Security Journal 2005, 18 (2), 75–76

Beyond Fear: Thinking Sensibly about Security in an Uncertain World

by Bruce Schneier

New York, NY: Springer (2003) ISBN 0387026 20 7
(295 pages, $25.00)

Reviewed by Robert J. Stokes

In *Beyond Fear*, Bruce Schneier offers an interesting take on post-9/11 security practices. Schneier, the author of a web resource for the security-minded (at *http:www.schneier.com*), borrows from a career of observations in the security field in formulating his ideas. A main theme of the book is that security measures have unintended consequences and involve economic trade-offs. Schneier's other contribution here is that large players in the security risk assessment process—be they government agencies or large providers of security services and technological systems—cause distortions that lead to inefficiencies in the market. Thus, many security measures and public policies turn out to be largely misguided because they undermine the economic calculus of countless personal risk assessments made every day by citizens and groups. That is, in the name of security enhancements for the masses, collective policies pursued at the level of larger systems actually lead to a less discerning and less able security consumer.

The book is organized into three parts. The first section lays out the author's main theme: security is gained through a series of individual, consumer behavioral choices that seek to weigh risks and alternatives that maximize outcomes. In his first chapter, Schneier offers a five-step process to determining whether a security measure is worth the trades-offs implicit in all security-related decisions. He uses this process as an analytic device thoughout the book to assess a variety of hypothetical, but realistic, risk types. The five steps include: the type of asset; the type of risk; the risk reduction strategy; additional risk exposures caused by a security measure; trade-offs required by the chosen security solution (these being economic or civic, to name two). Here, Schneier expands the concept of the typical risk assessment process (ie the traditional probability, criticality and vulnerability matrix) by injecting the law of unintended consequences. That is, for every security measure, even the most logical and rational response to a specific threat will result in other exposures and risks, while also requiring trade-offs. The author astutely points out that these potential threats are usually outside of one's risk assessment model. That is, the analyst cannot rationally conjure such threats with any analytic rigor, let alone what the risk ratios and cost estimates for such threats might be.

The second section contains insights into how security works. This section is nothing new to students of the field: it assumes a highly adaptable, reasoning perpetrator, while asserting the importance of integrated systems that rely on both technology and human diligence. He offers insights into security issues—ranging from airport security: 'searching kids and grandmas actually improves airport security, but arming pilots does not'; to elections: 'replacing paper ballots with computerized voting machines is a horrendously bad idea'; to credit card purchases: just as safe to use on the net as at a store, if not more so—while firmly rejecting the security efficacy of a national ID card as easily counterfeited, as well as reducing the effectiveness of human intuition into behavioral deviation of suspects.

The book's third section deals with the 'game of security'. In his penultimate chapter, entitled 'Negotiating for Security', Schneier restates a point made throughout the book: security decisions are clouded by the specific agenda of security 'players'. So airport security gets determined by the interests of the largest and most influential actor involved (in the US, the FAA), regardless of whether the system in question makes sense outside of the specific considerations of the agency. Most analysts in policy studies would not see this point as remotely novel. Instead, they would sum it up with the most ubiquitous word to explain variation in satisficed policy outcomes: politics.

Overall, Schneier's work is firmly nested in the language of neo-classical economic theory, with the notion that the free market is the most efficient and effective decision-making mechanism in matters of equity markets, widget production, or here, security. With this free market bias, it is no wonder that Schneier believes that recent government efforts at collective security distort market information regarding risk, while injecting a further distorting element—fear—into the daily lives of people. Schneier's work is thus firmly couched in two phenomena that have garnered much scholarly attention. The first appears in the literature related to criminology and social psychology with regard to the conflicting role of fear in warping rational processes related to decision-making. The second, nested in the broad field of economics—more specifically, economic psychology—looks at the irrationalities in market decisions (made here by consumers of security) caused by psychological triggers. More broadly, Schneier's work points (without citation or reference) to the practical theories developed in criminology over the past 20 years by Felson, Clarke and Taylor among others. That being said, Schneier is not an academic, and cannot be completely faulted for mirroring work already done in the fields of situational crime prevention and economic psychology.

As far as the writing is concerned, Schneier is an obvious adherent of the practice of having as many eyes on your work before publication as possible; to this end, he lists 100-odd people who had some input into the writing of this book. In this case, however, too many cooks did not spoil the broth, as I found this one of the better reads in the ever-expanding field (both in terms of raw numbers and the variability of their quality) of security publications.

Robert J. Stokes
L. Douglas Wilder School of Government and Public Policy
Virginia Commonwealth University