This figure represents a yearly trend within the United States only.

[6] Published in a 2001 report by Celent Communications. The projections were made using data from the Federal Trade Commission.

[7] Network shutdown.

computer crimes division, the National Infrastructure Protection Center (NIPC), notes that many banks are paying off extortion demands for fear of risking their reputations and losing their customer bases to competitors. The Egghead hacking incident of 2001 represented a case of extortion. Hackers penetrated a database containing 10,000 credit card numbers and then demanded that the company pay them a large sum of cash to protect against the posting of those numbers in a chat room. Despite hackers' assurances to the contrary, every one of those compromised cards was charged a twelve dollar fee.

Figure 3. Hack Attacks in Asia (by Industry)



Source: Riptech Study 2001. ASP = application service provider.

Viruses are another computer-transmitted disease that swiftly compromises a system's integrity. A virus sets up residence in a system, and it is virtually impossible to kill it without replacing the infected parts of the system. Viruses did not exist before the early 1980s. Only recently have countries implemented legislation that makes infecting a system with a virus a crime.[8]

Box 1. Identity Thief: Abraham Abdallah

The most infamous of all identity thieves was Abraham Abdallah, a Brooklyn busboy. When police arrested him in March 2001, he had *Forbes* magazine's issue on the 400 richest people in America, as well as Social Security numbers, credit card numbers, bank account information, and mothers' maiden names of an A list of intended victims drawn from the issue, including Steven Spielberg, Oprah Winfrey, and Martha Stewart. Abdallah is accused of using Web sites, e-mail, and offline methods to try to steal the celebrities' identities as well as millions in assets. In May 2001, the Justice Department said in a statement to a congressional panel on Internet fraud, "Identity theft is the nation's fastest-growing white-collar crime." John Huse Jr., the Social Security Administration's inspector general, testified that the misuse of Social Security numbers in fraudulent activity is a "national crisis."

Source: New York Electronic Crimes Taskforce 2001

The banking system is no more vulnerable than the securities or the insurance industries. The U.S. Treasury recently discovered an infiltration of the electronic distribution system for its securities (see Box 2). In this case, defects in the risk-management processes employed by U.S. Treasury Direct in permitting access led to a situation in which one individual who was not creditworthy was almost able to compromise the whole system.

[8] Robert J. Morris wrote a computer program known as a worm that brought U.S. computers to an abrupt halt in 1988.

Box 2. U.S. Treasury Direct: The Case of Louis Lebaga

In what is now a formal indictment, Louis Lebaga is accused of manipulating the Treasury Direct online system for auctioning U.S. government debt in order to obtain $1.3 billion of U.S. securities at the end of January 2002 in an attempt to defraud the U.S. Treasury and Union Bank of California (UBOC). He was able to open a deposit account at a bank and also establish a Treasury Direct account. He was able to make what amounted to a very large number of bids for U.S. Treasury bills amounting to $160 million and 231 bids for U.S. Treasury notes totaling $1.155 billion between January 29 and January 30. He could do this because the Treasury Direct system provides for no explicit cutoff with respect to the number of bids that one retail investor can make, and it does not require the explicit posting of cash and collateral. On the first issue date for the securities on which he bid, Lebaga was able to get $160 million in securities delivered electronically by the Federal Reserve (the fiscal agent for the Treasury) to a bank account at the UBOC and to have funds transferred electronically to pay for the purchases. After UBOC realized that good funds were not in the account, it notified the Federal Reserve, and the funds were returned the following day. Note, however, that if Lebaga had not wanted to carry out more transactions, he would have had more time and options to transfer funds or services.

Further, Lebaga was able (because of human error and defects in the U.S. Treasury Direct system for checking documentation of users) to obtain this electronic transfer of funds without adequate credit checks. On arresting Lebaga, law enforcement authorities learned that he was $2,000 in arrears on his rent and that eviction papers had been served. The reality is that this one individual could have used these techniques to effectively compromise the Treasury Direct system. It is interesting to note that both Brazil and the Philippines have developed electronic distribution systems for government securities, catering to retail investors.

Source: John Frazzini, Special Agent for U.S. Secret Service Financial Crimes Division. Interview on April 8, 2002.

Both examples in the boxes illustrate that the overall risk-management system permits a breach. Usually the problem is not the result of the adoption of a specific technology but happens because appropriate risk-management processes were not implemented.

Trends in cyber crime reveal significant growth. Attacks on servers doubled in 2001 from 2000. The 2002 CSI/FBI Computer Crime Survey[9] reported that 90 percent of organizations in the United States (including large companies, medical institutions, and government agencies) detected security breaches. Moreover, 70 percent in 2001 versus about 60 percent in 2000 reported serious security breaches such as theft of proprietary information, financial fraud, denial-of-service attacks, and compromising of networks. In most of these cases, the organizations cited their Internet connection as the critical point of attack. The 2002 CSI/FBI Computer Crime and Security Survey also indicated that 273 companies lost more than $266 million. Most important, according to U.S. law enforcement authorities, these numbers are likely to understate actual intrusions and associated losses. When considered worldwide, these trends are even more troubling, given the relative sophistication of the U.S. security industry and the protections employed by financial services providers.

In the United States, a 2001 CSI/FBI Computer Crime Survey identified the following five major reasons organizations did not report electronic intrusions to law enforcement:

- Negative publicity.
- Negative information competitors would use to their advantage—for example, to steal customers.
- Lack of awareness that they could report events.

[9] See http://www.gocsi.com/

- Decision that a civil remedy seemed best.
- Fear among IT personnel of reporting incident because of job security.

Lack of accurate intrusion reporting to regulators and law enforcement is the core reason that issues related to electronic security are not being recognized as an immediate priority.

II. The Electronic Security Industry

Today's electronic security industry boasts an ever-growing array of companies. The types and numbers of choices can be confusing for the expert and overwhelming to the novice. These companies are involved in every facet of securing the networks used by financial services providers. They range from those that provide active content filtering and monitoring services (even virus detection companies are an example) to those that undertake intrusion detection tests, create firewalls, undertake penetration testing, develop encryption software and services, and offer authentication services.

In scope, the e-security industry increasingly is becoming a worldwide presence as it grows parallel with the expanding connectivity to the Internet. The growing integration of technologies among the Internet, wireless, Internet provider (IP), telephone, and satellite will also present new challenges for electronic security and the structure of the financial services industry and e-finance.

From the vantage point of financial services providers, the earlier the security is built into the design process, the greater will be their return on investment in security-related services. For example, studies show that spending $1 to fix a vulnerability during the design process saves $99 of the $100 that must be spent later when the system is implemented (See Berinato 2002; Soo Hoo 2001). This cost avoidance or cost savings makes or breaks many IT projects. The increasing extent to which technology platforms drive financial services and the increasing rates at which computer electronic security incidents are occurring emphasize the importance of using risk management in making business decisions to avoid greater future costs.

Electronic Security Vendors

A rich variety of vendors operate in what is becoming a global industry for electronic security. Many types of companies operate in this industry. In the United States alone, $5.1 billion in security software was sold in the year 2000—a 33 percent increase over the prior year.[10] These companies are involved in every facet of securing the wide area networks over which financial services are provided. The following is a brief description of the major categories of vendors. (See also Figure 3.)

Active Content Monitoring and Filtering.[11] Companies involved with active content monitoring and filtering produce tools that examine for potentially destructive content material entering a network. These vendors provide tools to monitor all content entering a network for malicious codes, such as harmful attributes. Trojans, worms, and viruses are methods used to deploy an attack once the perpetrator enters the system. Viruses are programs that infect other programs on the same system by replicating themselves. Virus scanners are critical in mitigating

[10] See Cunningham, "Digital Security: Heightened Risks Demand Innovation," *Red Herring*, July 2001.
[11] For more details on this facet of the industry, see Annex II.

these attacks. Vendors of virus scanners provide software that scans and cleans networks and is periodically updated.

Intrusion Detection Systems Vendors.[12] Companies that produce network intrusion detection systems provide products to monitor network traffic and alert the systems administrator with an alarm when someone is attempting to gain unauthorized access.

Firewall Vendors.[13] Companies that produce firewalls provide a virtual "security guard" at the gate of the customer's facilities. A firewall is a system that enforces the access-control policy between two networks. Vendors create these virtual guards to protect a network's integrity.

Penetration Testing Companies.[14] These consulting organizations simulate attacks on networks to test for a system's inherent weaknesses. They then patch the holes found during the simulated attacks. Typically, vulnerability-based scanning tools provide a current snapshot of a system's vulnerabilities.

Cryptographic Communications Vendors.[15] Vendors who supply this product enable the client company to protect its communications with an encryption envelope. Encryption uses complex algorithms to shield messages transmitted over public channels. It provides safe passage from point A to point B. When the message reaches its destination, the recipient uses another algorithmic key to open it. It is highly recommended for use by mobile workforces and/or large noncentralized corporations or institutions.

Authentication Vendors. Authentication asks users such questions as "Who are you?" and "Are you allowed to do that?" and permits a user to access the system only if these questions are answered correctly. This type of service can be broken into four general categories: passwords, tokens or smart cards, biometrics, and encryption. (See Annex I for more details.)

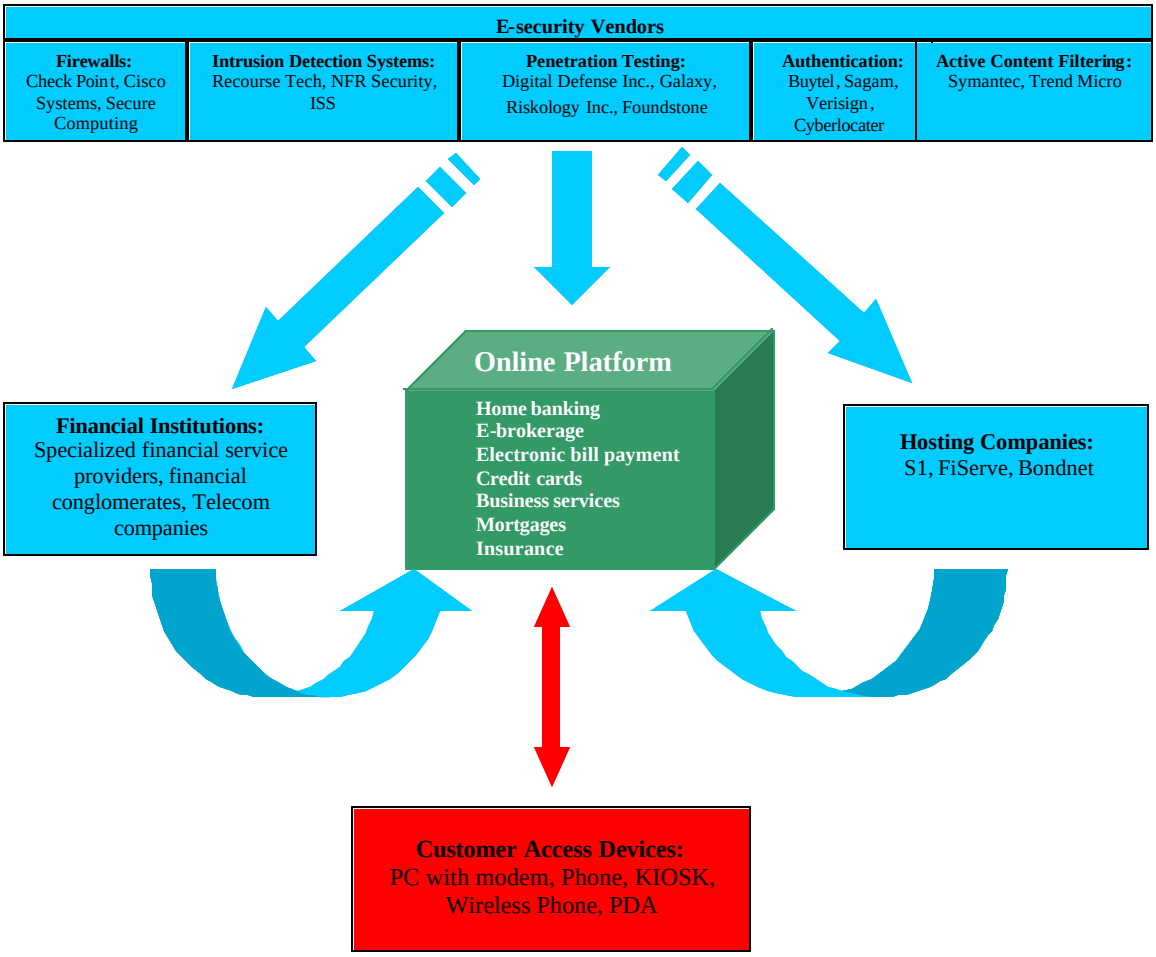
Links to E-Finance

Because E-security companies are becoming increasingly global in nature, it is important when designing public policy to understand the links between such companies and the electronic finance industry. Figure 4 provides a stylistic example of some of the links among the many types of vendors of electronic security services and financial services providers.

Figure 4 also shows a potentially disturbing reality about the electronic security industry. One vendor may provide multiple services to several interlinked customers. For instance, a vendor may provide security to the financial services provider's online platform. This same vendor also may provide security services directly to the bank for its offline computer systems. In addition, it may supply security services to the hosting company. Telecommunication companies in many emerging markets provide hosting—or what many refer to as "e-enabling services"—to the banking community. By establishing a convenient online platform that customers can access through a variety of electronic devices, these hosting companies (e.g., ISPs) have become targets of organized crime.

[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Ibid.

Figure 4. E-Security Industry and E-Finance



In many emerging markets, the telecom company may have an interest in or own outright the ISP provider and the hosting company and may provide various forms of financial services as well. Moreover, many telecom companies also have multiple interests in many different forms of technology providers, from fixed-line telephony to wireless to satellites. This industry structure should raise concern—it signifies the need to discuss and debate difficult public policy issues now, such as competition policy, and how these issues might be addressed in designing new legal and regulatory elements of the present frameworks (see Claessens, Glaessner, and Klingebiel 2002).

Along with a complex industrial organization, convergence in technologies will present special challenges in the design of public policies relating to electronic security. Specifically, increasing points of vulnerability will exist, and any well-designed electronic security system must address them. These new points of vulnerability might include the potential interfaces between customer access devices, such as a PC with modems, land-line phones that can be linked with any Internet platform through voice recognition, wireless phones, or personal digital assistants (PDAs) with an online platform. The point at which the message leaps from one

channel to another is the point at which it is most vulnerable. Hence, financial services providers will need to address a much wider array of risks and expend effort to define liability, and public policymakers will need to examine the impacts of potential weaknesses, given what is already a complex e-finance industrial structure.

Box 3 highlights an inherent conflict: The need to secure systems against physical risks that can involve use of multiple technologies in different locations runs up against the fact that the most distributed and decentralized networks are more vulnerable to interception and unauthorized access at the point of interface. As technologies converge, development of more effective standards for securing such points of interface will become far more important.

Box 3: Evolution of Technology and International Standards

A fundamental security dilemma is embedded in global information networks. The global IT network infrastructure (i.e., the physical machinery that allows electronic linkages on a global scale) is on the one hand most secure and immune to destruction by natural disasters or terrorist and cyber-criminal attacks when it is most distributed and decentralized. After the great Kobe earthquake and the destruction of all fiber optic connections in the city during that natural disaster, the Japanese government proceeded to install satellite VSAT[16] terminals at post offices throughout the country to ensure the basic integrity of national communications.

On the other hand, the most distributed networks are most vulnerable to interception and unauthorized access. Often maximum vulnerability to interception exists at the point where fiber, coax, satellite, and terrestrial wireless systems interconnect. Air interface standards are but one example of modern telecommunications and IT systems open to interception.

A few years ago, telecommunications were projected to follow the model known as the "Negroponte Flip," whereby all narrowband traffic would go onto wireless (and largely mobile) systems, but all broadband service (in order to conserve frequency) would go onto fiber networks. This model was focused on the United States rather than the rest of the world, and it was technology-driven. In fact, the popularity of wireless systems (both satellite and terrestrial wireless) has continued to increase, and the market has demanded more and more Direct Broadcast Satellite (DBS) satellite entertainment service and broader band wireless now in the form of third generation systems and soon fourth generation systems. The market has thus actually followed the trend of the so-called Pelton Merge, which calls for continued improvement of "seamless interface standards" that allow the smooth interconnection of fiber, coax, terrestrial wireless, satellites, and other new and evolving technologies such as high altitude platforms. The challenge is thus to develop standards that allow easy and reliable interconnection and yet also protect security.

One example of a standard is the ISO seven-layer model of telecommunications. The current standard, however, does not really treat the security issues in the seamless interface between these technologies. Hence, it is necessary to consider the creation of a new layer that is truly secure, based on a 256- or even 1024-bit code that is constantly updated. Further study would be needed to determine whether the ultimate solution is a separate layer or the reengineering of part of an existing layer that could be devoted to this task. The extension of security identification module (SIM) smart cards that could be used throughout the world would also be a major step forward.

Source: Dr. Joseph Pelton, Executive Director of the Clarke Institute

One example of how convergence of technologies creates vulnerability occurs when a wireless Groupe Spécial Mobile (GSM) phone is used to initiate a transaction through an interface with the Internet (e.g., via indicating transactions on the online platform of the financial services provider).

[16] **V**ery **S**mall **A**perture **T**erminal, but more simply put it describes a small satellite terminal that can be used for one-way and/or interactive communications via satellite.

Specifically, a secure way of integrating between the two technologies—GSM and the Internet—is needed. This typically requires seamless connectivity and an integration of standards, including those for security worldwide, that are not in place today. Wireless messages have to travel through a gateway,[17] which channels them to a wired network (e.g., the Internet) for retransmission to their ultimate destination. At the gateway, the message sent and encrypted in GSM using what is called Wireless Application Protocol (WAP) and the associated use of Wireless Transport Layer Security (WTLS) must be converted into the industry standard for secure messaging over a wired network—secure socket layer (SSL). At this point (in the gateway), the message will be unencrypted before being reencrypted, and there is vulnerability

III. Electronic Security Infrastructure in a Risk-Management Framework

Regulation of the Electronic Security Industry

To develop a framework for thinking about the public policy issues that arise in examining electronic security, it is necessary to identify the fundamental source of "public interest" and the case for regulation in this area. For several reasons, electronic security warrants some form of public intervention now.

First, financial services and the payment system in particular, or banking more broadly, constitute one of the eight identified areas of "critical infrastructure."[18] A compromise of the payments system caused by illegal access and hacking can have broad ramifications for an entire economy, as could similar impacts in other critical infrastructure areas, from transportation to energy, and so on. Hence, the public interest and welfare are potentially at risk when business and commerce fail to meet certain minimum electronic security standards.

Second, the role of government and law enforcement can be justified on much more familiar classic market-failure grounds.[19] Specifically, the existing base of information that supports projections about the extent of the electronic security problem is substantially flawed. This is because financial services providers, hosting companies, and other enabling companies have inadequate incentives to report intrusion or penetration information accurately, given their legitimate concerns about the disclosure of such information and its potential damage to both their reputation and public confidence in their business. In this case, insurance markets cannot price the insurance risk in an actuarially fair manner. Similarly, information technology is subject to large increasing returns to scale on both the demand side and the supply side (see, e.g., Shapiro and Varian 1999). Market outcomes in such industries (including financial services, which is heavily dependent on IT) will tend to be somewhat concentrated and often will require industry standardization and coordination.

[17] For more detailed analysis of this problem, see Annex III.

[18] The Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (PDD-63), issued by the Clinton Administration in 1998, provided a starting point for addressing cyber risks against the United States. This directive identified the critical sectors of an electronically dependent economy and assigned lead agencies to coordinate sector cyber-security efforts. This directive identified eight sectors—finance, transportation, energy, water, government, aviation, telecommunications, and emergency—presenting the vision that "the United States will take all necessary measures to eliminate swiftly any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."

[19] Classic reasons for a failure in a market are asymmetric information, increasing returns to scale, and network externalities. See Bator (1999), Varian et al. (1999), and Kahn (1999).

Any approach to defining public policies through law and regulations (including prudential regulations, such as capital standards) must account for the impacts electronic security considerations or the lack thereof have on a set of risks. Specifically, financial services providers react to incentives. In many cases, analysts pressure financial services providers to produce targeted returns, while at the same time pushing them to outsource in order to reduce costs. Meanwhile, technological advances have created a much more complex inter-relationship between electronic security and risks of different types. In effect, electronic security and electronic finance can have an impact on operational risk, risk of identity theft, fraud and extortion, credit quality deterioration, and systemic risk, and can even have implications for the risks in undertaking failure resolution.

Operational Risk. Inadequate electronic security can result in interruptions of service and—in some cases, depending on the nature and adequacy of backup systems—even the loss of critical information. As part of managing operational risk, financial services providers worldwide need to pay greater attention to the way they secure their IT systems. As discussed in Section VII, the risks involved in electronic security often relate to extortion and reputation risk, which usually are not specifically taken into account in the allocations set aside to cover operational risk.

Risk of Identity Theft, Fraud, and Extortion. As noted in Section II, penetration by hackers often leads to extortion demands. In addition, identity theft is a growing concern for e-finance service providers. Its growth has been rapid, but as in the case of hacking, it is not reported in a timely manner or accurately; thus, its growth may be considerably understated. This problem is not unique to financial services—it also affects the integrity and reliability of the credit information gathered and assessed by credit bureaus, downstream to credit decisions.

Risk of Credit Quality Deterioration for the Financial Services Provider. Although not often acknowledged, a substantial denial of service or long-term intrusion that results in fraud, impersonation, or corruption of data can effectively cripple a bank's operations for a period of time. If that time is sufficient, it can irreparably damage the bank's reputation and possibly compromise its credit standing. Because market participants' confidence is critical, such an event could have a pernicious impact in a relatively short time.

Systemic Risk. One of the most important links between e-finance, e-security, and risk is the systemic impact that the associated risks can have on the related payment systems through interaction with compromised networks. Appropriate security should be proportional to the value of underlying transactions. For this reason, in the case of large-value clearinghouses, extensive electronic security is or should be in place. Any intrusion or interruption in a payment system's electronic messaging could easily create significant system-wide exposure.

Risks in Failure Resolution. A final form of risk associated with the delivery of e-financial services and security relates to the risks introduced when a brick-and-clicks or wholly Internet-based bank fails. Here the process of closure itself is difficult to define and even more difficult to implement if the entity has its servers in offshore centers. Closure in this case would require extensive cross-border coordination among authorities in what could be numerous disparate jurisdictions. Cooperation, and thus closure, may not be feasible with the speed that can be applied in the case of a non-Internet-based bank. At the point of intervention, if the records and other essential information about digital assets are not preserved under well-defined guidelines, and if they are not secured or cannot be retrieved from servers, then, at the very least, claimants' rights may be compromised.

Trade-Offs: Security, Quality of Service, Privacy, Technological Innovation, and Costs

Designing public policy in this highly complex area requires balancing a number of essential trade-offs in creating legislation and regulation. This even applies in designing standards and guidelines that might be used by a self-regulatory agency or by an official agency.

Security and Costs. Security should always be proportional to the real value of the underlying transaction. Given this proviso, it appears that when transaction value is small, no clear economic or risk-management case can be made for employing the most sophisticated electronic security regimes when a less expensive form of security will yield the same return. For example, a financial services provider would not want to use an expensive and cumbersome authentication process, such as public key infrastructure (PKI), for small-value transactions when tokens or other simpler forms of authentication will mitigate the risk of theft, and so on, to an acceptable level.

Security and Quality of Service. Similarly, trade-offs exist between the convenience or quality of service, as computed in terms of speed and the extent and degree to which security is used. The more complex the security process used, such as PKI, the longer the transaction takes to be completed. Advances in these technologies are lessening this trade-off. Over time, effective authentication or encryption systems will be available that do not slow the speed of transactions and do not disparage the quality of service. Moreover, one can argue that confidence in the security of services is an essential aspect of quality in providing financial services.

Security and Technological Innovation. For electronic security systems to be effective, it is important to ensure that private parties agree to certain standards and guidelines. But the proliferation of technologies that can be used to transmit information and their rapid rate of integration inherently creates a reluctance to adopt standards or guidelines. Technological innovation can be stifled and customer service can suffer if security standards are not sufficiently flexible and technology-neutral. As will be noted in later sections, even the definition of an electronic signature needs to be very carefully designed so as not to preempt the use of a number of alternative technologies. In other words, the concept of technology neutrality is an important one to adopt when formulating legislation and regulation. (See Section VI.)

Security and Privacy. Ironically**,** the need for more effective electronic security may sometimes conflict with and negatively affect the user's privacy. Inadvertently, it may also affect the privacy of third parties who are identified in affected information. This tension is natural, and it is not new. On the one hand, certain types of electronic security services may be consistent with protecting privacy (e.g., programs such as cyber patrol). On the other hand, security may be needed to track and verify the user's movements. In other cases, however, the person undertaking the transaction may want to remain anonymous as part of a trading strategy. Developing the proper balance between security and privacy is a delicate matter. It often is decided within a cultural paradigm. Sometimes this means that something considered private in one culture may not be deemed so in another. Moreover, the laws (e.g., bank secrecy provisions) often compromise the ability of the authorities to investigate properly and take enforcement actions in complex electronic crime cases.

The Pillars of an Overall Framework

This paper is built on the concept that trust and confidence of market participants is a key component of a robust economy. Given this assumption**,** seven fundamental pillars are needed to sustain a framework of reform and to improve the security of the market. These are

- An adequate legal and enforcement framework in certain critical areas.
- Adequate treatment of electronic security in the case of payments services and those that undertake to provide e-enabling services to financial services providers, such as money transmitters.
- An effective supervision and prevention regime to manage emerging electronic security requirements.
- Public partnerships with private insurance companies to monitor the efficacy of security systems on a macro level and promote the development of minimum standards for electronic security.
- Public partnerships with private entities to develop and adopt transactional security levels for transactional information and electronic signatures, together with criteria to protect document and data classification standards.
- Public partnerships with private entities to develop and maintain accurate incident databases and a related reporting framework for electronic security incidents to be used in assessing systemic risk over time.
- Public education about how technological change and related electronic security risks need to be addressed.

Issues usually arise in each of the areas identified above when the challenges posed by electronic security are addressed in a more systemic manner. The sections that follow explore each of these pillars.

IV. Pillar I: Legal Framework and Enforcement[20]

Laws, Policies, and Practices Bearing on Electronic Security

Countries adopting electronic financial services should address and incorporate security concerns as they develop policies, laws, and regulations. In this way, they can build a security framework that will support the safe and sound operation of their institutions and combat crime and cyber terrorism. The following areas of law, at a minimum, should be included in any e-finance legal framework:

- Electronic transactions and commerce law
- Payment systems security law
- Privacy law
- Cyber crime law
- Anti–money laundering law

These five categories of law address the *basic relationships and transactional activity* that flow through the e-payments system.

The cornerstone of an e-finance legal framework is recognition of the legal validity of electronic signatures, transactions, or records. Further, these laws should prefer technology-neutral solutions, provide basic consumer protections for electronically based transactions, promote interoperability, and address records retention. Two basic models exist: the act developed by the United Nations Commission on International Trade Law, titled UNCITRAL, and the Uniform Electronic Transactions Act (UETA). An electronic commerce law

[20] The authors thank Edward Gilbride, Counsel for the Federal Deposit Insurance Corporation, for very helpful written inputs in the context of the discussion in this section.

might address all non-consumer-related financial transactions and records. It should focus on governing conduct with consumers and on basic financial payment mechanisms such as EDI, EBT, EFT, and ETC. Specifically, it defines what constitutes a secure financial services system in an open network architecture and requires entities to practice due diligence.

Electronic Transactions and Commerce Law: The past seven years have produced tremendous growth in electronic-commerce-related legislation. In 1995, only a handful of countries had basic computer or intellectual property laws. Today, almost every country has enacted an electronic signature or electronic transaction act. The basic elements of these laws are the same, with minor variations. Most of the laws use UETA, promulgated in the United States by the National Conference of Commissioners on Uniform State Laws (NCCUSL), or UNCITRAL.

Significant differences exist in the provisions of UETA and UNCITRAL, but the objectives of both are the same: to promote electronic commerce and to ensure that electronic signatures, however they may be defined, have the same effect under the law as manual signatures. For example, UETA defines an electronic signature as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." UNCITRAL defines an electronic signature as "data in electronic form in, affixed to, or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message." Each provides a different perspective on timing and intent. UETA presumes that by signing the document, the signer intends to be legally bound. Its wording creates a presumption in favor of the validity of the contract. UNCITRAL, in contrast, uses permissive language, creating no presumption in favor of the contract. Further it should address the issues of record management and record retention.

With the proliferation of electronic signature and electronic transaction legislation over the past decade, electronic commerce has come into its own legally. In general, an electronic signature has the same force and effect as a manual signature in most of the world. The latest country to adopt electronic signatures was Russia, which enacted its Electronic Digital Signature Law on January 16, 2002. Typically, the law changes significantly more slowly than many other parts of a culture. The law appears, though, to be trying to adapt to electronic commerce needs as quickly as the world is coming online. This is a major phenomenon that raises issues of importance beyond the scope of this paper.

Payment Systems Security Laws. Though most countries have laws in place to regulate different components of the payments system, no country has yet addressed payments systems issues comprehensively. Payment systems legislation should identify, license, and regulate any directly related payment system entities, such as money transmitters and ISPs. It should require such elements to operate in a safe and sound manner so as to protect the integrity and reliability of the system. It should require the timely and accurate reporting of all security incidents, including all electronically related money losses. Finally, it should require all payment system entities to adhere to a documented security program and should encourage some form of shared risk protection.

Privacy Laws. Clearly, privacy is an area of the law that is undergoing considerable scrutiny throughout the world. It is an issue of fundamental importance, reflecting the very substance of our cultural identities, values, and mores, and it must be handled with the utmost care. Poorly considered decisions made in this arena may haunt us for years to come.

On the issue of privacy protection, some countries have chosen to legislate on a functional or piecemeal basis, while others have taken a more encompassing, process-oriented approach. Two approaches are also being used on the issue of consent. The first is to assume consent unless the party affirmatively chooses not to have the information sold or used for other purposes. The second is to assume that the party has not consented to any use of the information unless the party gives that consent. The United States follows the first approach in both areas. The European Union (EU) exemplifies the second in each area and continues to be the leader in providing privacy protection to its citizens with its 1990 EU Directive on Data Collection.

No matter which approach is used, at a minimum, privacy laws should embrace the Fair Information Practice Principles of notice, choice, access, and security. They should address privacy rights concerning any data collected, stored, or used by an entity for different purposes, in particular those uses that could affect a person's basic human rights, such as criminal, financial, business, or medical uses. In practice, privacy laws would require entities to do the following: advise persons about how data will be used; collect only the minimum data needed to complete the transaction or record at issue; use the data only for those purposes that it advised the person it would be used for; and permit persons to view any information collected and dispute the validity of any such information with timely corrections. Finally, the law should impose restrictions on any entity collecting, holding, or disclosing information in a form that would allow identification of the person it relates to, however that may be defined.

In practice privacy laws would require information gathering entities to advise persons from where they are collecting the information and how the data will be used.[21]

Cyber-Crime Laws. Significant debate is transpiring in legal communities worldwide over the impact of cyber crime on fundamental concepts of law, such as jurisdiction, and in particular on how the electronic culture is changing traditional paradigms. Financial cyber crime is a top priority in this dialogue because, more often than not, it requires intense international cooperation among what can be an overwhelming number of law enforcement agencies and regulators from different countries. Because no country is immune, every country should benefit from pooling resources to address this problem. But, more than any other aspect of computer law, financial cyber crime tests the continuing validity of the industrial regulatory and law enforcement model. Because of the underlying complexity of such cases and the overlapping jurisdictions of authority within a country, one of the first things the laws should address is who or what has authority and responsibility for these cases. A significant cost avoidance could result from such reform, and money saved could be invested in trained resource experts and the tools needed to investigate, prosecute, and punish cyber-crime perpetrators. Substantively, the laws should address abuses of a computer or network that result in loss or destruction to the computer, the network, or people, and should include provisions for restitution for associated losses.[22]

A December 2000 McConnell International survey provides a snapshot of the state of computer crime legislation worldwide. It examined the legal frameworks of 52 countries to determine each one's ability to prosecute perpetrators of 10 types of computer crime. The survey

[21] This data should be used only for those purposed that were intended. They should also permit the persons from whom they collected the information to view it and provide a process by which,such persons could dispute the validity.
[22] The United States has enacted various computer intrusion laws that treat identity theft and computer-initiated fraud as criminal offenses with severe penalties. Recent legislation grants individual banks the power to freeze customer accounts if criminal activity is suspected. Penalties for fraud and related activities perpetrated in connection with computers can include imprisonment of up to 25 years (see http://www.cybercrime.gov/cclaws.html).

showed that a patchwork of outdated and inconsistent laws effectively functions as a shield from prosecution for cyber criminals who attack electronic systems and information.[23]

For countries looking to develop cyber-crime legislation, the Council of Europe provides some guidance. In 2001, it developed the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security. The treaty also provides for a series of powers and procedures, such as the search of computer networks and interception.[24]

Anti–Money Laundering Laws. Worldwide, money-laundering is recognized as one of the most potent forces threatening political and economic stability. Since 1990, the Financial Action Task Force (FATF) has spearheaded the adoption and implementation of measures designed to counter the use of the financial system by criminals (see http://www1.oecd.org/fatf/). It established 40 recommendations that set out the basic framework for anti–money laundering efforts and are intended to be of universal application. In 1996, the FATF recognized the link between cyber vulnerabilities and money laundering when it modified its 40 recommendations 1996 to include number 13, which states, "Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes." The points addressed in cyber-crime laws also apply here. Substantively, at a minimum, these laws should define money laundering and should commit to international cooperation in the investigation, prosecution, and punishment of such crimes pursuant to the guidance provided by the FATF. The FATF regularly reviews its members for compliance with the 40 recommendations, with the result that the recommendations are now the principal standard in this field.

Enforcement Powers

The ability to enforce the laws and regulations within and across boundaries is as important as providing an adequate legal and regulatory framework within which to prosecute perpetrators and penalize those entities operating in an unsafe and unsound manner. To achieve enforcement, many countries need to take a number of critical steps.

Regulatory enforcement reforms should address, at a minimum, varying degrees of cease-and-desist orders and compliance actions. Cease-and-desist orders could range from removal of the entity from the online system until it comes into compliance to closing the entity down. While a financial services provider may not have access to online activity, it still may be conducting unsafe and unsound operations to such an extent that it is jeopardizing other entities.

Without a concerted international cooperative effort, e-finance hackers will commonly move to jurisdictions with the most lax legal and enforcement frameworks.

Access, availability, and interoperability should be the mantra to guide financial supervision and enforcement efforts. The traditional regulatory structure must expand to include all entities directly related to the delivery of financial services. This entails everything from ISPs to ASPs, software and hardware vendors, and security providers.

Legislation needs to incorporate these providers into the regulatory and enforcement net. Moreover, professional liability needs to attach to these providers, to the directors who contract

[23] See http://www.mcconnellinternational.com/services/securitylawproject.cfm

[24] See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

with them, and to the lawyers and accountants who provide services to them because, in the new paradigm, all are indispensable to the institution's ability to provide financial services. One approach might require that these providers be bonded, licensed, and subject to periodic audits and examination under the appropriate regulatory scheme. This would create a relevant basis from which to undertake enforcement actions. As stated already, traditional regulatory schemes are outdated, and as currently configured they cannot adequately address the new components of the payments system to determine whether a financial institution is operating in a secure manner.

V. Pillar II. Electronic Security of Payment Systems

Money Transmitters: Background

Convergence and integration are the keys to the revolution in money movement and to wholesale and retail payments services. Convergence of the telecommunications, computer, and financial services industries is changing the fundamentals of industrial organization in the financial services sector, as noted in Section III, redefining traditional boundaries and jurisdictional limits of responsibility because of shifting legal, regulatory, and financial concepts. The industrial age gave rise to certain agreed-upon regulatory concepts by which the telecommunications and financial services industries operated. Regulation of telecommunications was based on public safety, interest, and welfare through the use of universal access and service. The regulation of banking was based on safety and soundness with nondiscriminatory access to credit opportunities. Convergence, however, requires reassessment of this regulatory paradigm because of the necessity for universal access in a safe and sound environment**.**

Convergence and integration help realize the telecommunication and financial services goals of access, availability, and interoperability. Access to the financial system was once limited to a few complex protocols. Now anyone can access the system using microwave, wireless, satellite, public switched network (PSN), computer, IP telephony, interactive television, ATM, or brick-and-mortar structures. In addition, these advances have redefined and eliminated time so that the financial system is accessible to anyone, anytime, anywhere, using cash, debit card, check, credit card, stored value card, or smart card. Money is now interoperable, as telecommunications and computers facilitate the conversion from one currency to another simply by the push of a button. Eventually, even the servers of a telecommunications company, in addition to facilitating cellular calls, will be used for effecting payments between prepaid cell phone subscribers.

Under this new industrial structure, and given the increased outsourcing of operations, the following questions about the design of regulations seem reasonable: Who or what is a money transmitter? What is an ISP? Should the regulatory framework deal only with core financial activities, or should it include outsourcing entities? If it increases, what is the case for regulating these entities, and what agencies need to play a role or have ultimate responsibility? Such fundamental questions must be answered to create effective incentives for money transmitters and ISPs to adopt adequate electronic security. The regulatory objective must be clear and simple.

Who or what is a money transmitter? Today, the set of entities involved in money transmission or payments is more difficult to define than one might expect. These entities are not well regulated or supervised in many countries, even if they can be defined. For the purposes of this paper, a money transmitter is any commercial enterprise that engages in the transfer and exchange of monetary instruments and currency.

Money transmitters may perform a variety of services, including money order issuance, wire transfers, currency exchanges, check-cashing, and check-presentment. More recently, money transmitters have been providing electronic check-presentment services and point-of-sale money payment order information to the accepting bank. Money transmitters operate outside the depository institution but are often are associated in some way with one or more depository institutions in a downstream relationship.

What is an ISP? Whether an entity is an ISP can be difficult to determine under existing law. ISPs are not regulated in most countries, and countries that have tried to regulate them have experienced significant backlash. One recent example involved Australia's Broadcasting Services Amendment (Online Services) Act 1999, referred to by its critics, who claim it is overly broad, as the Internet Censorship Act. It has received international attention and is touted as an attempt by one country to impose a censorship regime on the Internet.[25] A number of entities, including financial services providers, could fall under its definition of an ISP.

This paper suggests that analysis of the payment system at large shows that hosting companies/ISPs have become a critical sector and can have a direct impact on the security of an institution. As an example, the use of multiple channels to distribute financial services or make payments has expanded the circle of providers to include a Web site hosting service, a third-party software developer to plan and implement the Web site, application software or service providers, a third-party processor to facilitate information movement from the Web site to the financial institution's network, a customer service call center, and one or more ISPs or money transmitters. Use of these new channels means that the financial services sector now broadcasts; publishes; provides or uses e-mail, Internet services, network services, and entertainment; hosts online forums; and uses bulletin boards. As the nondepository institutions involved become more varied, defining who is a money transmitter becomes more complex and requires a two-part test. First, to what extent is an institution relying on that provider to transact and deliver financial services? Second, to what extent can the provider have an impact on the payment system?

The expansion of the types of entities involved in money transmission creates both greater opportunities and more complex liabilities and responsibilities. Converging technologies have opened access to the payment systems. Disintermediation of the financial services sector has created an open competitive environment to all aspects of the payments system. Open access has resulted in the proliferation of money transmitters and their partnering with ISPs. With these developments, challenges have increased for electronic security of payments.

Safety and Soundness for Money Transmitters and ISPs

The question of how to ensure safety and soundness in the case of ISPs and money transmitters must address at least five basic, generic problems:

1. Lack of definition
2. Lack of reporting requirements
3. Limited or no regulation
4. Limited or no warranties, indemnification, and liabilities
5. Lack of security as a necessary element for service providers

[25] The Online Services Act defines an ISP as anyone who provides an Internet carriage service that is used for (a) the carriage of information between two end-users outside the "immediate circle" of the supplier, as defined in the Commonwealth Telecommunications Act of 1997—and when one person uses an Internet carriage service to view the content of a second person (e.g., by visiting a Web site), both of these people would be considered end-users of that carriage service; or (b) the carriage of information simultaneously to more than one end-user, at least one of whom is outside the immediate circle of the supplier.

Toward a Working Definition of a Money Transmitter

Money transmitters are often referred to as nonbank financial institutions or money services businesses. Numerous definitions exist for this payments system "service" sector. Generally speaking, and for the purposes of this paper, money transmitters are commercial enterprises engaged in the transfer and exchange of monetary instruments and currency. In the context of electronic payment systems, they typically serve as third-party automated clearinghouse (ACH) providers.

Money transmitters do not operate alone. They require access to telecommunications to transport information from point to point. Usually a money transmitter contracts with an ISP to transport the information across network lines.

Failure to require reporting or to review and expand regulations to include new money movement vehicles permits unsafe and unsound activities to use the payment system without check or prevention. Legislation should place an affirmative duty on executives to report incidents, and the intentional failure to report should carry potential punishment.

Liability of Money Transmitters

The money transmitter-ISP venture is usually structured as a layered relationship built on successive contracts, each containing no or limited liability. The money transmitter provides database software to the end-user that typically has limited or no warranties, and the money transmitter carries limited or no liability for providing the software or access. The ISP typically leases a number of telephone lines or telecommunications resources at a certain rate. The underlying service contract with the telecommunications provider is solely for leased space on the network. The network provider, typically one of the large public switched companies, provides only a transport mechanism. This arrangement is similar to right-of-way agreements for utilities or trains that allow use along the track but do not include access to the track. The ISP contracts with the money transmitter for cost-plus as a transport mechanism only, again incurring limited or no liability for this service.

The ISP may enter into a service-level agreement (SLA) with the user (i.e., the money transmitter). Industry standard norms require that the telecommunications system be operational at least 99.5 percent of the time during the service contract. The contract contains a formula for determining an appropriate refund mechanism dependent on the number of times/amount of time access falls below the service level. The money transmitter in turn assumes no liability, or limited liability, to the user. The money transmitter provides no additional value in the form of security for its service; it simply provides a type of bundled service to the user. In essence, the money transmitter charges a convenience fee. The user simply uses the money transmitter's software to create and store the payment order data, which it then sends on a periodic basis to a clearinghouse for deposit or credit to the user's account after it has wound its way through the payments system.

Money transmitters and ISPs that provide services to the financial sector should be required by regulation or legislation to provide liability. Sharing risk is a proven model in the financial services arena, and there is as yet no evidence that this would increase the basic service cost. In fact, only when service entities are required to report losses or suspected losses can sufficient information be garnered to improve pricing for e-security bonds and e-commerce liability insurance.

Lack of a Well-Organized Regulatory Framework for Money Transmitters

Until January 2002, money transmitters in the United States were not regulated at the federal level. However, they are coming under increased scrutiny, because there are now an estimated 200,000 money transmitters operating in the United States and the evidence is mounting that some are being used to launder money. In its 1998-99 annual report, the FATF noted a growing trend to use nonfinancial professional service providers as conduits for money laundering and other nefarious activities. Box 4 outlines how money-laundering concerns have triggered the need to regulate money transmitters in the United States.

As a result of the lack of standardization in regulation and oversight, many money transmitters insert significant risk into the payments system. Typically, they are undercapitalized, use little or no risk-management analysis, and are extremely susceptible to bankruptcy and failure. With the escalation of Internet-related commercial activities and the requisite need to provide ubiquitous payment system conduits, money transmitters are increasing the disintermediation of the traditional payments systems and have a higher profile in the eyes of law enforcement.

Box 4. Money Transmitters and Electronic Security

In 1996, seven money transmitters located on the east coast of the United States were indicted for accepting funds that were allegedly drug proceeds. The El Dorado Task Force, formed in 1992, is a joint federal, state, and local effort involving such entities as the Internal Revenue Service, the New York Police Department, and the New York State Banking Department. It targets industries that facilitate money laundering. That same year, the task force initiated a geographic targeting order (GTO) against 22 money transmitters in New York City and 3,500 licensed agents. The GTO required these transmitters and their agents to report information about cash transfers to Colombia greater than $750. As a result, the volume of money being transferred to Colombia dropped by 30 percent. Under federal law, the government can require a group of financial institutions within a limited geographic range to comply with special record-keeping requirements on a showing of need. Arguably, using a GTO, appropriate federal authorities could require financial services providers to report electronic losses for the same reasons.

Because the primary focus of legislative initiatives targeting money transmitters has been to deter money laundering, most of the activity affecting this industry is derived from anti–money laundering sources.[26]

Two efforts stand out:

1. The Uniform Money Services Act, adopted by the NCCUSL in 2000 and known as the Money Transmitters Act.[27] The act requires a money transmitter to obtain a license to operate; sets forth certain licensing criteria, enforcement, and compliance provisions; makes a statement on jurisdiction; and includes provisions on the scope of the act and audit and examination authority. It also contains bond provisions, minimum net worth criteria, provisions on management experience, and requirements that the money transmitter disclose prior litigation and criminal prosecution of management. Only seven states have adopted the act.

[26] See Section V for additional information on money laundering.

[27] See www.law.upenn.edu/bll/ulc/moneyserv/UMSA2001Final.htm

2. The MRTA Act, created by the Money Transmitters Regulators Association (MRTA), formed in 1989 as a state regulators organization. Though not as comprehensive as NCCUSL's Money Transmitters Act, it is still a model for dealing with the licensing and regulation of money transmitters. Only five states have adopted it.

Because so few states have adopted these acts, the United States is left with an inconsistent, tedious, and inadequate regulatory scheme. Nevertheless, those states that have shown foresight and initiative in adopting these laws should be able to collect badly needed information on this industry and provide a nucleus from which better regulation can emerge. More exploration is needed to locate the various money transmission channels and regulatory approaches other countries have used. When this paper went to press, none had been located, indicating that emerging markets are not treating these issues systematically.

The last and most promising regulatory effort is enactment of the Gramm-Leach-Bliley Act of 2001. This act affects the future definition of financial services in the United States in the following three ways:

First, the Federal Reserve Board (the Fed) is required to determine what is "financial in nature," taking into account the purposes of both this act and the Bank Holding Company Act; changes in the market and in technology; and an assessment of whether any new activity is necessary or appropriate to compete, to deliver services efficiently, and to offer customers new means of obtaining services.

Second, the Fed is required to decide whether, and to what extent, the following activities are financial in nature or are incidental to a financial activity:

- Lending, exchanging, transferring, investing for others, or safeguarding financial assets other than money and securities.
- Providing devices or means for transferring money or other financial assets.
- Arranging, effecting, and facilitating financial transactions for the account of others.

Third, the Fed may determine that an activity is complementary to a financial activity and by order or regulation deem that activity to be permissible for a financial services holding company.

The Fed has not initiated rules in any of the required or permissive areas. Nevertheless, this act has positioned the Fed to guide the expansion of regulation to include money transmitters and ISPs or any other entity that enables financial institutions to provide services. Thus, the opportunity and the need now exist to initiate global financial forums that call for harmonized approaches to these and other issues raised by the presence of the new market.

Security for Services Provided

ISPs and money transmitters do not necessarily provide additional security for their services. If either is able to offer security, the provider will distinguish between secure and unsecured services. A money transmitter called SWIFT, for example, is careful to distinguish that it provides secure EDI service only. Until a few years ago, SWIFT was a closed system. Today, it has access points to the public switched network. It continues to be one of the most secure transport mechanisms available in the global payments system. FEDWIRE is another example of a closed system, but it now is also connected to the Internet and is subject to vulnerability.

Lacking sufficient terms and conditions in the contract, a user has no way of knowing whether or to what extent an ISP or money transmitter provides security.

Great Britain passed legislation in 2000 that allows the government to track e-mails and seize encrypted Internet communications. It enables law enforcement authorities to demand records of Internet traffic and to view the content of encrypted messages. ISPs are required to set up secure channels to connect to the Government Technical Assistance Center. In turn, the government contributed $30 million to ISPs to cover the cost of installing the "black box" link to the M15 Technical Assistance Spy Center.

Actions to Improve Electronic Security of Payment Systems

The most important objective in a convergent technology environment is to mitigate risk to the extent possible in using an open, universal access architecture. This places greater emphasis on identifying and analyzing systemic risks and vulnerabilities, eliminating risks where feasible, and continually monitoring both risks and security. Few emerging markets appear to have dealt with these issues explicitly thus far. This poses the question of how to do more with less but still increase security and privacy.

In reality, the payment system has broadened and deepened, becoming far more porous and vulnerable. A system is only as secure as its weakest link. Therefore, the first defense recommendation is to enact legislation regulating all money transmitters and any ISPs that provide service to the financial services sector, requiring them to be secure. The Uniform Money Services Business Act would be a good basis for regulating these providers.

Another approach would be to use a request for proposal (RFP) process to shop for value and negotiate the needed terms and conditions in selecting providers. It is important to build in a service-level agreement with appropriate refund mechanisms, liability, and warranties to the terms and conditions.

At present, signing onto the Internet via an ISP results in an adhesion contract in which the vendor dictates all terms and conditions. The industry refers to such contracts as "User Agreements" or "Access Agreements." The contracts are posted on the Internet, and one either accepts the terms and conditions as set forth or does not use the service. Typically, such contracts require the user to check the Internet site periodically for any contract changes, and continued use of the service constitutes acceptance of the terms and conditions. Adhesion contracts, once considered unenforceable, are becoming the norm in the ISP and electronic-commerce-dominated industries, especially the financial services industries.

Another avenue of defense is self-regulation through the automated clearinghouse process or, more broadly, via specific arrangements outlining security standards in the case of wholesale or retail payment networks. Building clearinghouse rules requiring all entities to use vendors that provide an appropriate level of security and to post sufficient money or bond to cover losses would create an incentive for the parties to establish a proper electronic security standard. This approach needs to figure more prominently in the ongoing work of establishing wholesale and retail payment networks in emerging markets. Moreover, as in the case of securities regulation, central bank supervision of SROs that are responsible for retail or wholesale payments will become far more important.

Insurance coverage is yet another means of protection. Financial services entities should use insurance to protect themselves from gap loss, whereby e-risk is realized even after insurance

companies have required a financial services provider to meet specific security standards. Section VIII will examine this issue in more detail.

VI. Pillar III: Supervision and Prevention Challenges

Background: Electronic Security and E-Banking Supervision

In 1999, the Basel Committee established the Electronic Banking Group (EBG) to focus on adapting the Basel Committee Guidance as necessary to e-banking issues. Moreover, the Financial Stability Forum (FSF) has established a special overall contact group that is in the process of discussing what issues need to be addressed in the implementation of the 14 principles identified by the EBG (see Box 5).

Because e-banking is based on technology designed to expand the "virtual" geographic reach of banks and customers without necessarily requiring a physical expansion, market expansion beyond national borders significantly increases cross-border supervision challenges for bank supervisors. Although such supervisors agree that the supervisory principles of traditional banking are applicable to e-banking, changes in technology and dependence by banks on service providers magnify the level of risk. The 14 principles for risk management of e-banking issued by the EBG fall into three fundamental categories: (1) effective board and management oversight, (2) security risk issues, and (3) reputation risk issues.

The ability of regulatory agencies to regulate and supervise e-banking entities effectively in today's virtual banking environment must be strengthened to handle the special challenges of electronic security. Authentication, security control, integrity, and even incident response planning figure prominently in the 14 EBG principles. In particular, the EBG emphasizes the need for a bank's effective internal controls. Moreover, the EBG principles place liability on the banks in the event of electronic security problems with vendors. Despite this emphasis, there is still a need to make the chain of vendors involved in the delivery of electronic security services or other e-enabling services secure and to impose better downstream liability on these entities.

In many countries, a bank is subject to examination on a periodic basis. In the past, traditional examinations were done on-site and based on safety and soundness through the CAMEL rating system.[28] In addition, banks in most countries throughout the world are subject to some variant (where weights may differ) of the Basel capital adequacy guidelines. The challenges presented by electronic security breaches are not explicitly accounted for in this framework and, as noted below, even the present capital standards do not really address this form of risk in particular.

[28] Capital Assets Management Equity and Liquidity (CAMEL) is a system that is based on a ranking of one to five, with one being the best.

Box 5. Principles for Managing Risk in Online Banking

The Electronic Banking Group of the Basel Committee on Banking Supervision has identified 14 key risk-management principles for online banking. Banks and their supervisors should consider these principles when formulating risk-management policies and processes for online activities.

* Management oversight. Effective management oversight of the risks associated with e-banking needs to be in place, and e-banking risk management should be integrated with overall risk management.
* Management of outsourcing and third-party dependencies. Comprehensive, well-defined, ongoing oversight is needed for managing outsourced relationships and third-party dependencies supporting e-banking, including adequate prior due diligence.
* Segregation of duties. Appropriate measures are needed to ensure proper segregation of duties in e-banking systems, databases, and applications.
* Proper authorization measures and controls in systems, databases, and applications. Appropriate authorization measures and proper controls need to be in place for e-banking systems, databases, and applications.
* Clear audit trail for e-banking transactions. A clear audit trail is needed for all e-banking transactions.
* Authentication of all entities, counterparts, and data. Banks should authenticate the identity and origin of all entities, counterparts, and data transmitted over the Internet.
* Nonrepudiation (accountability) for e-banking transactions. Nonrepudiation should be ensured to hold users accountable for e-banking transactions and information.
* Comprehensive security control. Banks should ensure the appropriate use of activities and properly safeguard the security of e-banking assets and information.
* Integrity of transactions, records, and information. Banks should prevent unauthorized changes to and ensure the reliability, accuracy, and completeness of e-banking transactions, records, and information.
* Appropriate disclosure. To avoid legal and reputation risks, including risks for cross-border activities, banks should have adequate disclosure for e-banking services.
* Confidentiality and privacy of customer information. The confidentiality of customer information and adherence to customer privacy requirements should be ensured.
* Business continuity and contingency plans to ensure the availability of systems and services. Plans should ensure that e-banking systems and services are available to customers, internal users, and outsourced service providers when needed.
* Incident response planning. Incident response plans should be in place to manage and minimize problems arising from unexpected events—including internal and external attacks that hamper the provision of e-banking systems and services.
* Role of supervisors. Bank supervisors should assess banks' management structures, practices, internal controls, and contingency plans for e-banking.

Source: Electronic Banking Group of the Basel Committee on Banking Supervision; see also Annexes I–III of this paper to understand how such principles can be translated to distinct processes to reduce e-security risk.

Bank Capital Standards and E-Security

In May 2001, the Basel Committee on Banking Supervision issued a consultative document relating to capital adequacy regulations. This document defines operational risk as the "risk of direct or indirect loss resulting from inadequate or failed internal processes, people, systems, and external events."[29] It identifies three ways to measure operational risk: (1) the basic indicator approach, (2) the standardized approach, and (3) the internal management approach. Under the basic indicator approach, banks have to hold capital for operational risk that is equal to a fixed percentage of gross income. In the case of the standardized approach, a more complex process is used whereby the financial services provider breaks up its overall operations into distinct business lines and uses different indicators for each and then computes the capital charge

[29] See Basel Committee on Banking Supervision Consultative Document: The New Basel Accord, January 2001.

via use of a capital factor provided by supervisors. Finally, the most advanced approach is the internal measurement approach, which relies on calculations that result in expected losses.

None of these frameworks allows for what one might think of as kidnapping- or extortion-related risks caused by penetration of a bank's systems. Moreover, the concept of operational risk that is now used addresses only legal risk, not the problems of strategic and reputation risks. Since incentives to report losses or compromises of the system accurately are often lacking, taking proper account of electronic security risks in any concept of operational risk will be highly subjective and complex.

E-Security and IT Examination Processes

What, then, is the best way forward if capital regulations cannot be adjusted? One of the most fruitful avenues is to publicize the actions that can be taken to measure and manage the risk of electronic security breaches. Implementing new guidelines and risk-management processes that can be monitored by bank examiners would impose a minimum standard for dealing with electronic security because it could reduce the prospect of security breaches. Here, adoption of some form of layered electronic security risk protocol might also be worthy of consideration. Box 6, which draws on extensive consultations with electronic security industry experts, illustrates such a set of layered security measures (see also Annex I, which contains more detail). A bank could have many of these layers of security in place. A number of these actions are not costly to implement with any financial services provider, yet they are often lacking.

In recent years, IT examinations have been performed on banks that possess online transactional banking systems. IT examiners would often enter a bank and ask the following questions:

1. Do you have a firewall?
2. If so, is it configured properly?
3. Do you possess a local area network (LAN) or wide area network (WAN)? If so, are there encrypted channels?

Recently, a number of countries, including the United States, have passed legislation stipulating the need for financial services providers to strengthen their information security. For example, the GLBA, also known as the Financial Services Modernization Act or Title V 12 CFR 573, applies to "financial institutions." These are defined very broadly in Section 509(3) of the act to mean "any institution the business of which is engaging in financial activities described in section 4(k) of the Bank Holding Act of 1956." GLBA states that these institutions must adhere to the following actions:

- Identify and assess the risks that may threaten customer information.
- Develop a written plan containing policies and procedures to manage and control these risks.
- Implement and test the plan.
- Adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.

Box 6. Layered Security

In today's business climate, the gap between risk management of physical assets and informational assets is large. Layered security is composed of 10 core elements. Annex I presents a toolkit for effective risk management compiled from the contributions of industry leaders and law enforcement officials. The following categories represent the 10 core layers of e-security where security is a dynamic process, and, therefore, such policies and processes must constantly be reviewed.

Risk Management—A broad based framework based upon CERT's OCTAVE paradigm for managing assets and relevant risks to those assets.

Authentication—Establish the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication). The first line of defense is access controls; these can be divided into passwords, tokens, biometrics, and public key infrastructure (PKI).

Firewalls—Create a system or combination of systems that enforces a boundary between two or more networks. Annex I contains recommendations for proper firewall configuration.

Active content filtering—At the browser level, it is prudent to filter all material that is not appropriate for the workplace or that is contrary to established workplace policies.

Intrusion detection system (IDS)—This is a system dedicated to the detection of break-ins or break-in attempts, either manually or via software expert systems that operate on logs or other information available on the network. Approaches to monitoring vary widely, depending on the types of attacks that the system is expected to defend against, the origins of the attacks, the types of assets, and the level of concern for various types of threats.

Virus scanners—Worms, Trojans, and viruses are methods for deploying an attack. A virus is a program that can replicate itself by infecting other programs on the same system with copies of itself. Trojans do not replicate or attach themselves to other files. Virus scanners hunt malicious codes. Annex I details proper maintenance and configuration of these scanners.

Encryption—Encryption algorithms are used to protect information while it is in transit.

Penetration testing—Penetration testing entails obtaining knowledge of vulnerabilities that exist on a computer system or network and using that knowledge to gain access to resources on the computer or network while bypassing normal authentication barriers.

Proper systems administration—This should be complete with a list of administrative failures that typically exist within financial institutions and corporations and a list of best practices.

Incident response plan (IRP)—This is the primary document used by a corporation to define how it will identify, respond to, correct, and recover from a computer security incident. The main necessity is to have an IRP and to test it periodically. All employees should be aware of the correct procedures in the event of a computer incident. See Annex I for more detailed treatment of these issues.

Essentially, GLBA addressed the pivotal question, "What is being done to secure customer data, both physical and electronic in origin?" Although it is a step in the right direction, this law needs improvement vis-à-vis the specifics as to how banks should protect their electronic assets. An underlying tension exists within the banking community between whether to spell out how to secure IT systems or whether to even make the effort because of the ever-changing nature of technology and the multitude of acceptable ways to secure electronic banking systems. The 1996 Federal Financial Institutions Examination Council's (FFIEC) IT examination manual has been the industry norm, but it needs to be updated.

In many countries, IT examiners have to follow guidelines that are, in effect, a modified version of the FFIEC IT examination manual. These IT examiners perform "risk scoping," a practice wherein they only check new systems or software installations that have occurred since the last examination. If the examiner has checked an institution in the past and given it a good score, he or she will not recheck any of the older systems and configurations. This approach, however, can be highly problematic. Systems change, and new vulnerabilities in software and configuration appear daily. Examiners should not assume that systems checked in earlier audits

are still secure. If the practice of risk scoping exists merely to save time and costs, legislatures should mandate additional funding for regulatory agencies.

Hosting companies such as FiServe are examined by joint examiners from the Office of the Comptroller of the Currency (OCC), the Federal Reserve, Federal Technology Services (FTS), and the Federal Deposit Insurance Corporation (FDIC). The Bank Service Corporation Act states that if an entity provides a data processing service to a bank, then it, too, can be examined. These entities, however, cannot fail the exams. The examiners note deficiencies, and then the entity and examiners agree to a plan of action. If negotiation fails, the enforcement action calls for implementation of a cease-and-desist order. Yet again there is a loophole. Because no real reporting requirements are in place for these hosting providers for losses or rates of intrusions, the cease-and-desist "stick" is negated because there is no information on which to base it. Hence, no standard exists for the evaluation and subsequent regulation of e-security in banking institutions.

Box 7. ISO/IEC 13335 Information Technology—Security Techniques—Guidelines for the Management of IT Security (GMITS)

This ISO/IEC technical report, published in 1995, is generally known by the acronym GMITS. It is made up of five parts, designed to address different aspects of Internet security.

Part 1. Concepts and Models for IT Security
Part 2. Managing and Planning IT Security
Part 3. Techniques for the Management of IT Security
Part 4. Selection of Safeguards
Part 5. Management Guidance on Network Security

GMITS was written to be usable and useful in the worst-case environment; that is, a hostile environment, such as the Internet. The properties of assets (information) that need to be taken into account and protected are extended from the classical confidentiality, integrity, and availability to include accountability, authenticity, and reliability.

Vulnerability is refined to include any property of the asset that can be exploited for purposes other than intended. Thus, a firewall represents a single point of failure and is susceptible to a denial-of-service attack, which does not detract from its value as a protections mechanism but does mean that this vulnerability needs to be considered and addressed.

Likelihood is refined to be associated with use of the data to perform risk analysis, risk assessment, and risk management.

Part 3 focuses on the topics of risk analysis, risk assessment, and risk management. GMITS recommends that the organization establish a baseline minimum set of controls that will be applied to all aspects of the organization. This baseline will be maintained through the use of a median level risk analysis. Policy is used to ensure the enforcement of the baseline throughout the organization, so that all areas can rely on it.

There are never sufficient funds to implement the ideal set of safeguards, and thus safeguards that provide multiple functions are to be preferred, provided the compromise does not reduce effectiveness. The most important situation to guard against is a false sense of security, which is actually worse than having less security or no security at all. A modicum of paranoia is a good thing.

Having been developed as a generalized document, GMITS does not address in detail particular aspects or subtopics of IT security, such as network, cryptographic, or emanations security.

Supervision will have to be proactive, given the hostile nature of the Internet environment. As far back as 1995, the ISO/IEC 13335, better known as the Guidelines for the

Management of IT Security (GMITS), recognized that the Internet was a hostile environment that would require the use of proper electronic security.[33] Box 7 outlines the processes that were advocated. Note that the layered electronic security risk analysis advocated in this paper (see Annex I and Box 6) has many similarities to this ISO standard, which has not been well implemented in many types of institutions, including banks.

Toward a New Approach to Regulation and Supervision

Redefining Regulatory Authority and Legal Liability of Downstream Vendors. Regulatory agencies need improved powers and the appropriate authority to regulate fully all third-party money transmitters. Their budgets and legislative tools will need to increase and the means found to rely on auditing companies (if properly reformed) and the insurance sectors of emerging markets to play a role in this process. The following regulatory and compliance actions might help mitigate the threat of system compromise yet not extend the safety net. In addition, adoption of processes to monitor the extent to which financial services providers adopt and employ better layered electronic security risk-management practices will be essential as part of any enhanced regulatory and compliance regime.

Regulatory

- Expand the circle of regulated entities to include those elements that traffic in or assist in money transmission and directly connect to any payment system.
- Review regulatory goals and needs in an electronic environment.
- Train audit and examination special teams in risk analysis, risk management, and IT issues.
- Revisit capital adequacy requirements and the definition of operational risk to evaluate how best to accommodate e-risks noted in this paper.
- Provide report cards to the public on how well the financial services industry is doing to attain the new security objectives in this area.
- Require clearer management responsibility and accountability to create and sustain safety and soundness.
- Define the regulatory paradigm for the new market.

Compliance

- Develop analytical teams to assess and monitor e-risk management.
- Disconnect any entity from the system that is not in compliance.
- Require warranties, indemnification, and liability from service providers that connect to the payments system.
- Require insurance coverage to accommodate additional risk.
- Institute well-developed reporting requirements for all electronic money or electronic data losses from all service providers and financial services entities.
- Require information sharing between the regulator and the financial services entity concerning losses.
- Require artificial intelligence software, and make affirmative the duty to report all irregular activity from or through any service provider.
- Ensure that in management letters and other correspondence between examiners and management of financial services providers adequate attention focuses on communication

between the systems administrator and senior management and even the board of directors.[30]

Access, availability, and interoperability should also be key objectives of supervision and enforcement. The very interlinked nature of electronic security providers and e-enabling companies or money transmitters implies that the traditional regulatory structure must expand. It does not imply that a greater number of entities be under the safety net but rather that the regulatory framework create incentives for accountability in such entities as ISPs to application service, software, hardware, monitoring detection, and assessment providers. Liability must attach to these providers just as to the directors of those financial institutions that contract with them. These providers are as indispensable to the institution's ability to provide electronic financial services as lawyers and accountants. They should be bonded, licensed, and subject to periodic audit and examination.

In sum, traditional regulatory schemes are outdated and cannot adequately address the new components of the payment system to determine whether a financial institution is operating in a safe and sound manner.

Coordination in Supervision and Information Sharing Across Agencies

In many countries throughout the world, supervision and enforcement in the area of electronic security is complicated by unclear jurisdictional lines across relevant agencies. In practice, often the central bank, the securities or banking regulator (if separate from the central bank), law enforcement agencies, and many other entities must be in a position to share information and reports. In many cases, this can be problematic from a legal point of view, or a general lack of incentives may result in no established forum or process for undertaking coordinated action.

It is important to seek and promote cooperation between law enforcement agencies and regulatory authorities for financial services providers. Increasingly, such cooperation will be needed within and even across countries. Such arrangements will have to go beyond the pursuit of those engaged in money laundering activities; it will require the development of a more accurate and timely system for reporting all incidents of electronic security breaches, and not just loss-related information. This is an important area, in which worldwide cooperation will be needed on an increasing scale.[31] To achieve such cooperation may require greater harmonization across countries in fundamental areas of legislation, including bank secrecy statutes.

[30] During the Y2K effort, systems administrators were given more attention, but in many financial services conglomerates, very little communication goes on between management and the systems people until after the fact. As technology budgets and related security issues grow in importance, this is likely to change—but the regulatory authorities can make management more sensitive to these issues in the course of the examination process.

[31] See Section X, which includes a few examples of such cooperative ventures as Computer Emergency Response Teams (CERTS) or the New York Electronic Crimes Task Force.

VII. Pillar IV: The Role of Private Insurance as a Complementary Monitoring Mechanism[32]

Background

Despite formidable reportage problems inherent in establishing a benchmark to actuarially measure the risk of hack attacks, electronic identity theft, and other forms of related e-risk, insurance companies are writing coverage for such risk. The development of e-risk policies first occurred in the mid-1990s when insurers recognized the coverage gaps or gray areas in traditional insurance products for perils on the Internet. In response to those risks, insurers developed stand-alone e-risk policies rather than adding coverage to existing property and liability insurance. Market participants have used employee liability coverage as a model for pricing and issuing this insurance.

In underwriting this risk, insurers combined information security standards, such as the BS7799, with principles of risk management that included analysis, avoidance, control, and risk transfer. Today, insurers recognize the ISO 17799 information security standard, which addresses these issues in the following 10 major sections:

1. Business continuity planning
2. System access control
3. System development and maintenance
4. Physical and environmental security
5. Statutory, regulatory, or contractual obligation compliance
6. Personnel security
7. Security management for third-party access or outsourcing to a third-party service provider
8. Computer and network management to safeguard information assets
9. Asset classification and control
10. Security policy management support

As part of the e-risk application process, several major insurers, including AIG, Zurich, Chubb, St. Paul, Progressive, and Lloyd's, have incorporated the ISO 17799 standards into a baseline security questionnaire that becomes part of the insurance application in e-risk policies they underwrite. In order to bind coverage, the insured must meet a certain security threshold for insurability, and the precise nature of such thresholds has not been completely standardized within and across countries. In part, this reflects the very dynamic impact of technology in this area. Despite these developments, the use of e-risk policies is still nascent.

In the case of first-party coverage, such policies are being explicitly designed to provide coverage against network extortion, computer theft, damage to digital assets and information as intellectual property, and business or dependent business losses. In the case of third-party coverage, such policies are designed to cover network security or loss event liability and electronic publishing and multimedia liability.

In underwriting these special e-risk policies, insurers are increasingly assessing the extent to which specific providers of financial or other services are in compliance with appropriate standards in each of the 10 areas specified under ISO 17799. These areas are also relevant in the design of appropriate layered security systems, such as the guidelines in Annex I of this report.

[32] The authors thank Kurt Suhs of Galaxy Computing International for very helpful written contributions to this section.

These types of considerations still do not make it possible to actuarially calculate proper premiums for these forms of first- and third-party e-risk coverage. The underlying defects in the information about intrusions and extortion make the pricing of such policies anything but straightforward.

Traditional Insurance Policies

Typical insurance policies have not dealt with electronic security risks or, more broadly, the types of risks emanating from such security breaches. For example, so-called first-party coverage in the context of commercial property policies usually requires physical loss or damage to property via fire but not denial-of-service attacks via computer hackers or other types of e-risk. Also, an employee theft exclusion is usually included in such policies; in many cases of electronic security breaches, an insider or former employee may be involved. In fact, in Fall 2001, the insurance service office explicitly excluded software- and computer-related losses in commercial policies so that coverage would need to be sought via other specialized policies or arrangements. Commercial and crime policies generally cover theft of money and securities, not theft of information, as do many forms of fidelity bonds. Finally, kidnap and ransom policies often limit coverage for extortion to threat of bodily injury, not to the possibility of severe reputation damage associated with making public penetration into a bank's systems or theft of other information.

Recently, insurance carriers have been offering e-risk policies that do provide cover against cyber risk. Here there is the broader question of how to characterize the specific risks to reputation entailed in electronic security breaches and—because reputation risk is highly complex—the kinds of loss payouts for which insurance carriers would be liable. One could just as easily view these risks as similar to catastrophic risk, or perhaps even to kidnapping risk. The latter is relevant not only in the case of electronic identity theft, in which a ransom may be sought from the financial services provider, but also in the case of a pure hack where the hacker threatens to go public and may demand what amounts to a form of extortion payments. Defining the nature of the risk in the case of first-party coverage deserves more thought in light of how industry participants are now writing such e-risk policies.

Another form of insurance that is generally not adequate is third-party coverage. Here there have been gaps in the narrow provisions for advertising injury coverage in which claims can be sought only if the injury occurs in the coverage territory during the policy period—thereby excluding many possible electronic security events. Despite refinements made to the definition of advertising on the Internet via the electronic data liability amendment in Fall 2001, this is an area that remains unresolved. Also, because electronic data is not defined as tangible property, these forms of coverage have limited effectiveness.

Finally, many of the actual e-risk policies reviewed in preparing this report pay no attention to the special risks that wireless technologies are creating in the delivery of financial services. As documented in Annex III below and in a separate paper, Mobile Risk Management, insurance providers should clearly identify the standards for financial services providers to meet for wireless risk mitigation before they underwrite an e-risk policy. In so doing, the insurance industry could play a critical role in setting standards for electronic security risk mitigation.

Insurance Companies as a Force for Change

Over time, the growth in e-commerce liability insurance and, specifically, e-risk insurance is likely to be quite substantial. Estimates by AIG suggest that the market for this insurance may be as much as $2.5 billion.

The viability of providing this insurance coverage is related to more systemic approaches to improving the base of information for pricing the electronic security risks to be covered. Although vendors of electronic security services are working with insurance companies on this issue, government, industry, and law enforcement officials clearly need to find ways of improving the reporting of such information (see Section IX). Current efforts to develop public-private partnerships to solve this problem should therefore be a high priority.

The global insurance industry can and should act as an important force for change in electronic security arrangements worldwide. First, it should strive to improve the minimum standards for electronic security and should strongly advocate enhanced layered electronic security systems (see Annex I). Second, it will be interested in improved certification standards for vendors of electronic security services described in Section III as a way of mitigating risks of coverage and of spreading risk. Third, it will be concerned with improvements in worldwide cooperation and efforts to improve the data and information available with which to actuarially measure e-risks in companies and financial services providers. Finally, it will favor solutions that require vendors of electronic security and other related services (e.g., hosting) to bear some liability, in contrast to some of the current arrangements, which are entered into by parties in the financial services industry in outsourcing arrangements and do not create adequate incentives to maintain electronic security.

VIII. Pillar V: Certification, Standards, and the Roles of the Public and Private Sectors

Four potential areas of certification to address in the electronic environment are the following: software, hardware, IT security vendors, and electronic transactions. Software and hardware vendors were discussed earlier in the paper. Here the main concerns are that hardware and software vendors often provide products with known vulnerabilities that should not be used for financial transactions. Yet they sell these products and refuse to provide warranties or liabilities for them. The industry could provide certifications for these products, but a better approach would be to require vendors to warrant their products and provide either liability coverage or notice and disclaimers when a product is not suitable for certain uses.

Next are questions about the roles of government and the private sector in certifying aspects of electronic financial services, and the issue is broader than just how it relates to the PKI. First is the question of whether there is a case for regulators to license vendors that provide electronic-security-related services to the financial sector. Such vendors play a role in protecting the integrity of one of the eight critical infrastructure components of the electronic economy. However, licensing vendors would widen the regulatory safety net. Might another alternative provide assurance without unduly burdening the regulatory structure? For example, such vendors might post a form of performance bond, or they could be required to obtain professional liability insurance through private insurers. Or the industry could require them to obtain certification levels, enabling them to provide certain services based on the level of certification achieved.

Probably, industry regulation through a certification process will yield the most consistent results, particularly if insurance provides incentives to certified vendors as well as to institutions that use such vendors. This way, regulators can require vendors to share in the risk through professional liability. Only those parties essential to the delivery of the financial services would be included in the regulatory net, security would be a prerequisite for providing services to the financial sector, and all would share proportionately in the attendant risks. Thus, the scope of

regulation could be contained to those entities, such as money transmitters and ISPs, that hold themselves out as being able to provide hosting to the financial services industry. The steps in brief are for industry to certify vendors to levels of professional ability, have insurance concur through coverage or performance bonds, and have risk appropriately shared.

At the transactional level, as part of its business practice, an institution should analyze the benefits that each technology solution brings to the table and weigh that against the costs or concerns associated with each. Then it should implement a data security classification system through the business rules engine mechanism that automatically attaches a level of security to each type of transaction. The business criteria used to make these decisions should include at a minimum the following value matrix: integrity, reliability, authentication, verification, authority, and nonrepudiation. The value of a transaction should then be equal to the sum of the total risks associated with the transaction.

Using such a value matrix could also assist the insurance industry in evaluating coverage risks and pricing. Moreover, it could help the financial entity with self-monitoring by pinpointing where and why particular risks are greater. The value matrix would also help to enrich the information that is reported. The institution could use a mix of solutions, fitting the solution to the value and risks of the underlying transaction. Although insurance companies could play a role in encouraging the security industry to set standards and even to endorse best practices in terms of authorizing and verifying transaction elements, setting harmonized standards for authenticating documents and such related issues goes beyond the role of any private entity and requires significant cooperation between governments.

Traditionally, encryption has been used as a means to protect the information transferred over the Internet, together with various types of protocols (e.g., secure socket layer, fix, and others) designed to provide security to naked or "open" wide area network systems. Although effective, these mechanisms are meant only to provide protection against certain kinds of vulnerabilities.

The process of securely transmitting information over the Internet in countries or across countries has led to a proliferation of public and private key providers and related "certification authorities." These services can be provided by government agencies, such as postal authorities; by technology providers, such as GTE or Verisign; by telecom service providers, such as Nortel's Entrust; and by financial services providers. Eight global financial institutions are such providers.[33]

Every user of public key cryptography is freely provided a key. The creation and storage of such keys, as well as the attendant certification processes, present major challenges. As Annex II shows, there are many ways to authenticate that can be used along with encryption.

First, it is necessary to address the development of a proper certification process for public and private keys and the levels of use of the process. Some countries have opted to endorse only one recognized public certification authority (such as the postal service). In other countries, both public and private authorities provide this function. Although one could claim that certification is a "public good" and therefore should be kept under the control of a public entity, such as the post office, private companies could act as certification agents as long as there is a

[33] The certification authority authenticates the public key by distributing it with a certificate (digitally signed by the certification authority). The potential liability of the certification authority, as well as the reputation implications of security-related breaches, have been used as an argument for the outsourcing of the public key infrastructure to private providers. The seven banks that are certification authorities are ABN, Bank of America, Deustche Bank, Barclays, Chase, Citigroup, and Hypoverensbank.

viable means of cross-certifying to check on the competence of the service being provided. In all likelihood, the desire to maintain the institution's reputation will act as a significant incentive to resolve the moral hazard problem.

Second, governments need to address the issues of authentication, confidentiality, and nonrepudiation in designing valid electronic transactions, because these form the backbone of transactional activity. Annex I discusses these issues in detail and compares the benefits and drawbacks of potential technologies, such as biometrics and digital time stamping. More generally, government needs to encourage the development of technologies that can be used to authenticate with or without certifying. To preserve confidentiality, the government can require the double signing of a key or the use of certain encryption. Again, government should encourage the private development of solutions that maintain confidentiality and privacy for businesses and consumers. In fact, a global industry has already developed, and many U.S. companies are providing privacy and security solutions to companies and consumers worldwide, as noted in Section III.[34]

Third, the integration of technologies through multiple channels for delivery of financial services, as noted in Section III, implies the need to explore how best to harmonize standards across countries. Technologies will need to interface, but sufficient security must be in place so that commerce can be conducted across countries even if they have different forms of certification. The ISO standards could play a constructive role (see Box 2 in Section III), but the challenges will not be small.

Finally, it is important to consider how to ensure an appropriate level of trust in any given transaction. The legal or regulatory transactional framework must be technology-neutral. In reality, a variety of technologies can certify or authenticate transactional elements and can protect against nonrepudiation. The next subsection reviews the major technologies in use today and examines their strengths and weaknesses.

Trust and Confidence in Authentication Technologies and Certification. **"**Trust and confidence" translates into the following: Party A is able to access online services and transfers funds from one account to another. Party A then checks his account balances, and the correct amount has moved from one account to the other. At the end of the month, he goes online again and confirms that all activity for that month has been properly posted and that the account balances match his figures. As a result, he has a high level of trust and confidence in the system. Or Party B receives certain monies from the government on a monthly basis. Or Party C sets up automatic bill paying for all her utilities. Each month, her account is debited for the correct amount of the utilities. Studies have shown that when someone uses a new technology, that party will bond with the use of the technology if it works favorably with no complications the first three times of use. Conversely, assume that Party D approaches an ATM and attempts to take money from his account. He inputs his personal identification number, and the transaction is refused. He tries again, and it is refused again. The third time, the ATM machine eats his card. Studies show that the opportunity to create trust in the technology has been lost. This person will not willingly use the technology again unless no other delivery channel is available.

PKI Technology. An extraordinary amount of research and development money has been spent on developing PKI and certification authorities over the past decade. As a result, PKI is the best known electronic signature verification technology. (See Annex II.) Clearly, it has its

[34] These solutions include systems providing safety in browsing to detect cookies or manage cookies; e-mail security; and even personal firewalls for retail consumers.

strengths. But easier and simpler technologies perform just as well. Again, it is important to understand the business drivers and the consequential risks in choosing an appropriate technology. Moreover, there is no accepted standard legislation, and record retention requirements for certification authorities are often undefined.

Notaries. One alternative to PKI is to offer a new type of notary license. In this scenario, a notary could apply for a Class A license. This would authorize the notary to accept and certify digital and biometric signatures and to time-stamp documents and notarize manual signatures. Or a notary could apply for a Class B license. This would authorize the notary to time-stamp and notarize manual signatures only. Or the notary could apply for a Class C license. Under this scheme, the notary could only notarize manual signatures. This multi-license notary scenario is a tempting resolution to the issue of nonrepudiation for a number of reasons. First, it simply expands an existing, accepted, and regulated framework for verifying signatures. It assesses a greater fee for a Class A license than for the others, and this in turn acts as a user's fee, which can be used by governments to pay for the necessary personnel and equipment to provide online assistance to users and to the expanded notary industry. The negatives of such a solution are also fairly clear. In emerging markets, notaries may not be well trained to undertake this role, and they would need to receive certifications to perform this function. Another concern is that the licensing system, or in many cases the notaries themselves, may be subject to corruption; this concern emphasizes the need for sufficient oversight. Moreover, in the context of many transactional arrangements, notaries often increase the costs of transactions.

Digital Time Stamps. Another alternative to certification authorities is a digital time stamp (DTS) service provider. A time stamp associates a certain date and time with the creation of a digital document. The time stamp can be referenced to prove that the document was recorded at a specific date and time. For example, Party A signs a document and wants it time-stamped. She computes a message digest of the document using a secure one-way hash function and sends it to a DTS service. In return, the DTS service sends back a digital time-stamp document. This includes the message digest, the date and time it was received by the time-stamping service, and the digital signature of the time-stamping service. Later, Party A presents the document to verify its creation date, and a verifier recomputes the message digest and determines whether it matches the digest in the original time-stamped document. The verifier then verifies the digital signature of the time-stamping service. The strengths of this process are that a message digest does not reveal the contents of the document but simply verifies that the underlying message was received on a certain date and time. As stated, a DTS could be an added dimension to a notary's license. In addition, or separately, the DTS could be provided by the post office for set fees. Again, this would use an existing entity that is familiar to the consumer.

Biometrics and Certification. Biometrics is another alternative to the verification process. Biometric authentication techniques can be used to verify the identity of people online automatically through their distinctive physical or behavioral traits. A biometric identifier represents a physical characteristic of the user (see Annex II). The global recognition of this authentication technology will assist in the nonrepudiation of financial transactions and subsequent documentation. These technologies facilitate the process by which entities can transact on a medium that facilitates anonymity. In this case, the two issues to address would be (1) certifying the specific biometric technology and its accuracy, and (2) defining a digital signature in a broad enough manner to allow certification of the parties to a transaction through whatever authentication technology makes sense.

In summary, government should let the private sector lead where possible but should temper this approach by adopting open standards; endorsing technology-neutral solutions;

encouraging the industry to self-regulate and certify; and helping insurance and other industries use incentives to share risk and responsibility in identifying and correcting vulnerabilities.

IX. Pillar VI: Accuracy of Information on E-Security Incidents and Public-Private Sector Cooperation

One action that would improve electronic security worldwide would be the creation of a set of national and cross-border incentive arrangements encouraging financial services providers to share accurate information on denial-of-service intrusions, thefts, hacks, and so on. Ample evidence shows, as noted in Section II, that no accurate base of information exists either within or across countries. This situation limits both awareness and the scope of private sector solutions that can be provided and may even be increasing the cost to companies and financial services providers of insuring against such risks.

Prompted by law enforcement, industry participants, and the academic community, greater public-private cooperation is starting to become more of a reality in the United States and, increasingly, in many other countries as well. Some innovative examples of such efforts, but by no means the only ones, are described below.

The Internet Security Alliance (www.isalliance.org) and the Computer Emergency Response Team (CERT).[35] This is a collaborative effort between Carnegie Mellon University's CERT Coordination Center and a cross-section of private international companies that include NASDAQ and Mellon Financial, TRW, and AIG. This alliance is an industry-led, global, cross-sector network focused on advancing the security of the Internet. CERT (see Glossary for detail) is expanding its operations and now has counterparts in more than 140 countries. It is beginning to implement its methods for extracting this information from users on a global basis.

The Forum of Incident Response and Security Teams (FIRST). FIRST brings together a variety of computer security incident response teams from government, commercial, and academic organizations. FIRST aims to foster cooperation and coordination in incident prevention, prompt rapid reaction to incidents, and promote information sharing among members and the community at large. When FIRST was founded in 1990, it had 11 members. By the end of 2001, FIRST consisted of more than 100 response and security teams, which spanned the major global regions.[36]

The Electronic Crimes Task Force (ECTF).[37] The six-year-old ECTF focuses primarily on the New York area, but its network is expanding to include the rest of the United States. The ECTF, a sort of central cyber-crime clearinghouse for all arms of local, state, and national law enforcement, is headed by the New York office of the Secret Service and has a membership of 180 top federal and local law enforcement agencies and prosecutors. The ECTF is careful to guard its top secret data, but it welcomes new members to its network, which consists of about 200 companies from the private sector, mostly from the telecommunications, banking-finance, and vendor-services communities. With the passage of the Patriot Act in 2002, this task force model has been expanded to include the cities of Washington, Boston, Chicago, San Francisco, Miami, and Las Vegas.

[35] www.isalliance.org
[36] www.first.org
[37] http://www.ectaskforce.org/

InfraGard.[38] InfraGard is a partnership between private industry and the U.S. government, represented by the FBI. The InfraGard initiative was developed to encourage the exchange of information by the government and the private sector. Private sector members and an FBI field representative form local area chapters, which set up their own boards to govern and share information within the membership. Each chapter is also part of the larger InfraGard organization. The NIPC (www.nipc.org), in conjunction with representatives from private industry, the academic community, and the public sector, further developed the InfraGard initiative to expand direct contacts with private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats. The initiative, encouraging the exchange of information by government and private sector members, has continued to expand through the formation of additional InfraGard chapters within the jurisdiction of each FBI field office.

All these arrangements rely on trust, because they make clear that they will not divulge respondents' identities. In some cases, such as with the New York ECTF, partnerships have gone so far as to allow private market participants and law enforcement agencies involved to sign explicit nondisclosure statements as a form of legal safeguard against disclosure of the information being provided. A universally trusted third party collects such information and disseminates it without providing information that could identify the provider, given the possible reputation and other damage related to such a disclosure.

A fruitful exercise might include further study of existing arrangements to share information about electronic security breaches among industry participants, law enforcement, and possibly academic entities with expertise in the technology issues involved. Multilateral lenders such as the World Bank might play a more active role in facilitating such cooperation. In addition, the initiatives of the World Bank and the International Monetary Fund in such areas as initiatives against money laundering and the establishment of financial intelligence units (FIUs) will have to be properly integrated into any well-defined information-sharing framework. For example, suspicious activity reports often can lead to investigations that relate to electronic security breaches and related crimes (e.g., identification thefts).

X. Pillar VII: Education and Prevention of E-Security Incidents

In many countries throughout the world, statistical analysis reveals that more than 50 percent of electronic security intrusions are carried out by insiders. An uneducated or undereducated workforce is inherently more vulnerable to this type of incident or attack. In contrast, a well-trained workforce, conscious of security issues, can add a layer of protection. Hence, the safety and efficiency of technology is directly related to the training and technical education of the persons using the technology.

That correlation suggests that any effort to reduce and prevent the occurrence of electronic security incidents must rely on an extensive educational effort operating at the following levels: first, the authorities and the persons assigned to examine the financial services providers; second, the systems personnel and others in management at financial services entities; and finally, the users of financial services.

[38] www.nipc.org

Any plan of action to improve education will need to involve a number of important actions, such as the following:

- Improve awareness and education of financial sector participants about cyber ethics and appropriate user behavior on networked systems. Ensure that employees (and also management), especially those involved in payment system transactions and systems administrators, are aware of the risks and proper approaches to layered security.
- Create institution-wide e-security policies on appropriate behavior and the corresponding channels for reporting intrusions or incidents in close coordination with any effort to improve worldwide information in intrusions (see Section X).
- Develop awareness in the banking community in emerging markets about the need to formulate "incident response plans." In many countries, this will involve efforts to improve capacity; to teach risk assessment, risk management, and prevention; and to develop the essential components of a good security program.
- Facilitate cooperation and transfer of know-how among law enforcement entities, FIUs, and supervisory agencies in developed and emerging markets through such methods as more active exchange programs between personnel. This kind of cooperation can facilitate better education of law enforcement officials, supervisors, and others in emerging market economies about how to deal with e-security.
- Launch some education initiatives in this area targeted to bank examiners, such as at the Toronto Institute, the Federal Reserve courses for bank examiners, or the Financial Stability Institute. The focus of the education should be on techniques for determining whether the layered electronic security systems of brick-and-click banks can be better assessed and evaluated.
- Consider developing a cross-border university outreach program (e.g., involving such entities as Carnegie Mellon's CERT) to promote the training of future e-security professionals, and develop innovative approaches to sharing of information in e-security incidents. Some private entities (e.g., Cisco) provide training at reduced costs for government.
- Develop online programs to improve education of users of e-financial services; develop processes and incentives to have customers report suspicious activities in the use of their accounts. Users and the information they provide are critical to any overall approach to electronic security and risk-sharing.

References

Allen, Julia. 2001. *CERT Guide to System and Network Security Practices.* Indianapolis, Ind.: Addison-Wesley.

Bank of International Settlements. 2001. *Electronic Finance: A New Perspective and Challenges.* BIS Papers No. 7. Basel, Switzerland:

Berinato, Scott. 2002. "Finally, a Real Return on Security Spending." *Chief Information Officer (CIO) Magazine.* February 15.

Claessens, Stijn, Thomas Glaessner, and Daniela Klingebiel. 2002. *Electronic Finance: A New Approach to Financial Sector Development.* World Bank Discussion Paper No. 431. Washington, D.C.

Claessens, Stijn, Glaessner, Thomas, and Daniela Klingebiel. 2001. *E-Finance in Emerging Markets: Is Leapfrogging Possible?* World Bank Financial Sector Discussion Paper No. 7. Washington, D.C.

Cunningham, "Digital Security: Heightened Risks Demand Innovation," *Red Herring*, July 2001.

Gilbride, Edward. 2001. *Emerging Bank Technology and the Implications for E-Crime Presentation.* September 3.

Konda, Suresh, and Soumyo Moitra. 2000. The Survivability of Network Systems: An Empirical Analysis. Paper. Carnegie Mellon Software Engineering Institute, Pittsburgh, Pa.

United States Department of Justice. 2002. "McNeese" Press Release. Retrieved on March 1, 2002, from http://www.cybercrime.gov/mcneeseArrest.htm.

Shapiro, Carl, and Hal Varian. 1999. *Information Rules: A Strategic Guide to the Network Economy*. Boston, Mass.: Harvard Business School Press.

Soo Hoo, Kevin 2001. "Tangible ROI through Secure Software Engineering." *Secure Business Quarterly*. October.

Sullivan, Bob. 2001. "Massive Credit Heist Fraud Reported." MSNBC Online. Retrieved on December 22, 2001, from http://www.msnbc.com.

White House. 2000. *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0*. White House, Washington D.C.

Glossary

A -

Abuse of privilege: When a user performs an action that he or she should not have performed according to organizational policy or law.

Access: The ability to enter a secured area, and the process of interacting with a system. Used as either a verb or a noun.

Access authorization: Permission granted to users, programs, or workstations.

Access control: A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Access-sharing: Permitting two or more users simultaneous access to file servers or devices.

Alphanumeric key: A sequence of letters, numbers, symbols, and blank spaces from one to eighty characters long.

ANSI: The American National Standards Institute. ANSI develops standards for transmission storage, languages, and protocols, and represents the United States in the ISO (International Standards Organization).

Application level gateway [firewall]: A firewall system in which service is provided by processes that maintain complete TCP (telecommunications protocol) connection state and sequencing. Application-level firewalls often readdress traffic so outgoing traffic appears to have originated from the firewall rather than the internal host.

Application logic: The computational aspects of an application, including a list of instructions that tells a software application how to operate.

Audit: The independent collection of records to access their veracity and completeness.

Audit trail: An audit trail may be on paper or on disk. In computer security systems, it is a chronological record of when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.

Authenticate: In networking, to establish the validity of a user or a communications server.

Authentication: The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).

Authentication tool: A software or hand-held hardware "key" or "token" used during the user authentication process. See *key* and *token*.

Authentication token: A portable device for user authentication. Authentication tokens operate by challenge and response, time-based code sequences, or other techniques that may include paper-based lists of one-time passwords.

Authorization: The process of determining what number of activities is permitted. Usually, authorization is in the context of authentication. Once the user is authenticated, the user may be authorized different levels of access or activity.

Availability: The portion of time a system can be used for productive work, expressed as a percentage.

- B -

Back door: An entry point to a program or a system that is hidden or disguised, often created by the software's author for maintenance. A certain sequence of control characters permits access to the system manager account. If the back door becomes known, unauthorized users (or malicious software) can gain entry and cause damage.

Bandwidth: Capacity of a network or data connection, often measured in kilobits/second (kbps) for digital transmissions.

Bastion host: A system that has been hardened to resist attack at some critical point of entry and that is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be "outside" Web servers or public access systems. Generally, a bastion host is running some form of general-purpose operating system (LNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.

Biometric access control: Any means of controlling access through human measurements such as fingerprints and iris scans.

Business-critical applications: The vital software needed to run a business, whether custom-written or commercially packaged, such as accounting or finance.

- C -

CERT: The Computer Emergency Response Team, established at Carnegie-Mellon University after the 1988 Internet worm attack named Morris.

Challenge/response: A security procedure in which one communicator requests authentication of another communicator and the latter replies with a preestablished appropriate reply.

Chroot: A technique under UNIX whereby a process is permanently restricted to an isolated subset of the file system.

Client/device: Hardware that retrieves information from a server.

Clustering: A group of independent systems working together as a single system. Clustering technology allows groups of servers to access a single disk array containing applications and data.

Coded file: In encryption, a coded file contains unreadable information.

Combined evaluation: Method using proxy and state or filter evaluations as allowed by administrator. See Stateful evaluation.

Communications server: Procedures designed to ensure that telecommunications messages maintain their integrity and are not accessible by unauthorized individuals.

Computer security: Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

Computer security audit: An independent evaluation of the controls employed to ensure appropriate protection of an organization's information assets.

Cryptographic checksum: A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting file-system tampering on UNIX.

- D -

Data-driven attack: A form of attack that is encoded in innocuous-seeming data executed by a user or other software to implement an attack. In the case of firewalls, a data-driven attack is a concern because it may get through the firewall in data form and launch an attack against a system behind the firewall.

Data encryption standard (DES): An encryption standard developed by EBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in both government and private sectors.

Decode: Conversion of encoded text to plain text through the use of a code.

Decrypt: Conversion of either encoded or enciphered text into plain text.

Dedicated: A special-purpose device. Although capable of performing other duties, it is assigned to only one.

Defense in depth: The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

DES: Data encryption standard.

DNS spoofing: Assuming the Domain Name Server (DNS) name of another system by either corrupting the name service cache of a victim system or compromising a domain name server for a valid domain.

Dual-homed gateway: (1) A system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual-homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks. (2) A firewall implement that does not use a screening router.

- E -

E-mail bombs: Code that when executed sends many messages to the same address for the purpose of using up disk space or overloading the e-mail or Web server.

Encrypting router: See Tunneling router and Virtual network perimeter.

Encryption: The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm).

End-to-end encryption: Encryption at the point of origin in a network, followed by decryption at the destination.

Environment: The aggregate of external circumstances, conditions, and events that affect the development, operation, and maintenance of a system.

ERP (enterprise resource planning): ERP systems permit organizations to manage resources across the enterprise and completely integrate manufacturing systems.

Extranet: Extranet refers to extending the LAN via remote or Internet access to partners outside your organization, such as frequent suppliers and purchasers. Such relationships should be over an authenticated link to authorized segments of the LAN and are frequently encrypted for privacy.

- F -

Fat client: A computing device, such as a PC or Macintosh, that includes an operating system, RAM, ROM, a powerful processor, and a wide range of installed applications that can execute on the desktop or 100 percent on the server under a server-based computing architecture. Fat clients can operate in a server-based computing environment.

Fault tolerance: A design method that ensures continued systems operation in the event of individual failures by providing redundant system elements.

Firewall: A system or combination of systems that enforces a boundary between two or more networks.

Flooding programs: Implementing a code that when executed will bombard the selected system with requests in an effort to slow down or shut down the system.

Anonymous FTP [Define acronym]: A guest account that allows anyone to login to the FTP server. It can be a point to begin access on the host server.

- G -

Gateway: A bridge between two networks.

Generic utilities: General purpose code and devices—that is, screen grabbers and sniffers that look at data and capture such information as passwords, keys, and secrets.

Global security: The ability of an access-control package to permit protection across a variety of mainframe environments, providing users with a common security interface to all.

GPS (global positioning system) : Used primarily for navigation, this satellite-based system maps the location of various receivers on earth.

Granularity: The relative fineness or coarseness by which a mechanism can be adjusted.

GSM: Groupe Spécial Mobile, the European Union's digital cellular standard.

- H -

Hack: Any software in which a significant portion of the code was originally another program.

Hackers: Those intent on entering an environment to which they are not entitled entry for whatever purpose (e.g., entertainment, profit, theft, prank), usually involving iterative techniques, escalating to more advanced methodologies, and use of devices to intercept the communications property of another.

Host-based security: The technique of securing an individual system from attack. Host-based security is operating system- and version-dependent.

Hot standby: A backup system configured in such a way that it may be used if the system goes down.

Hybrid gateway: An unusual configuration with routers that maintain the complete state of the TCP/IP connections or examine the traffic to try to detect and prevent attack (may involve host). If very complicated, it is difficult to attach, maintain, and audit.

- I -

ICA: An acronym for Citrix's Independent Computing Architecture, a three-part server-based computing technology that separates an application's logic from its user interface and allows 100 percent application execution on the server.

IETF (The Internet Engineering Task Force): A public forum that develops standards and resolves operational issues for the Internet. IETF is purely voluntary.

Information systems technology: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction or the inability to process that information.

Insider attack: An attack originating from inside a protected network.

Internet: A web of different, intercommunicating networks funded by both commercial and government organizations. The Internet had its roots in early 1969 when the ARPANET was formed. ARPA stands for Advanced Research Projects Agency (which was part of the U.S. Department of Defense). One of the goals of ARPANET was research in distributed computer systems for military purposes. The first configuration involved four computers and was designed to demonstrate the feasibility of building networks using computers dispersed over a wide area. The advent of open networks in the late 1980s required a new model of communications. The amalgamation of many types of systems into mixed environments demanded a better translator between these operating systems and a nonproprietary approach to networking in general. Telecommunications Protocol/Internet Protocol (TCP/IP) provided the best solutions.

Intrusion detection system: A system dedicated to the detection of break-ins or break-in attempts manually either via software expert systems that operate on logs or other information available on the network.

IP sniffing: Stealing network addresses by reading the packets. Harmful data is then sent stamped with internal trusted addresses.

IP splicing: An attack whereby an active, established session is intercepted and co-opted by the attacker. EP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP spoofing: An attack whereby a system attempts to illicitly impersonate another system by using its EP network address.

ISO (International Standards Organization): Sets standards for data communications.

ISSA: Information Systems Security Association.

- J -

- K -

Key: In encryption, a sequence of characters used to encode and decode a file. One can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, which is a device used to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards or they may be loaded onto a PC as copy-protected software.

- L -

Least privilege: Designing operational aspects of a system to operate with a minimum amount of system privilege. This design reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.

Local area network (LAN): An interconnected system of computers and peripherals; LAN users share data stored on hard disks and can share printers connected to the network.

Logging: The process of storing information about events that occurred on the firewall or network.

Log processing: How audit logs are processed, searched for key events, or summarized.

Log retention: How long audit logs are retained and maintained.

- M -

Mobile code: A program downloaded from the Internet that runs automatically on a computer with little or no user interaction.

Multi-user capability: The ability for multiple concurrent users to log on and run applications from a single server.

- N -

Network computer (NC): A "thin" client hardware device that executes applications locally by downloading them from the network. NCs adhere to a specification jointly developed by Sun, IBM, Oracle, Apple, and Netscape. NCs typically run Java applets within a Java browser or Java applications within the Java Virtual Machine.

Network computing architecture: A computing architecture in which components are dynamically downloaded from the network into the client device for execution by the client. The Java programming language is at the core of network computing.

Network-level firewall: A firewall in which traffic is examined at the network protocol packet level.

Network worm: A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability, or availability. A network worm may attack from one system to another by establishing a network connection. The worm is usually a self-

contained program that does not need to attach itself to a host file to infiltrate network after network.

NIPC (National Infrastructure Protection Center): NIPC brings together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to protect the nation's critical infrastructures. NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response in cases of threats or attacks against electronic critical infrastructures.

- O -

One-time password: In network security, a password issued only once as a result of a challenge-response authentication process. Cannot be "stolen" or reused for unauthorized access.

Operating system: System software that controls a computer and its peripherals. Modern operating systems, such as Windows 95 and NT, handle many of a computer's basic functions.

Orange book: The Department of Defense Trusted Computer System Evaluation Criteria. It provides information to classify computer systems, defining the degree of trust that may be placed in them.

- P -

Password: A secret code assigned to a user, known by the computer system. Knowledge of the password associated with the user ID is considered proof of authorization. (See One-time password.)

Performance: A major factor in determining the overall productivity of a system, performance is primarily tied to availability, throughput, and response time.

Perimeter-based security: The technique of securing a network by controlling access to all entry and exit points of the network.

PIN (personal identification number): In computer security, a PIN is known only to the user and used during the authentication process. (See Challenge/response; Two-factor authentication.)

Policy: Organizational-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Private key: In encryption, one key (or password) is used to both lock and unlock data. Compare with Public key.

Protocols: Agreed-on methods of communications used by computers.

Proxy: (1) A method of replacing the code for service applications with an improved version that is more security-aware. Preferred method is by "service communities" rather than individual applications. Evolved from socket implementations. (2) A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Public key: In encryption, a two-key system in which the key used to lock data is made public, so everyone can "lock." A second, private, key is used to unlock or decrypt.

- Q -

- R -

Remote access: The hookup of a remote computing device via communications lines, such as ordinary phone lines or wide area networks, to access network applications and information.

Remote presentation services protocol: A protocol is a set of rules and procedures for exchanging data between computers on a network. A remote presentation services protocol transfers user interface, keystrokes, and mouse movements between a server and a client.

Risk analysis: The analysis of an organization's information resources, existing controls, and computer system vulnerabilities. It establishes a potential level of damage in dollars or other assets.

Rogue program: Any program intended to damage programs or data. Encompasses malicious Trojan horses.

RSA: A public key cryptosystem named by its inventors—Rivest, Shamir, and Adelman—who hold the patent.

- S -

Salami slice: A hacker method for the acquisition of funds. A database of account information is copied. Then on a later date all accounts are charged a minimal amount, so as not to arouse suspicion.

Scalability: The ability to expand a computing solution to support large numbers of users without having an impact on performance.

Screened host gateway: A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.

Screened subnet: An isolated subnet created behind a screening router to protect the private network. The degree to which the subnet may be accessed depends on the screening rules in the router.

Screening router: A router configured to permit or deny traffic using filtering techniques; based on a set of permission rules installed by the administrator. A component of many firewalls usually used to block traffic between the network and specific hosts on an IP port level. Not very secure; used when speed is the only decision criterion.

Server: The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.

Server-based computing: An innovative, server-based approach to delivering business-critical applications to end-user devices, whereby an application’s logic executes on the server and only the user interface is transmitted across a network to the client. Its benefits include single-point management, universal application access, bandwidth-independent performance, and improved security for business applications.

Server farm: A group of servers that are linked together as a "single system image" to provide centralized administration and horizontal scalability.

Session shadowing: A feature of Citrix WinFrame and MetaFrame that allows administrators and technical support staff to join remotely or take control of a user's session for diagnosis, support, and training.

Session stealing: See IP splicing.

Single-point control: Helps to reduce the total cost of application ownership by enabling applications and data to be deployed, managed, and supported at the server. Single-point control enables application installations, updates, and additions to be made once, on the server, and then instantly made available to users anywhere.

Smart card: A credit card–sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Social engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user to attempt to gain illicit access to systems.

Stateful evaluation: Methodology using mixture of proxy or filtering technology intermittently, depending on perceived threat (or need for speed.)

- T -

TCO (total cost of ownership): A model that helps IT professionals understand and manage the budgeted (direct) and unbudgeted (indirect) costs incurred for acquiring, maintaining, and using an application or a computing system. TCO normally includes training, upgrades, and administration as well as the purchase price. Lowering TCO through single-point control is a key benefit of server-based computing.

Thin client: A low-cost computing device that works in a server-centric computing model. Thin clients typically do not require state-of-the-art, powerful processors and large amounts of RAM and ROM because they access applications from a central server or network. Thin clients can operate in a server-based computing environment.

Token: In authentication, a device used to send and receive challenges and responses during the user authentication process. Tokens may be small, hand-held hardware devices similar to pocket calculators or credit cards. See Key.

Trojan horse: (1) Any program designed to do things the user of the program did not intend to do or that disguise its harmful intent. (2) A program that installs itself while the user is making an authorized entry, and then is used to break in and exploit the system.

Tunneling router: A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network for eventual de-encapsulation and decryption.

Turn commands: Commands inserted to forward mail to another address for interception.

Two-factor authentication: Two-factor authentication is based on something a user knows (factor one) plus something the user has (factor two). In order to access a network, the user must have both "factors," just as he or she must have an ATM card and a PIN to retrieve money from a

bank account. In order to be authenticated during the challenge and response process, users must have this specific (private) information.

- U -

User: Any person who interacts directly with a computer system.

User ID: A unique character string that identifies a user.

User identification: User identification is the process by which a user identifies herself to the system as a valid user—as opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system.

User interface: The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

- V -

VPN (virtual private network): A private connection between two machines that sends private data traffic over a shared or public network, such as the Internet. VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies.

Virtual network perimeter: A network that appears to be a single protected network behind firewalls, but actually encompasses encrypted virtual links over untrusted networks.

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

- W -

WEP (Wireless Equivalent Protocol): A protocol designed to be implemented over WLANs to offer the same security features as a physical wire: confidentiality, access control, and data integrity.

Windows-based terminal (WBT): A fixed-function thin-client device that connects to a Citrix WinFrame or MetaFrame server and terminal server to provide application access. The key differentiator of a WBT from other thin devices is that all application execution occurs on the server; there is no downloading or local processing of applications at the client.

WLAN (wireless local area network): A wireless Network that corresponds to wireless laptops.

- XYZ -

Y2K: An acronym for the year 2000 problem, which involved three issues: two-digit data storage, leap-year calculations, and special meanings for dates.