College of Business book Review by Dan Clapper

Title: "Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity"

Authors: [Byron Acohido](http://www.amazon.com/exec/obidos/search-handle-url/ref=ntt_athr_dp_sr_1?%5Fencoding=UTF8&sort=relevancerank&search-type=ss&index=books&field-author=Byron%20Acohido) and [Jon Swartz](http://www.amazon.com/exec/obidos/search-handle-url/ref=ntt_athr_dp_sr_2?%5Fencoding=UTF8&sort=relevancerank&search-type=ss&index=books&field-author=Jon%20Swartz)

Publisher: Union Square Press

Length: 304 pages

Price: $19.95 (paperback)

Reading time: 10 hours

Reading rating: 8 (1 = very difficult; 10 = very easy)

Overall rating: 4 (1 = average; 4 = outstanding)

“Zero Day Threat” is a guided tour through the dark world of data theft, credit card fraud, identity theft and the individuals and entities that facilitate and commit those crimes.

The book presents the case that blaming the increase in cyber crime solely on criminals is a much too narrow view. Instead each chapter in the book has three sections -- Eploiters, Enablers and Expediters -- each of which covers groups that commit, enable and facilitate data theft and fraud.

The authors define Exploiters as the drug addicts, scam artists and crime lords who carry out the gritty aspects of data theft and financial fraud. These sections tell the story of a group of meth addicts in Edmonton, Canada, who stay up for days at a time working on scams to steal data and turn it into cash. We also get to follow the Edmonton detectives who work to catch and prosecute them.

It is a fascinating set of stories as the authors follow the arc of the group from their rise to criminal notoriety -- at their peak they were bringing in many thousands of dollars a day in cash -- to their subsequent fall and incarceration. The book balances a clear eyed look at the crime they commit with an often sympathetic look at the drug addiction that drives them and their efforts to break free from it. At its best it reads like very good crime fiction, but in the process you gain a unique understanding of the motivations and schemes of the criminals who want to profit from stealing your confidential information.

The Enablers sections focus on both the history and current practices of credit card companies, banks, credit bureaus and data brokers. These are the entities that have created the fast, easy to use credit card economy we are accustomed to. Unfortunately, despite amazing technological achievements, easy and convenient does not also mean safe and secure. These sections highlight how security has often been sacrificed for speed and ease of use and consequently enabled criminals to commit financial crimes. While not as compelling as the Exploiter sections, it provides an interesting and disturbing look at the dark side of our credit card economy.

Finally, the third section “Expediter”, details the role of technologists – on both sides of the law – in finding or fixing technology holes that can be used by criminals. While there were a number of interesting and informative stories in these sections, they seemed less cohesive and engaging than the other two sections.

Despite the obvious importance of information security to business organizations, it is all too easy for non-technical folks to get lost in a maze of security terminology. Once lost, it’s very difficult to move from a general sense of “We need to improve our security” to the sort of meaningful conversations with IT staff and consultants that actually make that happen.

This book won’t dramatically improve your understanding of the terminology, but it will provide a much clearer understanding of the sorts of people out there who are constantly looking for (and finding) new ways to steal data and profit from it. I think most readers will find that understanding both chilling and motivating.

It may terrify you at times, but “Zero Day Threat” should make it very clear that the problem of data theft and fraud is not going away anytime soon and now is the time to start working on preventing your organization from becoming a victim.

Dan Clapper is an associate professor of computer information systems in the College of Business at Western Carolina University. He teaches secure application development for both the desktop and Web environments. For previously reviewed books, visit our web site at www.wcu.edu/cob/.