Statement of Research

Sunil Hazari
sunil@sunilhazari.com

My interdisciplinary background has shaped primary research interests in electronic commerce security, web usability, and networking/telecommunications. My research interests are more applied than purely theoretical, and utilize quantitative as well as qualitative methodologies.

Using the web, organizations have successfully leveraged information systems in their business strategies, products, and services. During the past few years, electronic commerce had emerged as a new model of doing business. Following initial hype, e-commerce services are now supplementing traditional business models by making available real-time data to customers, suppliers, and distributors. A company's web site is the primary interface through which a customer interacts. Failure to provide information to meet customers transaction needs in a organized and secure environment could create loss of customer confidence and lost sales. **Web usability** therefore is a critical component of business operations. While empirically tested models are needed to study system infrastructure that supports transactions as well as buyer behavior, my research has used action research for determining web usability of ecommerce sites. The body of knowledge in e-commerce area and web usability has increased in recent years, and action research is most appropriate for problem diagnosis, reflective learning, and action intervention in this area. The bottom line in understanding web usability principles for e-commerce sites is to rely on underlying theory and existing models of information systems such as Technology Acceptance Model (Davis, 1999), applied to web infrastructure. There is a strong need for research in this area especially by applying theoretical models to practitioner situations.

Since a large portion of corporate data travels across the Internet, **Information Security** is of critical concern to companies. An enterprise security strategy is needed that goes beyond application of technology to solve problems to also include people and policies. The human element is the weakest chain in maintaining digital security. Technology acceptance models such as Rogers'(1995) innovation diffusion theory, and reasoned action and planned behavior (Mathieson, 1991; Ajzen, 1985) models have been studied widely by Information Systems researchers in terms of human factors and IT adoption. Since these models and theories have also been researched in context of Internet technologies and electronic commerce applications (Gefen & Straub, 2000), it is reasonable to extrapolate that these theories can be applied to security applications in terms of user acceptance.

Information security awareness research has been mostly descriptive and has not explored the possibilities offered by motivation/behavioral theories or related theory of planned behavior and the technology acceptance model specifically in the information security domain. I have recently completed an

empirical study, “Perceptions of security professionals' requirements in personal firewall software” in which the behavioral aspects of information security are addressed. Information security is usually considered a technical discipline with much attention being focused on topics such as hacking, break-ins, and encryption. Security products such as anti-virus programs and personal firewall software are now available for end- users to install on their desktops to protect against threats endemic to networked computers. The behavioral aspects related to maintaining enterprise security has received little attention from researchers and practitioners. Using Q-sort analysis, this study investigated issues affecting selection and diffusion of personal firewall software in organizations. Technical information on firewalls was also provided for IT professionals. Implications of these results to IT managers, vendors of security software and researchers in information security area are discussed in the study.

Networking issues also play a part in supporting new technology applications. As an example, new generation of XML application firewalls are being designed to protect against vulnerabilities of web services that may demand higher bandwidth to be most effective. Networking professionals need to have in place strategies to manage mission critical applications that run on corporate Intranets and Extranets. This task is made difficult due to lack of standards and interoperability issues. I am also conducting applied research in other areas such as Enterprise Application Integration, Wireless Security, Web Services, and Enterprise Portals, focusing on electronic commerce and digital security.

References:

Ajzen, I. (1985), “From Intentions to actions: A theory of planned behavior”, in Kuhl, J. and Beckmann, J. (Eds.), Action Control: From Cognition to Behavior, Springer-Verlag, Berlin, pp. 11-39.

Davis, F.D. (1989), “Perceived usefulness, perceived ease of use, and user acceptance of information technology”. MIS Quarterly, Vol. 13, No. 3, pp. 319-340.

Gefen, D. & Straub, D (2000), “The relative importance of perceived ease of use in IS adoption: A study of e-commerce adoption”. Journal of Association for Information Systems, Vol. 1, No. 8. Available (JAIS) http://jais.aisnet.org/articles/default.asp?vol=1&art=8

Mathieson, K. (1991), “Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior”. Information Systems Research Vol. 2, No. 3, pp. 173-191.

Rogers, E.M. (1995), Diffusion of Innovations (4th ed). Free Press, New York.

[Note: Details on research presentations and papers are available from my web site http://www.sunilhazari.com/education]