Cyber Security Impacts on Logistics and Supply Chain Management

– **Ashish Agarwal**
Associate professor, School of Engineering and Technology
ashisha@ignou.ac.in

Cyber Security is a major binding force in most buyer-supplier transactions in today e-commerce business. It is significant when uncertainty and asymmetric product information are present in the transaction across the supply chain. One of the important characteristics of cyber security is developing trust among trading partners of a supply chain. E-commerce provides opportunity for cost cutting while improving the quality of goods and services. It also helps in increasing the speed of service delivery and corporate decision-making. It helps in reducing traditional operating costs. The transaction cost through e-commerce is minimum as network of communication reduces the cost of installing a virtual store on web. Internet is primary carrier of trading along the supply chain. Trading partners of supply chain fear insecure transactions as web sites can be counterfeited, identities can be forged and the nature of transactions can be altered. There is lack of personal interaction between buyer and supplier. Geographic dispersion of trading partners creates new and unprecedented opportunities for consumer abuse through fraud and deception. Use of digital signature has not guaranteed that the message comes from the person signing it. This can be due to the fact that the institute issuing the signature has inadequate administrative routines (Ba, 2001).

Introduction

Therefore one of the most prevalent issues, follows the introduction of e-commerce system along the supply chain is the ability to establish dynamic and flexible structures for buyer-supplier relationships and on-line trust that deterministically drive both parties towards strategic partnerships and cooperation. The past study on e-commerce, buyer-supplier relation and cyber security shows that because of cost based differences between traditional markets (such as retail stores) and electronic markets both from buyer and supplier prospective, there is shift towards greater electronic market utilization for transactional intermediaries and interactive service providers (Ba, 2001).

Cyber Security is a binding force in most buyer- supplier transaction (Ba, 2001). It is especially critical when two situational forces are present in a transaction: uncertainty and asymmetric product information. Many researchers proposed that cyber security is essential for developing trust and for understanding interpersonal behavior and economic exchanges (Hirsch, 1978). Trust is perceived as a state of readiness for unguarded interaction with some-one or thing. (Tuay, 1994).

Three cyber security models are Review system, Certified third party system and Community system.

Review and Monitoring System (RMS)

The rationale behind the Review and Monitoring System is due to the fact that the reputation of an on-line participant is a signal of one's past trading behavior. A bad reputation (i.e. low feed back rating) will discourage others from conducting future transactions with the participant. Ratings (thus reputation) are based on on-line identities which are often not more than a e-mail address. Currently auction sites do not provide strong authentication. Consequently, a person with bad rating can easily acquire a new e-mail address and re-register with no trace of the earlier bad reputation. A person who has developed a very bad feed back rating at one site can go to another transaction site as a new user and cheat again. Both situations result due to the lack of strong authentication of on-line identities.

Certified Third Party System (CTS)

Certified Third Party System, an extra legal mechanism, model authenticates the identity of trading agents by issuing digital certificates. They also disseminate information about agent's behaviors. Digital certificate issued by a CTS serves not only as authentication of certificate holder, but also a reputation indicator. If a certificate holder is reported to have cheated in the market, the CTS will investigate the case and ask the cheater to pay a fine. This model provides the extra protection that the on-line market participants can not change their identities easily and their reputation history is tied to a fixed identity that will follow them no matter which on-line market they choose to participant in. CTS is not a legal institution that could enforce rules, thus paying fines adjudicated by the CTS is voluntary. If a cheater pays the fine, he will keep his digital certificate and others will treat him as an honest agent in the future. This model suffers a drawback when a player adopts a fly-by-night strategy and takes the profit without ever coming back to the market, the reputation left behind does not matter any more. Even when people do engage in repeated transaction, each party has a finite life time. At the last transaction, cheating can always happen and cheating partly does not bear the consequence of being punished by others. On-line agents are concerned about the privacy and anonymity issue in the on-line world.

Community Integrated System (CIS)

Communities play a strong role in impersonal market exchange. Community social structure enforce economic agents to condition their actions on one's social affiliations, therefore supporting inter-community, impersonal market exchange. The participantofcommunityresponsibility system have strong commitment to the community. They are linked by common interests and / or values. On-line communities involve sociability and sense of belonging as important ends in themselves. Placeless nature of on-line community interactions facilities long term contact without the loss of relationships that often accompanies residential mobility. On-line communities have been formed to serve various purposes, such as providing emotional support, socializing with others, sharing information on commonly interested tasks. Salient features of the community integrated system (Ba, 2001) are :

- Agents can trade with each other across communities at community level,
- Agents who want to be perceived as trust worthy and want the protection of the community structure from being cheated by others can join a community that has good reputation. There will be multiple on-line communities on the market, each with its own reputation standing,
- Each community aims to maximize the sum of the life time utilities of its constituting members. This mechanism is a transference-based trust promoting mechanism- when a community is trust worthy, the design of the community structure ensures that the members of the community can be trusted as well.
- When two agents from two different communities trade with each other, the transaction would take place as if the two communities were trading with each other . The game would therefore turn into an infinitely repeated game- it is reasonable to assume that although individual members of a community have a finite time period for trading, the community as a whole will carry an infinitely, replacing old members.
- In the community structure, agents identities are only known to their community. To agents outside of their own community, only their community membership is known. Thus, transaction can still remain impersonal, allowing agents to preserve their anonymity to a large extent. In a particular transaction, if transacting agents were members from several communities, exchange would be impersonal up to one's community label. The communities serve as a trusted part that others can trust.

Keywords: Cyber Security, trust, e-commerce, supply chain

References

- Agarwal A., Shankar R., (2003),"On-line Trust Building in E-enabled Supply Chain, Supply Chain Management: An International Journal, (MCB Press, U.K.), (2003), Vol. 8 No. 4, pp.324-334.
- Hirsch F., (1978), " Social Limits to Growth", Harvard University Press, Cambridge, MA.
- Sulin Ba, (2001), "Establishing online trust through a community responsibility system", Decision support system, Vol.-31, no. 3, pp. 323-336.
- Tuay D.C., (1994), " A Construct of Trust", PhD dissertation, University of Texas, TX.

Dr. Ashish Agarwal has been working as Associate Professor Mechanical Engineering at School of Engineering & Technology Indira Gandhi National Open University New Delhi India since 1993. Before joining IGNOU he was lecturer in Motilal Nehru Regional Engineering College Allahabad (Motilal Nehru National Institute of Technology Allahabad). He has earned his PhD from IIT Delhi in the area of Supply Chain Management. His papers have been published in International and National Journals. He has published his research papers in European Journal of Operational Research, Industrial Marketing Management, Supply Chain Management: An International Journal, Work Study, International Journal of Management Science and Engineering Management, Journal of Manufacturing Technology Management, International Journal Intelligent Enterprise, Production & Manufacturing Research, International Journal of Advanced Operations Management, Competitiveness Review, International Journal of Productivity and Performance Management, Productivity, Industrial Engineering Journal and Global Journal of Enterprise Information System. He is reviewer in International and National Journals. He has supervised nine PhD students in the area of Operations Management. He is at present supervising five PhD students. He is life member of Indian Society for Technical Education and Indian Institutions of Industrial Engineering.

ashisha@ignou.ac.in