Electronic Safety and Soundness

A. Overview of the Threat

Trends in cyber crime reveal significant growth. Attacks on servers doubled to over 53,000 in 2001. In 2002 over 83,000[1] security incidents were reported. Vulnerabilities in software code have grown from a total of 500 in 1995 to over 9000 in 2002 (CERT). The Internet Data Corporation (www.idc.com) reported that more than 57 percent of all hack attacks last year were initiated in the financial sector. The FBI has corroborated this statistic. FINCEN's Suspicious Activity Reports for Computer Intrusions have shot up more than 300% over the past year[2]. Over $222 B in losses were sustained to the global economy, as a result of ID Theft.[3]This is a direct result of three phenomenon: First, organized crime has made a business model out of hacking. Second, there is an overemphasis on funds transfer rather than the current modus operendis of identity theft, salami slicing and extortion. Finally, there has been an overemphasis on data in transit rather than data storage. High levels of encryption will not thwart hackers. Hackers target servers, remote users and hosting companies all of which have end-to-end encryption however their data storage points are only protected by firewalls which are not fool proof. Rather than business continuity data integrity and authentication should be priorities. Defense in depth e.g. Layered Security is essential.

B. Three Trends in E-fraud

1. **E-Fraud rates are more than 83 times higher[4]** than those experienced by the bricks and mortar merchants. According to Meridien Research, online credit card fraud totaled $9 billion in 2001. E-security incident reports increased 200 percent between 2000 and 2001 in the United States alone. Reported incidents of identity theft are projected to more than double, from FBI estimates of 700,000 in 2001 to 1.7 million in 2005, the National Fraud Center estimates that $55 Billion in costs to the financial sector associated with ID Theft last year. 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.

2. **Outsourcing is creating a security quagmire.** As in the S1 Case[5] in the summer of 2001. 300 Bank networks were compromised due to the successful hack of S1's servers. *Who or what is a money transmitter?* Today, the set of entities

---

[1] http://www.cert.org/stats/cert_stats.html#incidents

[2] Suspicious Activity Reports (SAR) for computer intrusions have grown from 419 in 2001 to over 1,293 in the first 8 months of 2002. http://www.fincen.gov/sarreviewissue5.pdf

[3] Aberdeen Group June 2003 Report on the Economic Impact of ID Theft

[4] *The Myth of Online Payments*. Mike Voorhees (2002).

[5] Glaessner, Kellermann and McNevin. 2002. E-security Risk Mitigation in Financial Transactions. World Bank. May.

involved in money transmission or payments is more difficult to define than one might expect.[6] 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. 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 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. 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.

3. **New Trends in Hacking.** There has been an overemphasis on denial of service attacks in the financial sector as well as funds transfer. Hackers, like bank robbers, do not want to burn down the bank. They would rather copy account information or subtract pennies from thousands of accounts e.g. the salami slice. In addition there has been a 700%[7] increase in the number of worms in the wild. Code Red, Nimda and Slammer were all worms. Worms exploit vulnerabilities in software code, allowing them to circumvent perimeter defenses like firewalls, intrusion detection systems, virus scanners and encryption. According to CERT, over 4,000 such vulnerabilities were discovered last year. Though known blended threats are exploiting only a miniscule fraction of vulnerabilities, they are doing so with tremendous success. Only through frequent vulnerability testing coupled with short timetables for patching these holes, will these threats be averted. Credible sources of Cyber-intelligence assist in the forecasting of such phenomenon.

[6] For further information, see the EU directive 2000/46/EG, pertaining to electronic money institutions and the regulatory framework for money transmitters in the EU.

[7] www.cert.org

C. Systems and Operational Risk Management

First, define e-security at an industry-wide level.
The E-Security definition per “E-Security: Risk Mitigation”:
"Broadly speaking, electronic security is any tool, technique, or process used to protect a system’s information assets. Electronic security enhances or adds value to a naked network and is composed of soft and hard infrastructure. The soft infrastructure components are the policies, processes, protocols, and guidelines that protect the system and the data from compromise. The hard infrastructure consists of hardware and software needed to protect the system and data from threats to security from inside or outside the organization."

Second, per this definition of e-security, strictly identify and outline core areas (or agenda) for security assessment by the Fed.
A. The hard infrastructure includes an identification of what point banks are in implementation of the technical components of the 12 layers. These are: CSO, access controls/authentication, firewalls, active content filtering, IDS, virus scanners, encryption, vulnerability testing. These can be classified into implemented, in-process, being upgraded, etc.
B. The rest of the 12 layers can be thrown into a procedural bucket, or soft infrastructure. Identify and implement a risk management framework, define what is proper systems admin, does the bank use of policy management software, and have a coherent and narrowly defined Incident Response Procedure.

The three general axioms to remember in building a security program are as follows:

- Attacks and losses are inevitable.
- Security buys time.
- The network is only as secure as its weakest link.

Table 1: 12 Layers of Security[8]

12 Layers	Details	Implementation Status*	Risk Level** (1-5)
Chief Information Security Officer	Bring the issue to the C-level. For Accountability's sake. CISO is a General who is responsible for layering defenses according to best of breed cyber-intelligence.		**3**
Cyber-intelligence	With 11 new vulnerabilities as well as over 230 new viruses, worms and Trojans discovered daily, this is critical.		**5**
Authentication	Passwords are obsolete and can be compromised and easily. PKI is only as strong as the private key storage. 2 Factor authentication is critical.		**5**
Firewalls	It is very important to remember that the firewall *does not* stop traffic on the ports that *are* allowed. A firewall cannot prevent what is already allowed through the system. Proper Firewall configuration is essential.		5
Intrusion detection systems	Intrusion detection systems (IDSs) need to be monitored 24 hours a day to obtain the best return on investment. This work schedule positions the institution to respond to suspected intrusions in a timely manner and prevents the inadvertent loss of resources resulting from a misconfigured IDS. IDS are reactive in nature.		3
Virus Scanners	Virus scanners should be updated every night. Beginning with an institution's e-mail gateway, every inbound attachment should be scanned for viruses.		4
Policy Management Software	Bank policy vis-à-vis computer usage necessitates enforcement by a software program. The verbal policy dimension should be translated into machine code.		4
Vulnerability Testing	Proactive way of testing your defenses.		**5**
Encryption	Symmetric and asymmetric		4

[8] Table 1 identifies perquisites for electronic safety and soundness. Shaded rows represent areas within the defensive posture, which are currently neglected.

	key encryption both are used to scramble data so completely that an attacker lacking the correct "key" is unable to determine the message. Encryption merely creates a steel tunnel. Layered security is essential for the ends of this tunnel.		
Proper Systems Administration	Eg. Network administrators should be responsible for installing and verifying patches and updates to operating systems weekly.		5
Active Content Filtering	At the browser level, it is necessary and prudent to filter all material that is defined by policy to be inappropriate for the workplace or that is contrary to the institution's established workplace policy.		4
Incident Response	Too much emphasis is paid to this. What good is backing up the data if it has been corrupted and or compromised? Although necessary highly reactive.		3
Wireless	WLANs create a connection to the heart of any network these should be managed through a 15-layer process depicted in Annex III of E-security: Risk Mitigation in Financial Transactions.		**5**

**Implemented, In-Process, Being-upgraded, Not Implemented*
***Risk Level refers to 1 as the lowest level of risk, and 5 as the higher*

Once layered security is in place Continuous Monitoring, Reporting & electronic risk audits should be performed. Most Banks are currently deficient in proactive vulnerability testing, credible cyber-intelligence, and two factor authentication. Over reliance on Firewalls, encryption and virus scanners is commonplace.

Financial Service Providers should adopt these practices in multiple steps. For example, the first round should entail inventory. Banks can identify what hardware they are using in order to pinpoint potential areas of vulnerability-- types of servers, types of databases, software, etc. Next, each bank can identify what defenses they are using. Then, establish internal procedures for monitoring and reporting both technical and policy. After this, make e-security reporting practices a part of the routine. For example, standardize reporting procedures in confidential, anonymous reports to the Fed, or make them a part of quarterly reports so that there is a level of accountability.

Finally, education on the hard & soft infrastructure is critical. Education should entail explanations of each of the technologies, e.g. what is IDS, how does it work, how can one implement it to maximize its effectiveness, and where can you get the most up-to-date info on IDS? Also, what policy framework will be used (CERT, OCTAVE) and how will it be assessed, e.g. what does "proper" sys admin mean, and how will this be monitored? Proper Systems administration is dealt with in Annex I of E-security: Risk Mitigation in Financial Transactions and the FFIEC IT Examination Handbook.

It is important to note that the FFIEC Handbook does not address the WLAN security, instant messaging vulnerabilities, Voice Over IP Vulnerabilities, Satellite vulnerabilities and finally the 700% growth in worms and how these new threats circumvent perimeter defenses by exploiting vulnerabilities in software code. The World Bank White Paper E-security Risk Mitigation in Financial Transactions does address all of these issues.

Conclusions

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 special audit and examination teams in e-risk analysis, risk management, and IT issues. These teams should focus on the 12 layers of security and review the integration for new technologies like WLANs.
- Require clearer management responsibility and accountability to create and sustain safety and soundness. Management should include a Chief Information Security Officer who is accountable for implementing the 12 layers and utilizing outside independent firms to audit his or her security posture.

Compliance

- Develop analytical teams to assess and monitor e-risk management.
- Disconnect any entity from the system that is not in compliance.

Produced by Tom Kellermann, Sr. Data Risk Management Specialist, Integrator Unit, The World Bank June 13,2003

- 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, chief information officer, security officer, etc. and senior management (including the CFO, CEO) and even the board of directors.[9]

For more information please refer to www1.worldbank.org/finance (Click on E-security)

[9] 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.

Produced by Tom Kellermann, Sr. Data Risk Management Specialist, Integrator Unit, The World Bank June 13,2003