Joel Dubin, CISSP has just sent me the update of his useful guide to computer security, _The Little Black Book of Computer Security_. In October 2005, I published a review of the first edition and I refer readers to that review for a sense of the first edition’s qualities. The book so much I ordered it for the assigned readings in one of the seminars in the MSIA program.

The book has grown from 150 pages to 207 pages (38%), but its price has changed from $19.95 to $25.95 (30%) – seems fair. It still fits in a (large) pocket. More important, the content has significant changes. Dubin begins with an insightful commentary in his introduction (quoting exactly):

> IT security has broadened dramatically. Its issues have expanded from the technology arena into the business arena. In other words, IT security no longer consists solely of the IT department working to lock down networks. It has moved into the boardroom as business leaders grapple with the business impacts of potential data breaches. Those leaders are now concerned with complying with legal regulations, protecting the privacy and identity of their customers, and keeping their brands intact if data breaches _do_ occur. Consequently, IT security has developed into the more wide-ranging field of information security.

Furthermore, as the network perimeter has dissolved, the old-fashioned firewall has evolved. Hackers have become more sophisticated, bypassing firewalls and other network controls by inserting malicious code into Web sites. Today, even innocent sites can serve as repositories of dangerous malware that can defeat the toughest network defenses. In other words, the threat has shifted from the network to the application. The new paradigm therefore entails not only safeguarding hardware and networks but also protecting data wherever it happens to be – a Web site, a database, or anywhere in between.

There are three new chapters. Quoting from correspondence with Mr Dubin,

- Chapter 19 on compliance and working with auditors, since this has become such a big part of many IT security professional's lives.
- Chapter 20 on security awareness training, since this has become part of compliance with tips on the bare bones minimum of what should go into an security training program.
- Chapter 21 is a simple explanation of encryption, which IT security pros can use to distill this complex topic for the business folks.

Other improvements in the guide include updated and expanded recommendations on

- Endpoint security and network access control and mobile device security
- Application security, including vulnerability and pen testing, with an emphasis on the new security threats
• from the Web and Web 2.0 technologies
• Wireless security
• Privacy and identity theft and regulations related to privacy
• How to use full-disk encryption

Finally, the author has updated the appendices in the back with fresh links for helpful security Web sites, bulletins and tools.

So is there anything I don’t like in the book?

It’s not a question of liking or disliking (well, except for using “data” as a singular word). I disagree with a few of the recommendations; for example, on page 54, Mr Dubin writes, “Lock out an account after three failed logon attempts” and then explains that users should have to call the IT group to reset their password. “This practice offers the easiest defense against a brute force attack.” Well, no: it offers an attacker a trivial way of executing a denial-of-service attack on every user account for which (s)he knows the userID. It also raises the cost of such an attack by orders of magnitude because of the amount of time wasted by both users and the Help Desk. Pretty well the same level of defense against brute-force attacks can be achieved by inserting a modest delay in accessibility of the account – say, a few minutes. That’s enough to put brute-force attackers out of business simply because of the length of time it takes to test the keyspace (OK, half the keyspace on average). Put in a simple routine to alert the security group that a userID is being attacked and you have the start of either an investigation or a reasonable defense.

But one should not dismiss a handbook because one disagrees with a few recommendations: it’s not supposed to be a list of recommendations to be followed without thought. It’s useful even if there are things you don’t agree with. And that’s certainly the case with the Second Edition of The Little Black Book of Computer Security.

And so today I just placed our order for a batch of these handy little guides for our graduate students.

[NOTE: Since so many book reviewers seem to delight in tearing apart the books they review and heaping abuse on their authors, readers may be suspicious of my enthusiasm. For the record, then, I have no relationship whatever with Joel Dubin other than liking his book. I think it’s very nice that he stuck some of my comments on the front cover of the new edition, but that has nothing to do with the content of my review and I have received no financial or other benefits whatever in return for that enthusiasm.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 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.