

Book Review: The New School of Information Security

Hardcover: 288 pages

Publisher: Addison-Wesley Professional; 1 edition (April 5, 2008)

Language: English

ISBN-10: 0321502787

Review written by Don Franke, 10 Apr 2009

While much of may read as a primer to an information security professional, there were some very interesting nuggets that could be found throughout this book, such as:

- "How people are motivated to behave can be as important as, or often more important than, how the system, is designed to behave." The impact emotions have on making the right decisions when it comes to evaluating risk. An example of this is the observation that the number of car accidents far exceeds the number of terrorist attacks, yet the latter garners a disproportionately larger amount of spending.
- Some interesting anecdotes on Risk Compensation, such as a study that shows that anti-lock brakes have done little to reduce the number of car accidents because people tend to drive more recklessly, assuming ABS will protect them. Conversely, in cities where safety measures such as crosswalks and speed bumps have been removed, the number of accidents has actually decreased, since people are forced to drive more carefully.
- Comments on how users don't appreciate the impact their infected PC has on the world. They could be unsuspectingly feeding a botnet that is attacking their own power grid.

Chapter 1: Observing the World and Asking Why

An introduction to the need for good information security (with some good crime examples and statistics), the different types of attack, and the growing threat.

Chapter 2: The Security Industry

Discusses the "prisoner's dilemma" and mild game theory. Also some interesting thoughts on our perception of a threat and the actual threat, and some of the psychological motivators behind how security is sold.

Chapter 3: On Evidence

The challenge of gathering objective data from evidence, surveys and statistics, and how the trade press may skew the facts depending on the business situation.

Chapter 4: The Rise of the Security Breach

Companies are very reluctant to admit mistakes (or breaches) but are being forced to more and more for the sake of public welfare, thanks in large part to California Senate Bill 1386 leading the way.

Chapter 5: Amateurs Study Cryptography, Professional Study Economics

Can't professionals also study cryptography? Discusses the cost and poor application implementation and low adoption rate, how typical users personally deal with information security, and the pros and cons of DRM.

Chapter 6: Spending

The various factors that go into how companies determine how much to spend on security, including fiscal and psychological ones, and the emerging reasons to spend on information security.

Chapter 7: Life in the New School

Training users does not help users behave more securely, perhaps due to the psychology of risk compensation. This chapter also makes some points about the need to disclose and share information security for the benefit of everyone.

Chapter 8: A Call to Action

A review of the previous seven chapters, which are recommendations to approach information security in a new way, with a fresh perspective, and to make it your goal to help society by sharing and teaching what you know.

There are also fifty pages of end notes and a 15-page bibliography, so there is plenty of items for your continued research. The book seems well researched and inspired by someone who really cares about the subject. There was some slight bias in the book also, unfortunately, such as fee-based security organizations are cliques and elitist. But overall, I thought it was a well-paced and informative book, and should be picked up by seasoned security professionals and just those entering the field.