WPS3586

Capital Markets and E-fraud

Policy Note and Concept Paper for Future Study

The World Bank
Operations and Policy Department

Tom Kellermann, CISM and Valerie McNevin

Public Disclosure Authorized

World Bank Policy Research Working Paper 3586, May 2005

CAPITAL MARKETS AND E-FRAUD[1]

Policy Note and Concept Paper for Future Study

Abstract

The technological dependency of securities exchanges upon internet based (IP) platforms has dramatically increased the industry's exposure to reputation, market and operational risks. In addition, the convergence of several innovations in the market are adding stress to these systems. These innovations affect everything from software to system design and architecture. These include the use of XML as the industry IP language, STP or straight through processing of data, pervasive or diffuse computing and grid computing as well as the increased use of Internet and wireless. The fraud is not new, rather, the magnitude and speed by which fraud can be committed has grown exponentially due to the convergence of once private networks online. It is imperative that senior management of securities markets and brokerage houses be properly informed of the negative externalities associated with e-brokerage and the possible critical points of failure that exist in today's digitized financial sector as they grow tomorrow's exchanges. The overwhelming issues regarding e-finance is to determine the true level of understanding that senior management has about online platforms, including the inherent risks and the depth of the need to use it wisely. This policy note will attempt to highlight the various risks that have been magnified by the increasing digitalization of processes within the brokerage arena and explain the need for concerted research and analysis of these as well as the profound consequences that may entail without proper planning. An effective legal, regulatory and enforcement framework is essential for creating the right incentive structure for market participants. The legal and regulatory framework should focus on the improvement of internal monitoring of risks and vulnerabilities, greater information sharing about these risks and vulnerabilities, education and training on the care and use of these technologies and better reporting of risks and responses. Public/private partnerships and collaborations also are needed to create an electronic commerce (e-commerce) environment that is safe and sound. Section I of the working paper, attempts to provide a background as to the adoption of technology in capital markets. Section II is an overview of 7 case studies in e-fraud perpetuated within capital markets and the various operational risks of utilizing IP based networks. Section III provides the conclusion and rationale for further research in the area of E-fraud.

[1] Authored by Tom Kellermann and Valerie McNevin 2004. The Authors would like to thank Gerard Caprio, Jim Nelms, Shrimadt Tripathy, Yumi Nishiyama, Thomas Glaessner and Ernesto Revilla for their valuable insights and written contributions.

I. Introduction and Background

On October 14th,2004 New York Federal Reserve President Timothy Geithner[2] stated:

"The increased risk of terrorist attacks and increased sophistication of cyber-attacks on electronic networks have added new dimensions to the traditional concerns of safety and soundness and operational resilience," he told a financial services conference in Atlanta. Geithner said the growing challenge of cyber-attacks will require a "major ongoing commitment of resources". "Beyond the direct financial losses from criminal activity, these threats pose a broader risk to confidence in the integrity of financial institutions, payments systems and, ultimately, the global payments network," he said.

All financial institutions are facing this critical operational risk. Geithner's statements echo the warnings made by law enforcement entities for the past 5 years. *Operation Uptick*[3] was the largest securities fraud under-cover operation to date. In a ten month investigation involving the US Attorney's office, the FBI and the SEC, it culminated in the arrest of over 200 people, the involvement of brokerage firms and a network of six organized crime families, brokerage firms, brokers and over $50 million in illegal proceeds. Tracking a period of more than 5 years it exposed a criminal enterprise that was able to bribe brokers and pension officers, compromise every type of market and law enforcement professional, inflate stock prices, and sell shaky investments through a significantly corrupted brokerage system. Most disturbing, its prosecution showcased the changing business model and modus operandi for organized crime and foreshadows the havoc that organized crime can wreak undetected in the securities industry.

The technological shift to IP based technologies has had a direct impact in the financial industry, most obviously in the areas of e-banking and online securities trading. E-finance penetration is best observed in online securities trading and internet banking[4]

E-finance use is increasing around the globe, including that of emerging markets. Despite the intrinsic weaknesses in the financial, legal, regulatory and technological infrastructures of emerging countries, some such as Korea, Brazil, and India have been early adopters of e-finance, using the new delivery channels to expand access, provide opportunities and effectively circumvent some of the constraints of traditional modes.

In the world's securities markets[5] according to the World Bank's financial sector research, by 2005, online brokerage could rise to 80 percent in industrial countries (which was around 28% at

---

[2] Fed's Geithner warns of cyber-attack risk to banks. REUTERS. Thu Oct 14, 2004 02:52 PM ET. By Victoria Thieberger.

[3] http://www.sec.gov/news/press/2000-81.txt

[4] Goldfinger, UNCTAD (2001)

[5] E-finance in securities markets include not only online brokerage but also electronic issuance and distribution of securities such as the Treasury Direct in the United States, where treasury securities are sold directly to the retail investors. Similar systems have been created in the Philippines, Brazil, Mexico etc. where e-distribution of securities is changing the landscape of primary markets for government securities. (Glaessner, Kantur, 2004)

the time of the research), and 40% in developing countries assuming that a better business and enabling environment is put in place[6].

The trend observed in the capital markets of more industrialized countries, such as the United States, Western Europe and Singapore, is continued growth in the use of online trading. In emerging economies, South Korea represents the high end. Since e-brokering was launched in Korea in 1997, the proportion of its total trading value steadily climbed from 19 percent in 1999, to 43 percent in 2003. In Russia, approximately 40 percent of stocks traded on the Moscow Interbank Currency Exchange (MICEX) occurs via the Internet. On the low end, in Singapore and Taiwan, e-brokering accounts for approximately 10 percent of total trading volume. In Chile, market players estimate that 5-10 percent of securities trading occurs online. The table below depicts a snapshot of the growth of internet based trading in certain markets.

Table I: Penetration of Online Trading

	1999	**2003**
EU Nations	2 %	10 %
South Korea	19%	43%
Singapore	5%	10%
Hungary	6%	
India	11%	
Brazil	6%	
Mexico	3%	

E-Finance promises many benefits to users and adopters. First, e-finance lowers the costs of intermediation and increases competition in financial services. It also expands the reach and scope of access to financial services by formerly unreachable clients (Claessens et-all 2001). This increased penetration of e-finance in developed as well as developing countries is are also erasing the boundaries between finance and technology, transactions and information processing, and finally financial service providers and technology providers. The distinction between "e-finance" and "finance" will become obsolete, as financial delivery assumes the use of electronic means.

E-finance however exacts numerous costs that have not been appropriately examined. For example, the dependence of online backend operations has increased operational risk significantly. Although transactions appear to be completed in less time, the underlying complexity required to handle such transactions in an automated fashion has increased exponentially. As a result what we appear to achieve in terms of transactional efficiency on the one hand may be lost through transactional complexity on the other.

Over time, it is now clear that online fraud rates for e-commerce are much higher than for those transactions completed via more traditional modes[7]. The anonymity and speed perpetuated by the internet allows for greater rates of fraud. At present the most valid number to come forth

[6] Claessens, Glaessner & Klingebiel. 2001. *E-finance In Emerging Markets: Is Leapfrogging Possible?*. World Bank.

[7] Glaessner, Kellermann & McNevin. October 2003. Electronic Safety and Soundness: Securing Finance in a New Age. World Bank.

from studies indicates that the online fraud rate is 83 times higher that offline. Further, it is also well established that the financial sector is a target of choice for online crime.[8] As a result of the dot com revolution, increased access to financial services cannot distinguish between rightful from illegal access.

A fundamental principle of criminology is that crime follows opportunity. Opportunities to perpetrate crime abound in today's computer reliant world. The financial services industry is now increasingly vulnerable to inappropriate manipulation and consumers are often defenseless with out appropriate warning whether or not they choose to transact financial activity online. The scope of this problem is multi-dimensional.

First, increased dependence on technology for the delivery of financial services and the processing and storage of financial information without an appropriate understanding of the network's security or business continuity needs inordinately exposes the financial system to e-security risks and threatens the long-term integrity of financial transactions and their underlying information.

Second, Internet and electronic payment systems enable providers of financial services to create complex financial products and services and to expand their reach to an unprecedented number of people from all around the world, at much lower costs than ever thought possible. This opens the door to create unregulated financial products or for unlicensed or illegitimate entities to offer financial services with the intent to defraud unsophisticated consumers.

II. The Potential for E-fraud: 7 Case Studies

This section describes certain risks to which capital markets are exposed in today's online environment. The following are examples of ways in which hackers have compromised systems for illegal purposes.

1. E-brokerage Customer Compromise—Hijacking an account is a preferred method of compromise. By hijacking an account, the perpetrator can change the amount of shares traded and/or the change the time of the trades. By breaking into a broker's account a hacker can insert a Trojan to steal user names and passwords.[9] The hacker then uses this information to trade securities under a victim's name.

> *In October of 2003, Van Dinh, a 19 year old Pennsylvania man, was convicted of using a Trojan horse to capture the password of an investor's online account.. Nineteen-year-old*

[8] Ibid. Of the 142,000 reported electronic security incidents experienced in the United States last year over 50% were targeted against the financial sector. Recently the FBI has corroborated this statistic.

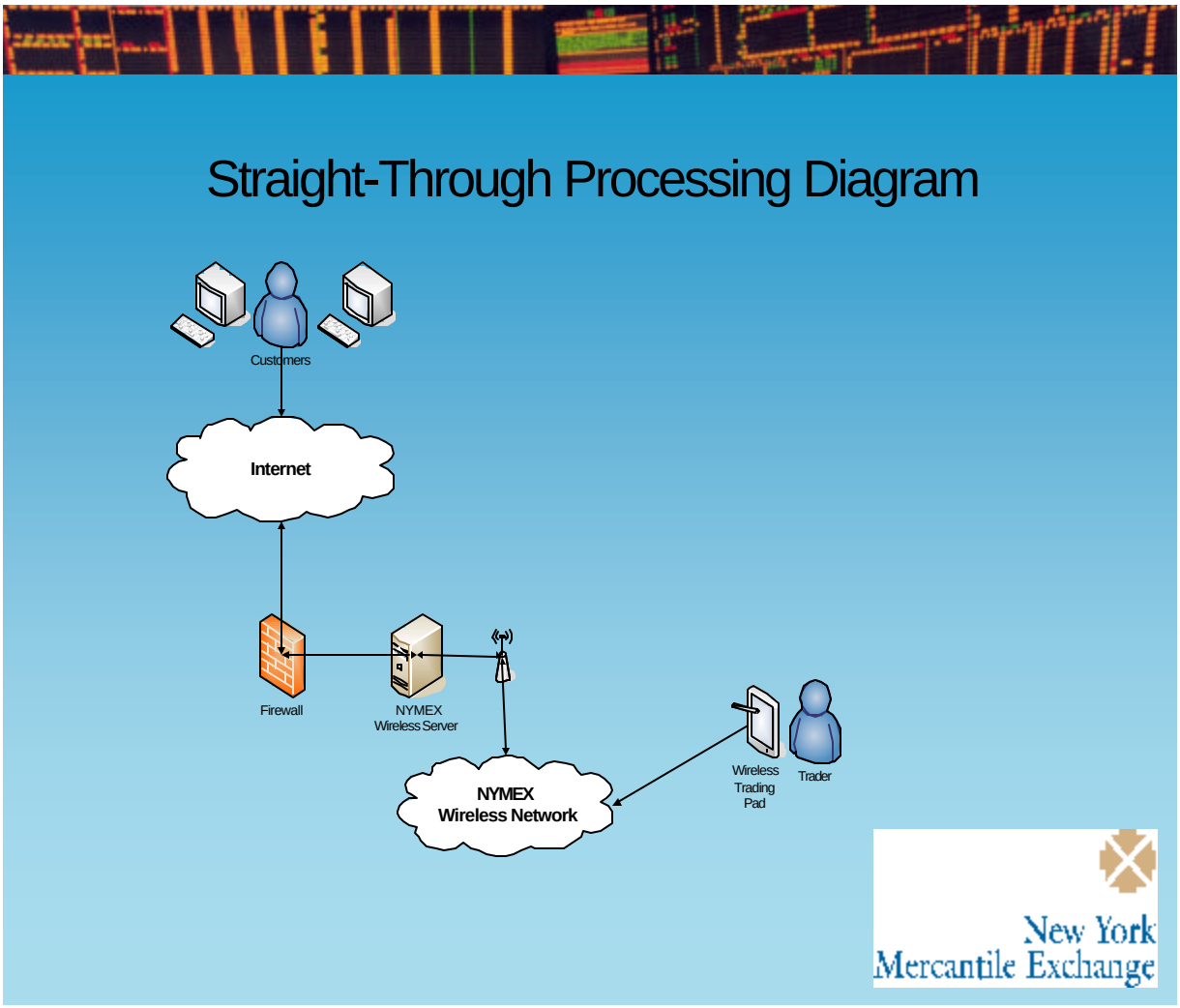
[9] A Trojan horse program cloaks malicious code by appearing as an innocuous attachment. Trojans are designed to gain covert and unlawful access to a user's computer system. Once inside, they can rapidly reproduce and spread worldwide in a matter of minutes, performing damaging acts along the way including, but not limited to: stealing sensitive information, e-mailing information to remote hackers, and enabling remote access and control over a computer system. For additional information, please see Tom Kellermann and Yumi Nishiyama, "Blended Electronic Security Threats: Code Red, Klez, Slammer, and Bugbear" (June 2003) and "Digital Insider: Backdoor Trojans" (December 2003), World Bank.

> *Van Dinh now faces civil securities-fraud charges for tapping into a TD Waterhouse account held by a 34-year-old Boston man. In the criminal case authorities proved that Van Dinh used the hostage account to buy put options on Cisco that effectively cut his losses on a losing position he carried in his own online account at Cybertrader.com. Securities and Exchange Commission officials also showed that Van Dinh used contacts made at an online stock-discussion forum to encourage people to download a certain software in which he had inserted a Trojan horse. Van Dinh tricked victims into downloading the program. Once inside it monitored keystrokes, reporting these back to him, thus allowing him to learn these passwords and codes and obtain unauthorized access to the accounts.*

The victim has no coverage in the event of loss. Furthermore, though these online web sites offer a modicum of security through secure shopping software, there are vulnerabilities within the software itself that facilitate these criminal activities. The following case starkly illustrates the risks that online investors face in today's environment. It underscores the growing concern that trusted spaces such as discussion forums can be abused in such a way that erodes investor confidence, and exerts a new type of cost on investment.

2. E-broker Compromise—To brokers/traders time is always of the essence. Competitive positions today can be made or lost in seconds. Trading, in particular, is an activity where performance is dependent on being seamlessly connected to the "trading floor" at all times. With the growth in global wireless connectivity, many if not most traders and brokers utilize WIFI or GSM protocols to facilitate remote access. Although it provides real-time access to the trader it also provides a means whereby hackers can exploit weaknesses in wireless communication signals to obtain real-time critical intelligence information and/or manipulate trades—See Diagram A.

Diagram A: Wirelessly Enabled Straight-Through Processing



Source: Samuel Gaer, CIO, New York Mercantile Exchange, July 2004 Presentation.

As illustrated above, the New York Mercantile Exchange, is developing a Wireless Straight Through Processing System (refer to Appendix C). According to Mr. Gaer, CIO for the Exchange, such a system will: 1) Ensure order information is clear and accurate 2) Increase customer control 3) Guarantee the trade immediate entry into clearing 4) Guarantee instant order and status assignment information 5) Lower overall transaction costs due to fewer errors and paper supply and lastly, 6) Increase a trader's volume and performance. Although these six elements are characterized as benefits, deeper analysis reveals that such a system carries high administrative and security risks, which in turn requires investing in substantial human and technological resources at significant cost.

The expanding use of wireless and satellite systems for financial transactions represents a growing vulnerability. Such systems often run with little security, leaving the communications vehicle wide open to both techno-terrorist and criminal attacks. Technology creates the possibility for crimes of great magnitude and complexity to be committed very quickly.
For example, assume that a brokerage house transfers data over a T1 fiber optic line. That line can transfer approximately 154KB/sec or 9.2MB/min. once all of the packet buffering, etc is in

place. Now two questions must be asked--how much time does it take to steal the information and how much is the stolen information worth? Assume there is a total denial of service for 9 minutes. The answer is that the brokerage entity would be out of business.

Moreover, the more distributed a network is, the more vulnerable it is to interception and unauthorized access. Take for example, the system in Diagram A. This system exhibits four inherent weaknesses in its architecture: 1) The wireless trading pad running the "Epit application" can be hijacked by a Trojan horse or spyware can be inserted into the communication while in transit from its point of origin to its destination. 2) The Wireless Server/Access point is an easy entry point. 3) The NYME WLAN is susceptible to rogue access points and devices unless frequent audits are conducted for such intruders and 4) The end customer is using the Internet to communicate desired trades into this "secure system" the Internet and those applications that are permitted to move through the firewall have been polluted.[10]

There are ways to mitigate most of these operational risks. Application security, active content filtering, security for pervasive or diffuse computing and grid computing will be critical as will real-time configuration management. The widespread adoption of wireless local area networks (WIFI) are but one example of the convergence of modern telecommunications and IT systems which become open to interception. The popularity of wireless systems (both satellite and terrestrial wireless) has continued to increase. This spread of the technology often coupled with the lack of implementation of certain safeguards for systems[11], creates a serious risk, making wireless systems inherently vulnerable to being breached. Although *Straight Through Processing* (STP) coupled with XML and T + O appears to provide optimal efficiency, if fraud is committed there is no recourse in the settlement window. Unwinding is impossible in the traditional sense in a T + O environment. Today's settlement paradigm and its safeguards should be reviewed as the goal to operate in a T + 0 environment redistributes the risk of disputes about settlement to after the fact rather than trying to resolve such prior to settlement. By redistributing risk, the very nature of the contract changes and this in turn should impact cost and price calculations.

The issues posed by these innovations are not just the result of architecture and configuration but also result from how today's market defines efficiency and effectiveness. Inherently the securities market is different than banking. In banking, safety and soundness are primary, but securities is about assuring that investors are aware of and understands the investment risk. Now the question is whether the investor is adequately educated about the operational risk of the vehicle used to place the trade not just the market risk of the underlying security being traded. Arguably in the securities market if an investor knowingly chooses to use a riskier means of trading that's acceptable, the question then is whether the broker or trader has adequately advised

[10] Although applications are being developed according to common criteria e.g. www.wapforum.org . Many security gaps exist in both the procedural areas and technical areas if implementation per secure wireless networking.

[11] For best practice per securing WLANs, GSM, GPRS and GPS please refer to the Technology Risk Checklist. World Bank. October 2004.

the investor of this risk or should they be permitted to use riskier means to trade without their client's knowledge and if so who bears the burden of any loss that may result.

3. Distributed Denial Of Service (DDOS) attack[12]—DDOS attacks could take several forms. First a hacker may attempt to flood (overwhelm the network with vast amounts of data) a brokerage company's network just before the close of market, to prevent it from placing fresh quotes before the end of the day. This could result in penalties and subsequent "reputational risk". In a delivery vs. payment scenario the stock is not transferred to the buyer until payment is received. If payment orders are kept from being delivered then the stock will not transfer. In an Straight Through Processing (STP), TP, T + 0 environment this scenario carries significantly more risk. This scenario is particularly plausible in the New York Stock Exchange's new wireless trading model. Although the Exchange uses fiber optics as its primary transfer channel, it has installed a WLAN (wireless local asynchronous network) to serve as the redundant backup for those lines in the event of another terrorist strike. Unfortunately using the WLAN poses a significant vulnerability to the integrity of the stored market data. Or the hacker may cause the system to fail to respond to a time-based transaction(s) or a trade(s). For example, a system overload/failure, could delay the response time and cause a Call Option to be placed after its expiry date. Who is liable for a failed trade in that situation?

4. Market Data Sabotage—Market participants are heavily reliant upon the market data they receive from entities like Bloomberg's and/or Reuters as well as online chat rooms and discussion forums. Hackers have the potential to corrupt the data or insert erroneous data once it leaves the perimeters of financial information disseminators and aggregators such as Bloomberg's and Reuters. The integrity of the data can thus be called into question because it can be digitally manipulated. Since trading positions often are directly related to the interpretation of such data such error could result in loss of investor confidence or even panic once discovered. As importantly, chat rooms and discussion forums are fertile areas for manipulators to deposit disinformation. Because this can be done anonymously, quickly and with little if any opportunity to investigate in a timely manner there is little chance that such an event would ever be prosecuted.

5. Currency Trading Scenario—Currency trading is volatile and is more often than not dependent on fractions of seconds in trading positions. Suppose that the Euro drops in value relative to US dollars effective at 12:00:00 EST on a particular day. The holder of Euros is likely to wish that they had sold Euros before its drop in value. Suppose that the server time tagging the buy/sell orders is being controlled by the reception of GPS positioning and timing signals. A GPS electronic spoofing attack could be launched against the GPS time controlled transaction server. In order to "back-date" the sell order to show that it occurred before the Euros decline, the attacker alters the GPS timing (for example, 11:59:50 EST) thereby causing the system to order the sale and time stamp at a time prior to the decline in the Euros value. The

---

[12] A type of electronic attack in which malicious code is used to execute any type of system overflow or jam, thereby causing the server to shut down and deny service to its users.

electronic attacker then turns off the GPS spoofing signal and the GPS timing system once again receives the real GPS signal and returns to the correct time in the server.[13]

6. Insider Trading/dealing---Insider trading occurs when a broker or trader takes a position with respect to securities based on certain information obtained before it is made public. The Internet facilitates "insider trading" in numerous ways. E-mail and instant messaging programs on a trader/brokers computers can be compromised fairly easily. Trojans[14] and worms can be used to siphon material data from an insider's computer and transmitted to an outside party. For example Backdoor.Tkbot, by definition an IRC[15] Trojan has the capability to perform nefarious activities such as to "gather user/system information", upload a file to the victim's system, or download a file from the victim's system. The use of wireless devices by traders increases the potential for market manipulation due to the use of unsecured WLANs, GPRS, GSM and CDMA[16]. Criminals from outside the "secure enclave" of the trading floor can attack these devices and compromise them thus hijacking the markets for illicit gain. The relative physical security provided by the modern trading floor is bypassed by the wireless transmission of financial data throughout the facility and beyond.

7. Centralized Depository Attack-- Centralized depository, clearing and settlement services for equity and debt markets have been established in many countries over the past 5 years. The typical CDS provides its services with an online computer system with participants having direct online access to the system. Transfer of settlement funds occurs through the central bank the same-day funds. Here is an example of regulation and technology design in supervised arenas not keeping pace with best practice. Since 9-11, a distributed network with significant redundancies is considered best practice. However the debate continues. Pushing forward with a consolidated platform given the significant concerns is not wise and the pros and cons should be looked at dispassionately and with great care. If a consolidated platform is used since this is the delta of the settlement and clearance functions these facilities must maintain maximum security. The issues here are design and function, as well as centralizing high value assets. These are complicated issues. So how does one design a central depository system that is connected to the Internet or open network with sufficient back up, resilience, robustness and safeguards to mitigate the potential of compromising a critical point of failure. Staged cyber-attacks are now feasible in most countries due to the reality that CDS' are built within the Internet Protocol (IP) environment. The potential for reputational, operational and even systemic risks associated with poor non-layered security arrangements[17] upon these institutions is high.

Over the past few years cyber attacks have grown in complexity, sophistication and now represent powerful forms of targeted customized economic weapons that can destroy critical databases and render serious financial harm in an incredibly short amount of time. As countries work to create stock exchanges and central depositories, it is imperative to chronicle the lessons

---

[13] Although this is possible the effects of doing so are not yet known.
[14] A malicious program such as a virus or a worm, hidden in an innocent-looking piece of software, usually for the purpose of unauthorized collection, alteration, or destruction of information.
[15] IRC a.k.a. Internet Relay Chat
[16] For additional information, please see Tom Kellermann, *Mobile Risk Management*, World Bank March 2002.
[17] The World Bank's **Technology Risk Checklist v. 8.2** attempts to highlight the 12 layers of proper network security in detail.

learned so that these can be passed on and incorporated into new designs for the IT systems as well as the supporting legal, regulatory and policy infrastructure.

Table II: Select Case Studies of Hacking Attacks

Date	Location	Fraudster	M.O.
Jan 2004	The Securities Investor Protection Corp. (SIPC)	Investigation Ongoing	Hackers created a website for the fictitious International Brokerage Association, copying the SIPC's web content to confuse investors into thinking the fraudulent website was legit.[18]
Oct 2003	Stock market	Van Dinh	Dinh used keystroke loggers to steal U.S. brokerage firm customer accounts, and then used a victim's account identity as a means to unload Dinh's falling stocks.[19]
Feb 26, 2003	Bloomberg L.P.	Oleg Zezev	Zezev acquired access to customer financial data and attempted to extort $200,000.[20]
2002	H&R Block	Ivy Johnson, former H&R Block manager	The former H&R Block manager has been charged with mail and credit card fraud, for the identity theft of at least 27 customers.[21]
Aug 2002	**Korea**--Daewoo Securities	Investigation Ongoing	Hackers penetrated a bank's security system and illegally sold 5 million shares of Delta Information and Communications stock worth approximately $21.7 million.[22]
Mar 4, 2002	UBS PaineWebber	Roger Duronio, former UBS computer systems administrator	Duronio detonated a "logic bomb" program that caused more than $3 million in damage to the brokerage's computer network.[23]
Feb 7, 2002	U.S. Treasury Direct	Louis Lebaga	$158 million—Lebaga was apprehended only after attempting to steal $1.3 billion more five days later.[24]
Nov 12, 2001	**India**--S.S. Kantilal Ishwarlal (SSKI) Securities Pvt. Ltd., share broker in India	Hemant Sheth, former SSKI sharebroker, and accomplice Bhavesh Pabari,	Sheth and Pabari gained access to the Bombay Online Trading System (BOLT) with Sheth's trader ID and password issued by SSKI. The two then manipulated stock prices by utilizing their

[18] Associated Press, "Federal Web site copied in apparent fraud," accessed on 17 June 2004 at http://www.siliconvalley.com/mld/siliconvalley/news/editorial/7828271.htm

[19] BBC News, "US Hacker Accused of Massive Fraud", accessed on 10 Oct 2003 at http://news.bbc.co.uk/1/hi/business/3180358.stm.

[20] U.S. Dept. of Justice, "Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion," accessed on 21 June 2004 at http://www.usdoj.gov/criminal/cybercrime/zezevSent.htm

[21] The New York Times http://nytimes.com/2003/01/03/nyregion/03THEF.html

[22] BBC News, "South Korea probes online dealing fraud," 8/26/2002, accessed at: <http://news.bbc.co.uk/2/hi/business/2217584.stm>.

[23] CBS News, "'Logic Bomb' Dropped On Brokerage," accessed on 21 June 2004 at http://www.cbsnews.com/stories/2002/12/18/tech/main533450.shtml.

[24] 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.

		M.D. Doshi Securities employee	respective access to BOLT and the M.D. Doshi Securities system.[25]
July 1, 2001	Two unidentified online brokerage firms	Chang Shian-tang	NT$10 million—Chang Shian-tang used decoding software to steal the passwords and personal information of more than 2,000 customers; apprehended after the brokerage companies complained of unusually high incidences of short-selling.[26]
Mar 15, 2000	Internet Trading Technologies	Abelkader Smires	Denial-of-service attacks that caused major disruption of trading on the NASDAQ.[27]
1999	ETrade Group (plus eBay and Lycos among others)	Jerome Heckenkamp	Denial-of-service attacks that caused more than $900,000 in damage.[28]
Nov. 14, 1999	Shanghai Securities Department	Zhao Zhe	Changed 5 transaction records, causing turnover of 2 stocks to rise drastically and resulting in direct loss of $355,000.[29]

Online Frauds

1. Investment Scams

In the US and South Korea, where the penetration of e-finance in the capital markets have been the most wide-spread, seven out of the "top ten securities frauds" involve online investment scams.

Investment Scams are investment schemes created by illegitimate intermediaries to collect funds from inexperienced and small investors with false promises of extremely high returns in a very short time with little or no risk. Through the use of electronic means such as the Internet for securities transactions or dissemination of information, these individuals enjoy the advantages of anonymity and increased outreach to large groups of unsophisticated investors at minimal costs.[30]

Promissory notes scams or prime bank notes are investor scams that involve schemes where investors are told that they have access to "secret" trading programs that only a few privileged

[25] The Cyber Crime Investigation Cell of the Criminal Investigation Department in Mumbai (Bombay), India reported this first instance of online security fraud investigated by the cell. http://www.cybercellmumbai.com/Cyber%20Crime%20News/crimenews.htm

[26] The Taipaei Times, "Hacker Arrested for Online Trading Scam," accessed on 17 June 2004 at http://www.taipeitimes.com/News/archives/2001/07/03/0000092498.

[27] National Infrastructure Protection Center Major Investigations Web site: www.nipc.gov.

[28] USA Today, "Los Alamos employee may have history of hacking," accessed on 17 June 2004 at http://www.usatoday.com/tech/news/2001-01-26-los-alamos-hacker.htm

[29] Nando Times, "China Jails Hacker for 3 Years," accessed on 21 June 2004 at http://www.landfield.com/isn/mail-archive/1999/Nov/0029.html

[30] See http://www.sec.gov/investor/pubs/cyberfraud.htm

people will be invited to take part in. The scheme promises access to the trading of certain bank securities such as bank guarantees, notes, stocks, or debentures at a discount price and sell them at a premium. Investors are then asked to sign "non-disclosure " agreements which prevent them from talking about the deal with anyone, including a lawyer or financial advisor. Investors are asked to ensure their funds are "good, clean and clear of criminal origin". The notes usually claim to be guaranteed by a well-known bank. In some variations of this scam, the investor is instructed to send money to a foreign bank, for example in the Bahamas, the Cayman Islands, or the Isle of Man. Later, the money is transferred to an offshore account controlled by the con artist.

2. Online Investment newsletters and e-mail spams

While the Internet, when properly used can be an effective tool for legitimate research providers in giving investment advice and disseminating unbiased information about the market, it also provides a venue for securities “touting” or market manipulations. Hundreds of online investment newsletters are published on scores of internet sites. The most common fraudulent activity using online newsletters is where an investor manipulates a stock’s price upward by widely disseminating false news about the stock or the issuing company and then trading the stock to profit from the manipulated price. The same effect can be obtained by using e-mail or IM (instant messaging), where the manipulator sends a mass e-mail with “investment tips”, which then causes an investor to buy thus artificially inflating the price of the stock. This is also referred to as called “pumping and dumping of stocks”.

An economical means of choice for pumping and dumping stocks on a mass scale is spam. In the UK, according to spam-detection specialist ClearSwift, the number of spammed stock tips has risen more than 300 percent between December and March of 2004, which translates into thousands of bogus investment tips on a variety of obscure firms listed on exchanges around the world reaching a significant audience of small investors through e-mail. A spammed e-mail usually consists of millions of potential recipients.

3. Fraud through Social Engineering[31]

Impersonation of a credible entity on bulletin boards or a discussion forum can lead to leakage of vital information. It could also be the source for unwarranted malicious knowledge which can negatively affect the trader's decision making process. Decisions by traders can now be affected by manipulated through the impersonation a.k.a. spoofing[32] of legitimate sources of information i.e. websites and email address**.**

[31] In her book, "Information Warfare and Security", Dorothy Denning defines 'social engineering' as: "…operations that trick others into doing something they would not do if they knew the truth, for example, giving out a secret password or sensitive corporate information. Any medium that provides one-to-one communications between people can be exploited. All that it takes is to be a good liar." (pgs. 111-112).

[32] **Brand spoofing--**Hackers will fake or spoof websites of legitimate and existing organizations, in order to deceive the customer into thinking they are interacting with the legitimate company. Customers submit sensitive information such as user identification numbers, passwords, credit card numbers, bank account information, and other forms of financial data. Customers do so, unknowing that this information is going into illicit hands. This type of social engineering can involve a digital communication (e.g., e-mail) that contains a link to a website. Once the customer clicks on the link, (s)he is redirected to a fraudulent website. When a customer is lured to the website, their information and/or money is stolen from them through digital means. **Industry spoofing--**Fake or spoofed organizations or industries that purportedly exist to mitigate risks, such as escrows and other third party mediators, that customers are socialized into trusting.

III. Conclusions and Predictions for Further Research

The convergence of certain innovations in the securities market over the past decade is fostering a fertile environment for fraud, increasing operational risk and are amplifying the potential for systemic failure. By utilizing E-platforms, brokers can reduce costs and barriers to market participants but increase the probability of investor fraud. "Buyer beware" takes on significantly new meaning in the online, 24 x 7 environment. E-brokering coupled with the use of unsecured wireless devices by traders and those in the pit are indicative of the new kinds of operational risks that should be understood, analyzed and mitigated before they are incorporated into a business architecture. Certain costs and risks associated with the e-finance revolution have yet to be fully appreciated. Recently, technologists have published books which state that not all information or transactions belong in the online world. Decisions to put any information online should be made in a reasonably prudent manner after a thorough risk benefit analysis and awareness of the weaknesses and vulnerabilities inherent in the system.

The monograph ***Electronic Safety and Soundness*** presented a four pillar framework for policy makers in emerging markets to use in designing responses to the challenge of assuring electronic safety and soundness of their financial systems. As such, this monograph focuses in part on technological solutions; depicted within the architecture of the 12 layer matrix[33], but more importantly on the incentives of the many parties involved to assure the security of critical infrastructures ranging from telecommunications and financial sector service providers to the government as well as to final consumers of financial or other services.

Securing the open network is first and foremost the responsibility of the service providers. Businesses need to understand the risks and responsibilities of providing services via these channels and seek continuous improvement in maintaining e-security. Technology is only a part of the solution; sound business principles such as responsibility, accountability and trust are also essential to building infrastructure and a framework that can support e-business.

Utilizing ***Electronic Safety and Soundness*** as a foundation and methodology for further research, the authors of this white paper will attempt to discern the patterns of e-fraud and the operational risks experienced by capital markets and offer recommendations for legal, regulatory and technological safeguards that should be put in place to foster trust and confidence particularly in emerging capital markets.

[33] Specific layers range from the need to have a Chief Information Security Officer and an incident response plan, to finding the most appropriate type of firewall and encryptions systems. For more details refer to Appendix E.

Appendix A: Top Ten Traditional Investment Frauds[34]

According to a 2002 report by Kansas Securities Commissioner David Brant, in conjunction with the North American Securities Administrators Association (NASAA), the list of "Top Ten" Investment frauds that the securities commissioners are fighting are:

1. *Unlicensed individuals engaging in securities activities:* Unlicensed individuals often engage in securities market activities with insufficient credentials and disclosure. These individuals are also the ones who create and market investment scams where they collect funds from unsophisticated investors with false promises of high returns, and disappear with these funds or lose them in the market.
2. *Unscrupulous stockbrokers:* Brokers that are registered by the securities regulator also engage in fraudulent activities, such as "front running" and insider dealing.
3. *Analyst research conflict*:.[35] This includes analysts issuing overly positive research reports and making positive recommendations in order to win investment banking business for their firm.
4. *Promissory notes schemes:* These are short-term debt instruments issued by little-known or non-existent companies promising high returns with little or no risk.
5. *Prime banks*: These involve scammers promising investors triple-digit returns through access to the investment portfolios of the world's elite banks. They mainly target illegal groups of investors (like terrorist organizations) who wish to achieve high returns under strict secrecy.
6. *Viatical settlements*: These involve sale of death benefits by terminally ill patents to third parties where the insured gets a percentage of the death benefit in cash and investors get a share of the death benefit when the insured dies. These contracts are often bundled to be resold to unsophisticated investors. These are highly risky investments and generally are not regulated and are illegal.
7. *Affinity fraud*: These include scams that use potential investor's religious or ethnic identity to gain their trust and then steal their savings with false promises of high returns.
8. *Charitable gift annuities*: In some cases, it is a legal investment to sell at a higher price than their actual value, the difference constituting a charitable donation. However in some case, scammers put together false charities to steal the sale proceeds.
9. *Oil and gas schemes*: Investment scams involving speculation over oil and gas prices and promising unsophisticated investors high returns with no risk rising in frequency with predictions of oil shortages or a rise in gas prices.
10. *Equipment leasing*: While the vast majority of equipment leasing deals are legitimate, scams exist where investors are offered high returns with no risk, while in reality high commissions paid to the intermediaries and promised returns have been unrealistically high.

For more information, see: http://www.securities.state.ks.us/press/2002/topten8-26-02.html

[34] NASAA

[35] In May 2003, the New York Attorney General's office concluded a 10-month investigation into whether Merrill Lynch had issued misleading research reports by entering into a settlement agreement with the firm. Under the agreement, Merrill Lynch agreed to pay a $100 million fine and make significant changes to way it does business.

Appendix B: SEC Regulations and Guidelines per Information Security

Recent laws enacted by the U.S. Congress impose considerable privacy and security requirements on health information, financial information, and Government information and systems. They *each* require an enterprise approach to security, involving the senior management of the organization. Cumulatively, they impact a large portion of private sector systems. The two major laws directly impacting financial sector security programs are:

1) *Gramm-Leach-Bliley Act (GLBA)*
2) *Sarbanes-Oxley Act of 2002*

The Gramm-Leach-Bliley Act (GLBA),[36] states that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[37] The GLBA definition of "financial institutions" encompasses banks, securities firms, insurance companies, and other companies providing many types of financial products and services to consumers. This includes lending, brokering or servicing any type of consumer loan; transferring and safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; collecting consumer debts; and other types of financial services.[38] GLBA's definition of financial institutions has even swept up colleges and universities.[39]

Pursuant to the GLBA, the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and Federal financial regulatory bodies[40] have issued regulations requiring administrative, technical and physical safeguards for financial information. The statute specifies that the regulations are intended:

1) To ensure the security and confidentiality of customer records and information;

2) To protect against any anticipated threats or hazards to the security or integrity of such records; and

3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[41]

---

[36] Gramm-Leach-Bliley Act of 1999, Pub. Law 106-102, 113 *Stat*. 1338 (1999), http://www.ffiec.gov/ffiecinfobase/resources/management/con-15usc_6801_6805-gramm_leach_bliley_act.pdf (hereinafter "GLBA").
[37] GLBA, 15 U.S.C. § 6801, http://www4.law.cornell.edu/uscode/15/6801.html.
[38] "Financial Privacy: The Gramm-Leach Bliley Act," http://www.ftc.gov/privacy/glbact/.
[39] "Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information," *NACUBO Advisory Report 2003-01*, National Association of College and University Business Officers, Jan. 13, 2003, http://info-center.ccit.arizona.edu/~security/GLBA_Summary.pdf.
[40] The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, and the National Credit Union Administration.
[41] GLBA, 15 U.S.C. § 6801, http://www4.law.cornell.edu/uscode/15/6805.html.

The regulations set forth the required steps that must be taken, but they do not specify what the technical components of a safeguards program must be. For example, the Federal Trade Commission requires that financial institutions under its purview must develop a plan in which the institution must: (1) designate one or more employees to coordinate the safeguards, (2) identify and assess the risks to customers' information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks, (3) design and implement a safeguards program, and regularly monitor and test it, (4) select appropriate service providers and contract with them to implement safeguards, and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firms business arrangements or operations, or the results of testing and monitoring of safeguards.[42]

The SEC has historically emphasized the positive aspects of new technology, focusing on increased communications ability: "The Securities Act of 1933 and the Securities Exchange Act of 1934 are premised on the philosophy that investors are best protected in making investment decisions if they are presented with full and accurate disclosure of all material information about investments."[43] Accordingly, its guidelines and regulations regarding information security aim at ensuring easier access to and widespread adoption of new technology. A few examples include:

Rule	Date	Title
33-8410	4/21/2004	Mandated Electronic Filing for Form ID
33-8230	5/7/2003	Mandated Electronic Filing and Website Posting for Forms 3, 4, and 5
34-48167	7/11/2003	Electronic Filing by Investment Advisers; Amendments to Form ADV; Technical Amendments
33-7472	10/24/1997	Rule to Provide That the Commission Will Not Accept Paper Filings That Are Required To Be Filed Electronically
Release	**Date**	**Title**
Securities Act Release No. 7233, Exchange Act Release No. 36345	10/6/1995	Use of Electronic Media for Delivery Purposes
Securities Act Release No. 7288, Exchange Act Release No. 37182	5/9/1996	Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information

The SEC does address the impact of fraud on technology with the provisions it has adopted in the wake of the Sarbanes-Oxley Act of 2002.[44] Title VIII, Section 1348 of the Act, entitled "Securities Fraud," ensures that any person who tries to defraud another in connection with a security can be fined and/or imprisoned. Additionally Title XI, Section 105 of the Act deals with corporate fraud accountability and gives the SEC the authority to prohibit people from serving as

[42] *See* "Financial Institutions and Customer Data: Complying with the Safeguards Rule," http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.
[43] "Report to the Congress: The Impact of Recent Technological Advances on the Securities Markets," accessed at http://www.sec.gov/news/studies/techrp97.htm
[44] Sarbanes-Oxley Act, accessed at http://www.law.uc.edu/CCL/SOact/soact.pdf.

corporate officers or directors. Pursuant to the Act, the SEC has adopted the following provisions:

Section	Date	Rule Adopted
302	8/27/2002	Requires CEOs and CFOs to certify financial and other information in their companies' quarterly and annual reports
403	8/27/2002	Accelerates deadlines and mandates electronic filing of disclosures of insider transactions in company stock
401(b)	1/15/2003	Regulation G: governs the use of non-GAAP financial measures, including disclosure and reconciliation requirements
404	5/27/2003	Requires an annual management report on and auditor attestation of a company's internal controls over financial reporting

Additionally, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (or Patriot Act) contains a provision against fraud in the securities markets. Pursuant to Section 326 of the Patriot Act, the SEC, in conjunction with the Treasury Department's FinCEN, issued Rule 34-47752 entitled "Customer Identification Programs For Broker-Dealers." Effective 6/9/2003, the rule "requires brokers or dealers to implement reasonable procedures to verify the identity of any person seeking to open an account, to the extent reasonable and practicable; to maintain records of the information used to verify the person's identity; and to determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency. This final regulation applies to brokers or dealers in securities except for brokers or dealers that register with the Securities and Exchange Commission solely because they effect transactions in securities futures products."[45]

The Financial Modernization Act of 1999 (or the Gramm-Leach-Bliley Act) addresses the impact of privacy concerns on information security. Pursuant to section 504 of the Act, the SEC issued Rule 34-42974 entitled "Privacy of Consumer Financial Information (Regulation S-P)" which implements notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. Effective 11/13/2000, the Rule requires a financial institution to "provide its customers with a notice of its privacy policies and practices [nor] disclose nonpublic personal information about a consumer to nonaffiliated third parties unless the institution provides certain information to the consumer and the consumer has not elected to opt out of the disclosure."[46] Finally, the Rule provides appropriate standards to protect customer information.

? Though the Sarbanes-Oxley, Patriot, and Gramm-Leach-Bliley Acts, and the related SEC provisions, pertain more to protection against fraud than protection against hacking, the SEC is attentive to the problems hacking can bring. A 2003 paper entitled "Sound Practices to Strengthen the Resilience of the U.S. Financial System"[47] names four practices to ensure the resilience of the U.S. financial system: (1) identify critical activities; (2) determine the appropriate recovery and resumption objectives; (3) maintain sufficient out-of-region resources

[45] "Customer Identification Programs For Broker-Dealers," accessed at http://www.sec.gov/rules/final/34-47752.htm.

[46] "Privacy of Consumer Financial Information (Regulation S-P)" accessed at http://www.sec.gov/rules/final/34-42974.htm.

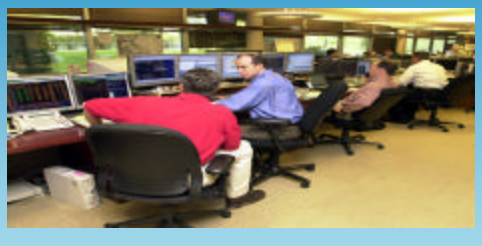
[47] "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," accessed at http://www.sec.gov/news/studies/34-47638.htm.

to meet recovery and resumption objectives; and (4) routinely use or test recovery and resumption arrangements. These practices focus on minimizing the immediate effects of a wide-scale disruption on critical financial markets.

Appendix C: The New York Mercantile Exchange and Wireless STP[48]

Wireless STP System

- Order information clear & accurate
- Increased customer control
- Immediate entry into clearing
- Instant order status & assignment information



New York Mercantile Exchange

Reduced Errors & Instant Feedback

- No more 'analog' errors:
  - No voice confirmation of orders
  - No handwriting to interpret
- Instant confirmation of:
  - Orders
  - Trade execution
  - Allocation

New York Mercantile Exchange

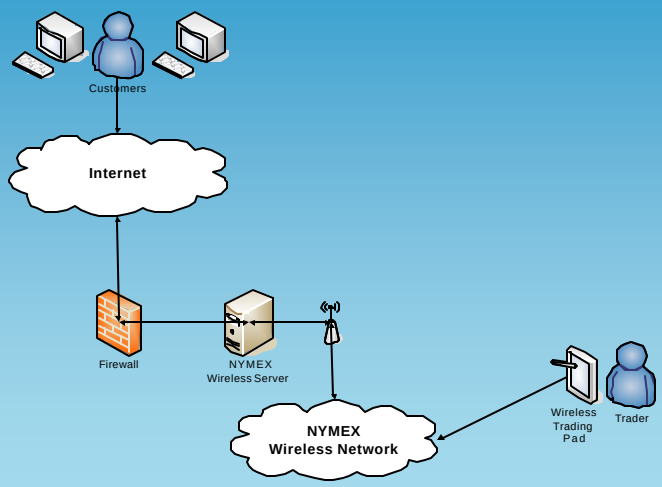
[48] This presentation was given by Samuel Gaer, CIO of the New York Mercantile Exchange, Inc, in New York at the IMN Wireless on Wallstreet Conference, July 29th, 2004.

Lowers Costs & Increases Volume

- Lowers costs:
  - Fewer errors
  - No paper to supply
- Increases volume
  - Automation improves performance
  - Historical track record
    - Pilot program in electricity futures over seven-week period, volume up 12%

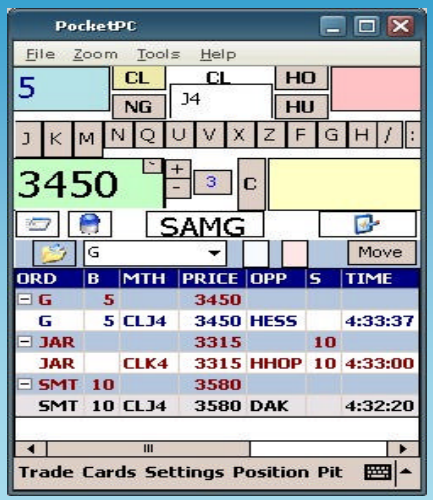
New York Mercantile Exchange

Straight-Through Processing Diagram



New York Mercantile Exchange

ePitCard Application



- User friendly
- Familiar layout
- Powerful
- Many valuable features

New York Mercantile Exchange

Appendix D: Organizations Working to Establish Best Practice per Web Services Security

E-finance is heavily reliant upon web services. Web services are one group of new technologies and standards for connecting to customers, exchanging data, and building applications across the Internet. Web services allow applications to communicate across platforms and programming languages using standard protocols based on XML. A number of organizations are attempting to develop best practice per web service security. These consortiums are defining many of the *infrastructure* standards that enable Web services as well as the *implementation* standards that are used in specific communities and across industries.

1. **Financial Services Technology Consortium**
   http://www.fstc.org

2. **The Liberty Alliance Project**
   http://www.projectliberty.org/

3. **The World Wide Web Consortium**
   http://www.w3c.org

4. **Organization for the Advancement of Structured Information Standards**
   http://www.oasis-open.org

Appendix E: The 12 Layer Matrix

Twelve core layers of proper security are essential for maintaining the integrity of data and mitigating the risks associated with open architecture environments, and in many instances, actual implementation of a specific layer need not entail large capital investments or outlays. The creation of the position of Chief information Security Officer (CISO), who oversees that the 12 layers are carried out and implemented in accordance with the best, is essential in order to preserve the survivability of the network.

1. **Risk Management—**A broad based framework based upon CERT's OCTAVE paradigm for managing assets and relevant risks to those assets.
2. **Cyber-Intelligence-** Experienced threat and technical intelligence analysis regarding threats, vulnerabilities, incidents, and countermeasure should provide timely and customized reporting to prevent a security incident before it occurs.
3. **Access Controls/Authentication—**Establish the legitimacy of a node or user before allowing access to requested information. The first line of defense is access controls; these can be divided into passwords, tokens, biometrics, and public key infrastructure (PKI).
4. **Firewalls**—Create a system or combination of systems that enforces a boundary between two or more networks.
5. **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.
6. **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.
7. **Virus scanners**—Worms, Trojans, and viruses are methods for deploying an attack. Virus scanners hunt malicious codes, but require frequent updating and monitoring.
8. **Encryption**—Encryption algorithms are used to protect information while it is in transit or whenever it is exposed to theft of the storage device (e.g. removable backup media or notebook computer).
9. **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.
10. **Vulnerability testing**—Vulnerability 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.
11. **Policy Management Software—**a software program should control Bank policy and procedural guidelines vis-à-vis employee computer usage.
12. **Business Continuity/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.

References

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

Gaer, Samuel. 2004. *The Benefits of Straight-Through Processing.* July 29. Presentation.

Glaessner, Thomas, Tom Kellermann, and Valerie McNevin. 2002. *"Electronic Security: Risk Mitigation in Financial Transactions."* Washington D.C. The World Bank. June.

Glaessner, Thomas, Tom Kellermann, and Valerie McNevin. 2003. Electronic Safety and Soundness: Washington D.C. The World Bank. October**.**

Kellermann, Tom. 2002. *Mobile Risk Management: E-Finance in the Wireless Environment.* May 2002. World Bank, Washington D.C.

Securities Fraud FAQs
http://www.timothykarenlaw.com/CM/Custom/Custom26.asp

Securities Fraud Infocenter
http://www.securitiesfraudinfocenter.com/information.php

MARKET MANIPULATION AND INSIDER DEALING
The introduction of revised legislative provisions concerning market manipulation and insider dealing.
http://www.jerseyfsc.org/pdf/Consultation%20Paper%20No6.pdf