I-WAYS, Digest of Electronic Commerce Policy and Regulation 28 (2005) 70
IOS Press

Editorial

Reduce Cyber Security Vulnerabilities by Stronger Controls On Government Information Systems

It has taken some time, almost three years since 9/11, for authorities in the US and other countries to fully grasp, analyze and begin to design strategies to cope with threats to "critical infrastructure" and information systems in particular. The US has established a Cabinet level Department of Homeland Security to consolidate and raise priorities to rapidly meet cyber security risks. Europe, Japan and Australia also are making assessments of threats and weaknesses but none have launched similar ambitious and expensive programs to thwart vulnerabilities. Today every organization is dependent on data networks to function – there are almost no "back-up" physical information systems anymore.

While the focus of this I-Ways is government data systems, E-Commerce cannot operate unless interlinked networks both private and public are functioning smoothly. The recommended security controls of the National Institute of Standards and Engineering (NIST) while addressed to government agencies, "may also be used by non-government organizations on a voluntary basis," NIST states. The ultimate objective, NIST concludes, "is to conduct the day-to-day operations or the organization and to accomplish its stated mission providing adequate security, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information."

Raising levels of cyber security carries a considerably different meaning to many people, because it presupposes a threat of harm to vital national systems. While the focus on the President's IT Advisory Committee is directed to "critical infrastructure such as power grids, air traffic control systems, financial systems and military and intelligence systems," the report makes strong linkages to the "growing dependence on these infrastructures on IT infrastructure means that the former cannot be secure if the latter is not." Living in a wired world means that far distances from the US do not significantly reduce a company's or individual's exposure to these threats and risks.

G. Russell Pipe

ISSN 1084-4678/05/$17.00