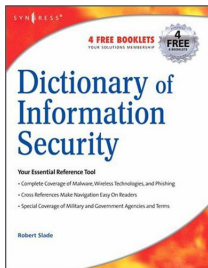


## BOOK REVIEW 1

### WAR OF THE WORDS

David Harley

Independent author, UK



**Title:** Dictionary of Information Security

**Author:** Robert Slade

**Publisher:** Syngress

**ISBN:** 1-59749-115-2

**Cover Price:** \$29.95

Although Robert Slade's *Dictionary of Information Security* has only just made it to the printed page, it replaces his online security glossary, which for

several years resided at <http://victoria.tc.ca/techrev/secgloss.htm>. (The glossary has now been removed, but the page remains as a home for errata and updates to the printed dictionary.)

Slade's credentials in the security field are impressive, as a writer, book reviewer and instructor. In fact, this book derives in part from his professional involvement with (ISC)<sup>2</sup>, whose Common Body of Knowledge (CBK) is the basis for the CISSP qualification. The web version of Slade's glossary was a popular free resource for CISSP candidates, and will no doubt be missed.

Glossary compilation in this area is a complex and frustrating task. The security field is knee-deep in obscure, inconsistently used jargon. Even worse, individuals and groups go to extravagant lengths to invent their own terminology, ignoring perfectly serviceable 'not invented here' usage. It is not easy to produce definitions that are reasonably short, clear, accurate, and which don't rely on an assumed knowledge of esoteric terms and concepts. Both the CBK and Slade's dictionary attempt to address these problems by introducing a consistent source of baseline definitions.

#### TARGET AUDIENCE

The cover notes and the author's preface suggest that the book is appropriate for security professionals and specialists, CISSP and other certification candidates, students of computer science or computer security, system and network administrators, and managers with security responsibilities.

#### STRUCTURE

The book contains no fewer than five forewords, each by a well-known and long-established name in information security and assurance: Fred Cohen, Jack Holleran, Peter G. Neumann, Hal Tipton and Dr Eugene Spafford. In addition, there are short biographies of the author and foreword

contributors, publisher and author acknowledgements, plus a preface and an 'Introduction to InfosecSpeak' by the author.

Does a relatively short dictionary actually need five forewords? Perhaps not. However, the fact that so many acknowledged experts are willing to contribute says something about the author's standing in the field.

The book is quite short, given the breadth of its subject matter: the main body runs to 222 pages, including the appendices. However, according to the author, the book's objective is to cover 'all the basic jargon of security, without bloating itself with every minor variation on a terminological theme'. The Preface and References sections include pointers to a range of alternative resources for those who need more detail in specific areas. (It's always a pleasure to read a security book whose author doesn't assume that no reader will ever need to consult another information resource.)

Unsurprisingly, the book follows a straightforward dictionary format (though there are no notes on pronunciation or, in general, etymology): a section for each letter of the alphabet, plus sections for symbols and numbers, which happen to contain one item each – '\*-property' and '3DES'. There are, however, two appendices.

- Appendix A is a references section: rather than attempting to supply references for each entry, the author simply lists (with a short evaluative description) a number of communications-related dictionaries, glossaries and encyclopaedias.
- Appendix B is an extract ('The Lagos Creeper Box') from the fictional story *Stealing the Network: How to Own a Continent* (also published by Syngress). It is included on the grounds that the security risks to which the book refers could qualify it for a place in a security awareness program. This extract reminded me a little of the *Net Force* Tom Clancy franchise offshoot, albeit with added techie cred. Not without interest, but it sits oddly in the context of a security glossary.

Though much of Slade's previous writing is malware-related, this book is by no means virus-heavy. In fact, the malware content, albeit accurate as far as it goes, seems oddly dated. A number of older malware examples get a mention, but very little more recent than Nimda or Hybris. I agree that it would be counterproductive to try to include the name of every virus that the reader may have heard about. However, it seems odd to mention more-or-less extinct malware such as Michelangelo or Jerusalem, but to omit more recent high-profile malware such as Sobig and MyDoom. Similarly, there is no specific reference to botnets, specific bots (though zombies get a mention), or to major network worms like Slammer and Blaster. It would improve the book to include a few more recent, high-impact

examples, or even to restrict the number of examples and include only those with a really high profile. There are definitions of phishing (and even of spear phishing), pharming and identity theft, but not of money-laundering or mules (or even of puddle phishing). However, the author points out that this is very much a work ‘in progress’, anticipating ongoing updates and further editions for years to come. He even includes a pointer to a mailing list for anyone wanting to help with the project, so it seems likely that such anomalies will be dealt with in due course.

## DOES THE BOOK KEEP ITS PROMISES?

The *Dictionary of Information Security* is well written, clear, and while no two security experts are going to agree on every aspect of every definition, accurate. The tone is informal and commendably anti-jargonist. Some of the entries are more flippant than others (check out Ohnosecond, the Ninety-Ninety Rule and Wannabe), but I found that rather refreshing.

A reasonably computer-literate general reader might find it a more consistent and accurate guide than most web resources, without being overly technical. It should find a ready market among computer science and information security students, and even more so among security certification candidates. It would be particularly useful to CISSP candidates to supplement the ‘Official (ISC)2 Guide to the CISSP Exam’.

Security professionals needing a definition outside their own speciality may find it a good starting point, and the seasoned generalist might find it useful sometimes as a reliable memory jogger. However, I see it as being more useful to those unfortunate souls who find systems security administration or management thrust upon them suddenly, and who are struggling to keep their nostrils above the water line.

Most of all, it will be appreciated as a source of dependable baseline definitions by anyone who has learned to mistrust the astonishing volumes of misinformation that appear when summoned by *Google* searches on security terms.

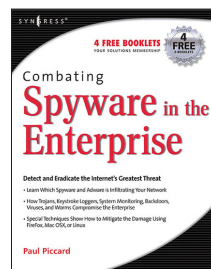
The editing and proofing is generally to a high standard, though there are one or two loose ends: for instance, the definition of ItW refers to the WildList, but there is no definition of the WildList or the WildList Organization. EICAR gets a mention, but CARO does not. URLs are not generally included, which makes sense: it’s much less painful to maintain a resource that is impervious to the whims of webmasters. However, definitions of items such as BS7799 and ITIL might benefit from specific information on where to find reliable further information.

Slade’s book fills a pretty wide gap in the market, and is highly recommended.

## BOOK REVIEW 2

### I SPY

David Harley  
Independent author, UK



**Title:** Combating Spyware in the Enterprise  
**Author:** Baskin, Bradley, Caruso, Faircloth, James, Piccard, & Schiller  
**Publisher:** Syngress  
**ISBN:** 1-59749-064-4  
**Cover Price:** \$49.95

According to the cover blurb, this book is essential reading for ‘anyone responsible for the security of an enterprise’s network’. It contains

some useful and interesting general material, but does it live up to its claim?

## CONTENT

The book begins with chapters entitled ‘An overview of spyware’ and ‘The transformation of spyware’, both written by Tony Bradley. The first defines spyware, malware, adware, parasiteware (browser hijackers), phishing and botnets. The definitions will not add much to the knowledge of readers of *Virus Bulletin*, but are uncontentious and clearly written, with examples of specific programs and the body text of several phishing emails.

A short description of how botnets work is followed by very short descriptions of a handful of bots. The separate section on malware seems a little odd, given that most of us would probably consider most of the programs described here to be malware. The second chapter is largely historical, describing the origins and evolution of spyware through targeted marketing, spam and cookies, and adware. A section on spyware and criminal activity introduces some slightly different or additional definitions (identity theft, ransomware) and is followed by a short US-centric section on anti-spyware legislation. While these chapters don’t really address the enterprise context, they do provide a reasonable introduction to the topic of spyware.

Chapter three, ‘Spyware and the enterprise network’ by Jeremy Faircloth, begins with brief descriptions of a selection of hardware and software keystroke loggers, including *Sony*’s DRM fiasco. A consideration of ‘spyware/backdoor combinations’ and ‘encapsulated trojans’ is followed by a couple of pages on fake removal tools. The content related to the enterprise network is sparse and very generalized (e.g. ‘Always use standard security practices...’).

Chapter four, ‘Real SPYware – crime, economic espionage, and espionage’ by Craig S. Schiller, picks up the pace

somewhat. The first few pages consist mostly of historical overviews of the criminal use of (loosely speaking) spyware and commercial and governmental espionage, and seem to suggest that profit-driven malware represents a shift from a previously ethical model of virus writing. (I'd love to hear that debate at a VB conference!) A more detailed overview of phishing is followed by a long section on botnet functionality, detection and countermeasures. There's some useful introductory-to-intermediate material here, though many enterprises will not have the resources or incentive to follow up on this material to the same level of detail.

Chapters five and six, 'Solutions for the end user' and 'Forensic detection and removal', were written by Brian Baskin. Home users might find the former quite useful. However, this chapter is surprisingly long for a book which supposedly focuses on the enterprise. Only one keylogger detection utility is mentioned, but a number of common toolbar utilities are named, as well as a few commercial solutions. However, these are considered from an individual PC user's viewpoint, rather than in terms of enterprise management. Of the mainstream security vendors with products or services that include spyware management functionality, only *McAfee AntiSpyware* gets a mention. Given the number of mainstream AV vendors with a foot in that door, this is disquieting.

Chapter six is useful, but inaccurately named. It considers detection of spyware by tools like *Hijack This*, examination of the Registry, processes, the hosts file and so on, but pays no significant attention to the presentation of evidence in a court of law, so in what sense is it forensic? Its juxtaposition of detection and removal techniques without even mentioning the need to preserve a chain of evidence is, if anything, anti-forensic. The final section of the chapter summarizes a handful of enterprise-level removal tools and services, but not in any great depth.

Chapter seven, 'Dealing with spyware in a non-Microsoft world' by Ken Caruso, addresses the general issues of spyware and security on the *Linux* and Macintosh OS X platforms. Caruso mentions the existence of *Linux* spyware and rootkits, but the only *Linux* threats he describes (briefly) are *Staoq* and *Slapper*, and the only preventative measures mentioned are the use of unprivileged accounts and (in the summary section) *tripwire* (which isn't described). Pre-OS X malware isn't mentioned at all, but *Leap* and *Inqtana* are described briefly. The only Mac security product mentioned is *MacScan*.

Chapter 8, 'The frugal engineer's guide to spyware prevention' by Paul Piccard, contains reasonable basic material, mostly on application security. It seems unhelpful to mention free versions of commercial AV here: very few enterprises will meet the licensing criteria to allow them to

use those versions. The descriptions of *Microsoft's WSUS* and *MBSA* and the sections on securing email, *Windows* and so on could be the starting point for a useful set of checklists, but leave a lot of ground uncovered.

The appendix, written by Lance James, contains some competent material on mule-driving, telephony, and malware trends. It does fit quite well with the heavy emphasis on phishing in other chapters, but doesn't really tie the subject in with the main theme of the book.

## DOES THE BOOK KEEP ITS PROMISES?

This is a disappointing book. It contains useful general information on spyware and a number of related areas (especially phishing), but it isn't the definitive work on spyware. While there are certainly links between phishing attacks and spyware, the terms are not so interchangeable as to justify the volume of non-technical phishing material. This would have been more defensible had there been more emphasis on corporate governance and non-technical countermeasures. I would expect a book centred on spyware in the enterprise to address topics around governance issues like policy, end-user education, top management buy-in, compliance issues and accountability, as well as purely technical matters. Even at the technical level, the book is much better on attacks than on countermeasures.

The book largely overlooks the strong presence of mainstream AV vendors in this space. More surprisingly, even the open source programs widely used as a supplement (or, more contentiously, as a substitute) for commercial AV are not considered. This is a pity: a responsible, well-informed discussion of when it is appropriate to use open source and freeware would have been a real service to the enterprise community. AV aside, the range of commercial solutions that *is* considered is astonishingly narrow.

This emphasis on in-house technical measures and cost-cutting misses an essential point about enterprise security. Many enterprises prefer to spend serious money on commercial products and services rather than rely on internal expertise and applications that aren't contractually supported. Why would they do that? Because the principle of transferring risk and accountability is, if properly managed, a viable security model. A book on enterprise security that doesn't give due weight to this model undermines its own credibility.

This book contains useful reading matter for non-specialists, and many system administrators and managers might benefit from it. However, as a guide to corporate handling of spyware, it is weak and even misleading.