"Self-Defense and Common Sense in Cyberspace"

Review of Daniel S. Janal's Book

Risky Business: Protect Your Business from Being Stalked, Conned, or Blackmailed on the Web (John Wiley & Sons, Inc. 1998; $US 27.95)

Reviewed by Walter A. Effross

Associate Professor, Washington College of Law, American University, and Chair, Subcommittee on Electronic Commerce, American Bar Association

(This review represents the author's personal opinion only, and not the official opinion of the American Bar Association or any of its Sections, Committees, or Subcommittees.)

E-mail: effross@wcl.american.edu

When I was in law school, a student group invited Dr. Ruth Westheimer to campus to give a speech and conduct a question-and-answer session. What struck me most about the event was not any particular nugget of information (although I still remember some of those) but the atmosphere that Dr. Ruth created: one in which everyone could discuss without embarrassment both the pleasurable and the dangerous aspects of activities that could be approached extremely casually but also could involve serious health and emotional risks.

In some respects, Daniel Janal, an Internet marketing consultant, has in Risky Business adapted this approach to the increasingly-popular pasttime of going on-line. Not that there's a lot of humor here: in his first chapter, entitled, "Cyberspace Is a Scary Place," Janal clarifies that "This book is meant to scare you but in a positive way. I hope to motivate, or alarm, you to take action to protect yourself and your organization." Indeed, accounts of true-life cybercontroversies punctuate each of the subsequent chapters. However, in his own way Janal demystifies many concerns that new and experienced users of the Internet may have, and reassures them that, with certain precautions, they can reduce their vulnerability during this form of interaction. Moreover, he provides at the end of many chapters a list of Web sites containing further relevant resources.

Like Dr. Ruth, Janal offers dozens of concrete suggestions to protect his readers in their various (though virtual) encounters. And, as with Dr. Ruth's audiences, some of the information will probably appear obvious to those with experience and/or common sense: for example, the author counsels against giving out a home telephone number on-line or posting revealing messages in a newsgroup, and recommends that before meeting a "cyberpal" face-to-face the reader call that person (presumably, if the on-line friend has also read Risky Business, at his or her office or a pay phone) "to verify information, age, and sex" and "[s]elect a public place such as a restaurant or shopping mall" to meet.

Yet I would be the first to give Janal's book to a friend or relative who was just going on- line. He provides many useful lists of tips that might not be obvious, particularly to someone caught up in an unusual cyber-situation: for example, "Eight Tips for Protecting Yourself If You Are Being Stalked" includes an array of escalating responses, from telling the stalker to stop, to leaving the chat room, to contacting the forum administrators and the police. Not everyone would automatically "[k]eep track of the chats, copies of e-mail, and other evidence that you can present" to the authorities. In addition, like Dr. Ruth, Janal devotes much of his discussion to making readers aware of, and thus more able to prevent, various hazards in his case, such problems as identity theft or being duped by an impersonator.

Risky Business, though, should not be dismissed as a newbie's guide to "Everything That You Wanted To Know About Cyberspace But Were Afraid to Ask." The more experienced reader will appreciate Janal's discussion of ways in which a consumer or business can prevent commercial fraud, software piracy, and password theft.. Most useful to the corporate user of the Internet will be Janal's analysis of the need for and parameters of company policies on Web use. The author helpfully includes a sample Employee Internet Usage Policy recommended by the Software Publishers Association, as well as a sample Corporate Policy for Internet Use contributed by a forum host on CompuServe. Also studded with practical tips are discussions of e-mail etiquette, evidentiary issues concerning computer-based records, fighting spam, protecting your business's intellectual property (including a chapter devoted to the purchasing and misappropriation of domain names), and how to gather "competitive intelligence" by perusing the sites and on-line postings of others.

In fact, many corporate users of the Internet may find the book's entire purchase price justified by Janal's discussion of an emerging but rarely-analyzed topic: how a Web site can be used to instigate or defuse a public relations crisis. Risky Business examines several real-life examples and proposed ways to counter an "attack site" set up by "disgruntled employees, upset customers, and even well-meaning citizens who are alerting their friends to what they think are abuses performed by your company." Janal also suggests how a company may deal with malicious rumors, or even "spoofs" (such as the widely-reported "news" that Microsoft was acquiring the Roman Catholic Church), that are being spread through the Internet, and devotes a chapter to enunciating guidelines for both corporate management and potential investors to prevent online stock manipulation.

Top that, Dr. Ruth.