

Abstract:-

Technological evolution is changing the way in which financial services are produced and delivered. The delivery of financial services has changed as the world has become a smaller place thanks to the worldwide networked infrastructure of the Internet.

Indeed, the delivery of financial services is moving toward an increasing multitude of alternative channels of delivery and away from the traditional bricks-and-mortar delivery channels (Claessens, Glaessner & Klingebiel 2004).

As the methods of delivery have changed, so to, have the risks involved with doing business. Internet users sending personal and proprietary data over the internet are increasingly at risk with respect to the information they send across the interconnected network, that is the Internet (Cranor, 2002). In the context of finance, these concerns hinge squarely upon the privacy of information. This paper will take a critical view of privacy and information security in finance. In doing this, the threats that arise because of the technologies of digital information and the kinds of countermeasures that can be effective will be discussed.

Information and privacy in the digital age

Information privacy relates to the right that the individual has in the controlling and handling of data about themselves (Clark, 1998). The emergence of the Internet as a vehicle for financial transactions has changed the nature of information transfer. While the Internet allows a myriad of social and economic transactions to occur effortlessly, at the same time, this technology enables a wide range of surveillance activities to occur which threaten our information privacy (Kang, 1998). Society is, of course, motivated by the great benefits that exist through the improved convenience and cost effectiveness of this technology. However, by putting our financial details onto networked computer sources, such as the Internet, we are potentially exposing highly private and sensitive information to outsiders. Indeed, the rapid uptake in the use of computer technologies has accentuated these privacy issues (Hann, Hui, Lee & Png 2000). The growth of electronic finance has raised public concerns regarding privacy as the Internet has introduced a myriad of threats to the integrity of this sensitive data. This paper will focus on digital communications and information resources and their respective impact privacy in the context of business finance

The traditional models of privacy, in the context of financial transactions which relied upon features of the built environments are becoming less relevant as increasingly the Internet is used for financial transactions. According to Claessens, Glaessner & Klingebiel; “financial trading is moving toward electronic platforms not tied to any location” (2004). Further, as information is now transferred seamlessly across interconnected networks, we see a shift in privacy concerns that simultaneously necessitates a shift in the efforts needed to protect personal information (Palen & Dourish, 2003). The use of the Internet to conduct financial transactions has been coined ‘electronic finance’. The term ‘Electronic finance’ includes all types of financial activities that can be carried out over the Internet. This involves online banking, electronic trading, and provision of financial services, electronic payment and the communication of financial information (Lin, Geng & Whinston 2001). These developments of electronic finance have greatly impacted on financial service industries (Lin, Geng & Whinston 2001).

There are two critical ways in which the financial service provision has been expanded through the use of information technology. The first way is through the point of contact. Many customers are using information technology driven communication channels rather than the traditional face to face methods of gaining access to financial services. The second way that financial service provision has expanded is through changes in trading systems. Trading systems are no longer tied to a particular location. Hence, trade can take place from any number of geographic localities. The major advantages that have come through the advancements of technology have been the lowering of costs associated in the provision of these services. Furthermore, the increased integration of consumers and financial services has resulted in an aggregation of the provision of services and demand that make financial services increasingly accessible and cost effective for both customers and suppliers (Lin, Geng & Whinston 2001).

From a financial service provider point of view, the most prominent rationale for the use of the Internet is the reduction of fixed costs and transaction costs. There has been a proliferation of electronic financial institutions using automated trading systems and virtual banks (Lin, Geng & Whinston 2001). Sadly, there is great disparity between the various approaches that are taken between utilities, retailers and consumers regarding the rules and laws relating to information-sharing and privacy (Claessens, Glaessner & Klingebiel 2004). The Wallis report in 1997 indicated that there needs to be a balance established between business efficiencies and privacy interests (Wallis, 1997). It's in the best interests of financial institutions to encourage customers to move to electronic varieties of banking and away from traditional forms of banking. Hence, an approach predicated upon pro-activeness rather than reactive is likely to lead consumers to embrace electronic commerce in its various manifestations (Tucker, 1999). Despite the success of the Wallis report in its many recommendations to the Finance sector it regrettably did not advance the privacy debate (Tucker, 1999).

While the potential benefits of electronic finance are substantial; there is nevertheless a need to mitigate risks associated with Internet based financial activities, in order to be able to reap the maximum possible benefits from this emerging trend (Claessens, Glaessner & Klingebiel 2004). Furthermore, these are substantial issues of trust that jeopardises the success of electronic finance. Indeed, overcoming trust issues is a priority for both business and consumers when it comes to dealing with electronic finance (Argy & Bollen 1999). Many organisations, including governmental agencies are increasingly taking steps, using Web-enabled technologies to develop consumer confidence. Importantly, technological solutions to privacy issues are steadily emerging.

The most prominent is the World Wide Web Consortium (W3C) Platform for Privacy Preferences (P3P) Standard. The P3P is a method for websites to encode their privacy policies in a computer readable format. Such tools allow users to control their use of personal information by providing warnings to users regarding the use of personal information. A shortfall of this P3P service is that it will only apply to those websites that voluntarily participate (Larson, Larson & Greenlee, 2003). Nevertheless, for those websites that do participate, the use of P3P allows computer users to make informed decisions regarding whether they would like to share information with this site. Further, this informs the user that if they are to use a particular site that their visit may involve the collection of data for marketing and other purposes therefore the user has the option to leave the site (Larson, Larson & Greenlee, 2003).

A number of empirical studies have evidenced that consumers have privacy concerns regarding e-commerce. Hershel and Andrews reported that many users show reluctance when it comes to purchasing on-line due to concerns regarding the privacy and security of their transaction information (Hershel & Andrews, 1997). While some industry associations have addressed the privacy issue through the use of P3P or the issuance of established codes of conduct (Clarke, 1999) there still seems to be a perception that the Internet is vulnerable to interception. Indeed, resolution of the trust issue for business will mean a dramatic boost to electronic commerce (Luo, 2001). McGraw notes that if a consumer trusts that the internet is secure and that their personal and transactional information will remain private they will flock to e-commerce (Keen, 1997). Similarly Reichheld and Schefter note that when consumers trust an electronic vendor they are more inclined to share personal information with that vendor (Reichheld and Schefter, 2000).

Encryption is a tool that is commonly used to promote internet security for financial transactions, essentially rendering the data unreadable to someone who does not have the encryption key. It involves the application of a symmetric encryption algorithm to data. Over time both cryptographic techniques and authentication methods for ensuring the integrity of private data have become a most valued security measure for financial transactions. Although while it is clear that encryption technologies continue to evolve and provide an increasingly formidable challenge to computer criminals, the computer criminals are also developing methods to circumvent such security measures. Therefore, it is clear that further technological safeguards are needed (Larson, Larson & Greenlee, 2003). Furthermore, the merging of finance and information technology necessitates further integration with respect to the security aspects of Internet use to foster consumer confidence to promote the further advancement of electronic finance.

This paper has taken a multifaceted view of privacy and information security from a finance perspective. Indeed, it is evident that the delivery of financial services is moving toward an increasing multitude of alternative channels of delivery and away from the traditional bricks-and-mortar delivery channels (Claessens, Glaessner & Klingebiel 2004). As a consequence of this, it is clear that in the context of finance, these changes come with threats, particularly those related to privacy and computer crime. This paper has considered some of rationales for emergence of electronic finance and also identified some of the key obstacles for consumers and financial service providers, namely trust. This paper also identified some methods that are being adopted to strengthen computer security.

Reference List

- Argy, P & Bollen, R 1999, 'Australia: raising the E-commerce comfort level', *IT Professional*, Vol. 1, Iss 6 pp. 56-58.
- Besnard, D & Arief, B 2004, 'Computer Security Impaired by Legitimate Users', *Computers & Security*, Vol. 23, pp. 253-264.
- Butler, S 2002 'Security Attribute Evaluation Method: A Cost-Benefit Approach, International Conference on Software Engineering. Proceedings of the 24th International Conference on Software Engineering, Florida pp. 232-240.
- Claessens, S, Glaessner, T & Klingebiel, D 2004, 'Electronic Finance: Reshaping the Financial Landscape Around the World', *Journal of Financial Services Research*, Springer Netherlands, Vol. 22, No. 1-2, pp. 29-61.
- Clarke, R 1999, 'Internet privacy concerns confirm the case for intervention', *Communications of the OCM*, Vol. 42, Iss. 2, pp. 60-67.
- Cranor, L 2002, *Web Privacy with P3P*. Oreily publications, United States.
- Greenleaf, G 2003, Australia's APEC privacy initiative: The pros and cons of 'OECD Lite', *Cyberspace Law and Policy Centre*, The University of New South Wales (11 January 2007) at http://www.bakercyberlawcentre.org/appcc/apec_ini.htm
- Hann, I, Hui, K, Lee, T & Png, I 2000, 'Online Information Privacy: Measuring the Cost-Benefit Trade-off, Proceedings of the 23rd International Conference on Information Systems, New York pp.1-10.
- Harper, I 1997, The Wallis report: An Overview, *The Australian Economic Review*, Vol. 30 Iss.3, pp. 288.
- Hershel, R & Andrews P 1997, 'Ethical implications of technological advances on Business communication', *Journal of Bus Communication*, Vol. 34, pp. 160-70.
- Kang, J 1998, 'Information Privacy in Cyberspace Transactions, *Stanford Law Review*, Vol 50, No. 4 pp. 1193-1294.
- Keen P 1997, 'Future of the Internet relies on trust', *Computerworld*, pp. 70.
- Larson, L, Larson, R & Greenlee 2003, 'Privacy Protection on the Internet', *Strategic Finance*, Vol. 84, Iss. 12, pp.49.
- Lin, L, Geng, X, Whinston, A 2001, 'New perspective to finance and competition and challenges for financial institutions in the Internet, *BIS papers*, No.7 pp. 13-25.
- Mercuri, R 2003, 'E-services: a cornucopia of digital offerings ushers in the next Net-based evolution', *Communications of the OCM*, Vol. 46, Iss. 6 pp. 15-18.
- Palen, L & Dourish, P 2003, 'Unpacking privacy for a networked world – Conference on Human Factors in Computing Systems. Proceedings of the SIGCHI conference on Human factors in Computing systems, Florida, pp. 129-136.
- Reicheld F, Schefter P 2000, 'E-Loyalty' *Harvard Business Review*, (July-August), pp. 105-113.

Smith, A 2004, 'Cybercriminal impacts on online business and consumer confidence, *Online Information Review*, Vol.28, Iss. 3, pp. 224.

Tucker, G 1999, 'Privacy recommendations for financial services – contrasting the Australian and Canadian approaches' *Privacy Law and Policy Reporter* vol.5, pp.1-4.

Wang, H & Rubin, B 2004, 'Electronic Government, *International Journal (EG)*, Vol.1, No.4.