International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Issues in Electronic security infrastructure in Banking System

CH.Nagabhushanam

Lecturer in physics, Dept. of Physics, K.B.N College, VJA

Abstract— 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 of tanned 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 insurances 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 is Susana key to enhancing prevention.

I. ELECTRONIC SECURITY

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. Given that the Internet is a broadcasting medium, constraints have to be added to target only intended recipients. As a result, the need for security is a constant of doing business over the Internet.

Electronic security will require more attention as new technology creates new risks and as technologies converge.

For purposes of this paper, e-finance is the use of electronic means to exchangeinformation, transfer signs and representations of value, and execute transactions in a commercial environment. E-Financecomprises four primary channels: electronic data interchange (EDI), electronic benefits transfers (EBTs), and electronic tradeconfirmations (ETCs), electronic fund transfer (ETF).

Today one criminal using tools 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.

Because electronic data is invisible to the naked eye and because most people do not have

Computer skills, they may erroneously believe that stored information cannot be captured easily. In truth, it often takes few skills to access the data and manipulate, pollute, or steal it. Ironically, it may require even fewer resources and skills to protect the data in the first place. All four channels of e-finance are susceptible to fraud, theft, embezzlement, pilfering, and extortion. Equally important is that in many breaches the breakdown results from a failure to implement appropriate risk-management processes or from the use of off-the-shelf commercial software.

The electronic security industry is growing - becoming global - and will present public policy challenges even in the areas of competition policy, potential conflicts of interest, andcertification.

E-security companies and vendors generally fall into three categories: access, use, and assessment. Today's industry includes companies that provide active content monitoring and data filtering, develop intrusion detection services, place firewalls, conduct penetration tests to expose hardware or software vulnerabilities, offer encryption software or services, and createauthentication software or services that use passwords, tokens, keys, and biometrics to verify the identity of the parties or the integrity of the data.

The public interest case for regulation of the electronic security industry must be recognized. Important trade-offs exist between electronic security and such areas as costs, quality of service, technological innovation, and privacy. Formulation of regulation and policy needs to take explicit account of these trades-offs.

Traditionally, the telecommunications industry has been regulated as being essential to public health, interest, and welfare. Hence, a core component of its regulatory model was

to expand service to give everyone access. In many countries, access to basic service is now considered anecessity of modern life. Historically, the financial services industry has beenregulated by the premise that trust and confidence are paramount to the orderly movement of trade, goods, and money. And, given that a special trust is conferred on financialentities, they must conduct their business in a safe, sound, and prudent manner. Convergence of the telecommunications industry and the financial services sector through the Internet heightens the importance of and the necessity for sound public policy and informed regulation to ensure that government, business, and people continue to have access to secure financial services.

Any attempt to develop public policy to improve or establish electronic security needs to be built on at least the following seven important pillars(issues): (i) an adequate legal and enforcement framework — which is not present today in many emerging markets; (ii) adequate arrangements to ensure electronic security of payment systems; (iii) an adequate supervision and prevention regime that creates better incentives to implement adequate layered risk - management systems for electronic security inside financial services providers; (iv) a framework within which private insurance companies can insure against and monitor e - risk, thereby helping to improve standards in this area via the underwriting covenants they require; (v) certification standards and processes established with respect to digital signatures and, more broadly, to vendors operating in the electronic security industry; (vi) actions to improve the accuracy of information available about e - security incidents and the roles of the public and private sectors in this process; and (vii) broad education on security issues as a means of preventing e - security incidents.

Pillar I: Legal Framework and Enforcement

Countries adopting electronic banking or electronic delivery of otherfinancial services (e.g., distribution and trading of securities) must incorporate electronic security concerns in their viiipolicies, laws, and practices, thereby allowing them to support secure operation of theirinstitutions and to combat crime and cyberterrorism. At a minimum, an e-finance legal framework should consist of the following:

- •Electronic transactions law and electronic commerce law
- •Payment systems security law
- •Privacy law
- •Cybercrime law
- •Anti-money laundering law

Pillar II: Electronic Security of Payment Systems

Payment systems are among the most important components of any financial system. The operative questions for this paper are whether money transmitters or ISPs add risk to the payment system, and, if so, how best that risk might be mitigated. Any answers to these questions must address at a minimum the following five problems:

Lack of definition for money transmitters.

Lack of reporting requirements.

3. Limited or no regulation.
4. Limited or no warranties, indemnification, and liabilities.

5.Lack of security requirements for service providers.

Pillar III: Supervision and Prevention Challenges

Beyond the monitoring of the payments system and the related supervision of money transmitters is the need to revisit regulation, supervision, and prevention approaches to financial services providers that engage in electronic banking or provision of other financial services.

Capital Requirements.The new Basel guidelines for capital, especially those dealing with operational risk, do not address the problem of measuring either the risk to reputation or the strategic risk associated with electronic security breaches. Hence, there is a question of how best to measure a bank's operational risks when the information about computer security incidentsnot accurate and when defining reputation damage is difficult, not to mention the needed adjustment to capital that would result from such a breach.

Pillar IV: The Role of Private Insurance as a Complementary Monitoring system

Because financial supervisory agencies are still in the process of developing their regulatory standards, and because of the difficulties of monitoring complex transactions with rapidly changing technologies, it is important to seek complementary private solutions to the monitoring of risk. The insurance industry already is playing a role in this area despite the defects inherent in the underlying information used to price e-risk coverage. Within the next few years, in the United States market alone, the growth in e-commerce liability insurance and, specifically, e-risk coverage is likely to become quite large and may total as much as $2.5 billion annually.

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

Both public and private entities must work cooperatively to develop standards and to harmonize certification and licensing schemes in order to mitigate risk. Two categories that require particular attention in terms of certification deal with electronic security service providers and transaction elements.

A necessary first step in securing e-finance is to require licensing by financial regulators of vendors that directly affect the payment system, such as money transmitters or ISPs. The nextstep is to require the industry to certify vendors that

provide electronic security services. Many vendors already offer some type of certification, and recently the security industry has developed a Security Expert certification. Industry experts should review this certification process and, if they deem it appropriate, endorse it. By using certification, the industry benefits by providing the consuming public with a recognized structure, accountability between the industry and its self-proclaimed experts, and a means of separating the approved expert from the self-authorized expert. It also elevates the craft to a professional status and creates an incentive for the industry to both raise and protect standards. Certification is a time-tested approach from which numerous professional groups, such as accountants and lawyers, have benefited.

A second area to address is certification of such transaction elements as electronic signatures. The value certification brings to a transaction in part depends on who or what provides the certification and on the elements that are being certified. In general, certification would provide an enhancement of an existing service, such as that of notaries. Or it could be offered by a quasi-private entity, such as a post office, or a private entity, such as a bank. Each of these scenarios, however, presents unique structural and governance issues. For example, post office certification would require the use of registration agents and storage to maintain a large information repository. By contrast, in many countries private companies (financial services providers or nonfinancial companies) may be better equipped to provide the information infrastructure required to act as certification agents or to provide cross-certification checks for a fee. This, too, necessitates the creation of an internal governing structure and an appropriate repository and record-retention scheme to house and protect the digital information for perhaps decades.

The important element essential to any of these scenarios is that certification structures located in different jurisdictions must consistently provide the same attributes to the transaction and that a certifier's scope of authority and liability must remain consistent across jurisdictional borders. Today, a significant lack of consistency exists in the means by which certification structures are organized under the law in the various states. For example, a certification authority in Utah has a very different scope of authority and operates under a different liability structure from a certification authority in Florida or Illinois. Thus, if a transaction is initiated in Illinois but concluded in Utah with a party in Florida, one should be acquainted with thelaws of each state in order to appreciate the ramifications of using certification authorities in each state.

Transactional certification is used primarily to ensure that the underlying transaction will be honoured. The main barrier that continually haunts the transactional side of e-commerce is the issue of nonrepudiation. It is essential that the parties "know" each other and,more important, know that each will perform and that each has legal remedy if the other fails to do so. The value of e-commerce is significantly undercut if this function cannot be provided in a simple, cost-effective manner. This function is accomplished in the electronic world by verifying or authenticating a party's identity. Technology offers numerous ways to insert such functions into the e-process. Although the use of PKI technology and certification authorities is often touted as the only accepted means of ensuring security, it is necessary to consider also the costs, the cumbersome structure associated with PKI, and the legal inconsistencies associated with certification authorities. It is also important to analyse the benefits of using alternative solutions, such as biometrics ordigital time stamps. The critical element is that the solution be consistent across borders in terms of scope and liability, no matter what technology is used to perform the function.

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

The lack of accurate information on e-security incidents is the result of the lack of incentives to capture the data, measure it, and inform. At worst, the failure to inform is tantamount to a breach of ethics; at best, it is a failure to notice. Electronic security would improve worldwide through the creation of a set of national and cross-border incentive arrangements to encourage financial services providers to share accurate information on actual denial-of-service intrusions, thefts, hacks, and so on. Today, ample evidence shows that no accurate base of information exists either within or across countries. Not only does this limit awareness but, even more important, it can limit the provision of private sector solutions (including insurance). This lack of information may even be acting to increase the cost to companies and financial services providers of insuring against such risks.

Pillar VII: Education and Prevention of E-Security Incidents

Statistical analysis reveals that in many countries throughout the world, more than 50 percent of electronic security intrusions are still carried out by insiders. An uneducated or undereducated workforce is inherently more vulnerable to this type of incident or attack. By contrast, a well - educated workforce that is conscious of security issues can effectively add a layer of protection. Educational initiatives will have to be targeted to financial services providers (both systems administrators and management), to various agencies involved in law enforcement and supervision, and to actual online users of financial services. Actions might include the following: improvement of awareness and education of financial sector participants about cyber ethics and appropriate user behavior on networked systems; creation of 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 on intrusions; development of

awareness in the banking community in emerging markets about the need for "incident response plans" in case an incident transpires; facilitation of cooperation and transfer of know - how among law enforcement entities, financial intelligence units (FIUs), and supervisory agencies in developed and emerging markets via such devices as more active exchange programs between personnel; design of well-focused courses for examiners under the auspices of the Financial Stability Institute or other training centres and development of a cross-border university outreach program to promote the training of future e-security professionals while also improving the education of online users of financial services.

II. Conclusion

For e-security truly a tool for trade in developing countries, a secure infrastructure which makes possible the electronic exchange of financial transactions is a necessary prerequisite. From technological perspectives this work discusses important issues for e-security in banking for developing countries in regards of lack of fraud repression and justice in those countries.

III. References

[1] Allen, F., McAndrews, J., &Strahan, P. (2001). E-finance: An Introduction, Working Paper No. 01-36. Financial Institutions Centre, Wharton University, Philadelphia, PA, 7 October,

[2] Anderson, E.W., & Sullivan, M.W. (1993). The antecedents and consequences of customer satisfaction for firms.Marketing Science, 12, (2), 125-43.

[3] Andreassen, T.W. (1999). What drives customer loyalty with complaint resolution?. Journal of Service Research, 1, (4), 324-32

[4] Bansal, H., &Voyer, P. (2000). Word-of-Mouth Processes Within a Service Purchase Decision Context. Journal of Service Research, 3, (2), 166-77.

[5] Black, N.J., Lockett, A., Winklhofer, H., &Ennew, C. (2001). The adoption of Internet financial services: A qualitative study. International Journal of Retail &Distribution Management, 29(8), 390-398.