As Malcolm X once pointed out, Western society is so thoroughly permeated with racism that “black” is almost always a negative word. We speak of a “black list” and a “black mark;” most pinko-gray people (E.M. Forster’s preferred description of “white” folks) think that there’s nothing peculiar about “denigrating” or “blackening” someone’s reputation. Books with “black” in the title have usually been focused on criminal hacking or virus writing. I’ve had a decade-long argument with Mark Ludwig, for example, about his habit of publishing books that provide full details of virus code (e.g., _The Little Black Book of Computer Viruses_ and _The Giant Black Book of Computer Viruses_). On the other hand, “black book” can also be used in a positive sense; one dictionary defines it as a book full of telephone numbers. By extension, “black book” has come to mean a concise technical manual that can be carried about easily – what was once called a “vade mecum” (Latin for “come with me”).

I recently received a review copy of a useful security _vade mecum_ called _The Little Black Book of Computer Security_ (ISBN 1-583-04120-6) by Joel Dubin, CISSP that is published by 29th Street Press, a division of Penton Technology Media (AMAZON link [http://tinyurl.com/cgwwa](http://tinyurl.com/cgwwa)). In 150 pages, Mr Dubin presents a neat package of valuable reminders about significant security best practices and security assessment questions. The jacket bio says that the author “works as an independent computer-security consultant who is based out of Chicago. He has received multiple certifications from Sun Microsystems in the Java programming language as well as MBA and BA degrees from Northwestern University.”

This little book is ideal for widespread distribution to employees throughout an organization as part of a security-awareness campaign. The 7”x4.5” book is just the right size to slip into a pocket, purse, or computer bag. It has 19 chapters and five appendices with topics such as

- Assessing Your System
- Writing Your Security Policy
- Taking Care of Physical Security
- Managing Human Resources
- Putting Software Access Controls in Place

and so on.

Flipping pretty much at random into the book to pick an example, I opened it at Chapter 9, “Protecting your system against viruses, Trojans, and worms.” Mr Dubin starts with a concise definition of malware, provides a simple and clear table distinguishing among viruses, Trojans and worms, and summarizes the main sources of infection with a paragraph each. Here’s an example – the section on Web sites: “Malicious Web sites and their pop-ups can contain malware in two forms: tiny blank images and HTML tags. The former are invisible on the page but contain spyware, for example, in embedded HTML code. The latter can use your browser to download malicious code from the attacker’s Web site to your computer.” Now, readers with
extensive technical knowledge may want to quibble with the details, but for educational purposes, this is an adequate introduction to some of the problems of malicious code on Web sites.

The malware chapter continues with clear, numbered recommendations for defenses. The numbering makes it easy for technical support or security personnel to refer to specific recommendations or steps when discussing the procedures with users. There are also occasional notes flagged with a special symbol to mark extra information; e.g., Chapter 9 includes this tidbit: “Generally, a firewall cannot protect a computer from virus attacks because most viruses operate at the application level (especially when they slip through as e-mail attachments). Similarly, trojans are like mini-application servers that open ports on the victim’s computer and then go to town. An application-level firewall or a proxy that strips e-mail attachments can provide some protection. Firewalls will be discussed in more detail in Chapter 11, “Defending Your Network Perimeter.”

This booklet is useful and inexpensive ($19.95 for single copies and less for bulk orders by arrangement with the publisher – contact Jan Hazen at mailto:jhazen@pentontech.com ). I am ordering several hundred copies for my graduate students as examples of useful awareness materials and to provide review and reminders of practical recommendations for first-level information security measures.

Good job, Mr Dubin.

[Disclaimer: I have no financial interest in this venture and Norwich University has received no special discounts as a result of this review.]

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management 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 © 2005 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.