Beyond Fear Into Reason

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Bruce Schneier has been one of my heroes for many years, not least because of the clarity of his thought and the crispness of his writing. Readers of this column have seen references in the past to his free monthly Crypto-Gram newsletter in the past and I hope that you have subscribed to that always-worthwhile publication.

In 2000, Schneier published a ground-breaking primer for non-nerds called _Secrets & Lies_ in which he confronted many misunderstandings and outright myths about security in the digital realm. In 2003, he continued his educational efforts with _Beyond Fear_, a superb analysis of the basis of rational thought about security in the wider world – not just computers and networks.

Schneier is so clear that even his chapter titles stimulate thought:

Part One: Sensible Security
1. All Security Involves Trade-offs
2. Security Trade-offs Are Subjective
3. Security Trade-offs Depend on Power and Agenda

Part Two: How Security Works
4. Systems and How They Fail
5. Knowing the Attackers
6. Attackers Never Change Their Tunes, Just Their Instruments
7. Technology Creates Security Imbalances
8. Security Is a Weakest-Link Problem
9. Britteness Makes for Bad Security
10. Security Revolves Around People
11. Detection Works Where Prevention Fails
12. Detection Is Useless Without Response
13. Identification, Authentication And Authorization
14. All Countermeasures Have Some Value, But No Countermeasure Is Perfect
15. Fighting Terrorism

Part Three: The Game of Security
16. Negotiating for Security
17. Security Demystified

One of the most important conceptual frameworks articulated by Schneier are five steps for analyzing any proposed security measure, whether for computers, networks or social systems (p. 14):

Step 1: What assets are you trying to protect?
Step 2: What are the risks to those assets?
Step 3: How well does the security solution mitigate those risks?
Step 4: What other risks does the security solution cause?  
Step 5: What trade-offs does the security solution require?  

Over and over, Schneier shows that sloppy thinking leads to poor choices of security solutions that can make security worse instead of better. His analyses include such diverse issues as protecting credit-card numbers used for Internet shopping (p. 84); security screening at airports (also p. 84); increased secrecy in the U.S. after 9/11 (p. 130); airline-passenger profiling (p. 164); home burglar alarms (p. 178); national ID cards (p. 204); military actions against terrorism (p. 231) and other interesting topics.

I would love to send policy makers in our nation’s government copies of this book, but I greatly fear that most would not read it. You, on the other hand, as intelligent readers of this column, will get a great deal out of reading Schneier’s book – and THEN you can try to explain its main points to your congress critters and to any policy wonks you happen to know.

Good luck – for all of us.

* * *

Crypto-Gram newsletter <http://www.counterpane.com/crypto-gram.html>


* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.