The review process of each book is not easy. The same was in this case; at the beginning I found the contents of this book to be less adequate than I expected. This was due to the fact that I am a computer engineer that is aware of the problem of computer systems security and rather interested in technical aspects of cybercrime. The omnipresence of IT solutions in contemporary businesses needs to be noted especially when we realize that these systems are a part of physical company resources and also store non-physical resources – information, which can be (and usually is) many times more valuable than storage systems and any other resources of a company. There can be many sources of cybercrime actions: ranging from malicious jokes, to revenge, to real criminal activity capable of inflicting heavy financial losses. The awareness of these sources is very important to system administrators, developers and integrators, who are responsible for system maintenance duties. In this book the reader can find a lot of interesting and informative examples, which occurred in the last decade and are real case studies of different cybercrime activities against a wide range of business.

The book consists of four main parts. The first shows the global nature of cybercrime and cyber security. For me this part of the book is the most controversial. In the text of Chapter I I have found a lot of simplifications and statements which were too general. For example, the author states that there is a large concentration of cybercriminal activity in Eastern Europe, but we are not told which countries actually comprise that area. Among the countries, which the author mentions as part of Eastern Europe are Russia, Ukraine and, surprisingly, Romania, which is actually a Central European country. This part should have been more consistent in that regard. Within the very same Chapter we can also read that Eastern Europe is not the only source of cybercrime, but this is a problem present in many other countries, even including “poor” North Korea – therefore, cybercrime cannot be attributed to any part of the world, because it’s a multinational issue. The author also tends to often refer to the term ‘system’, but he does not provide any definition of systems or how he understands that notion. Also, the sentence (at the end of Section 1.8.3.2) about “right wing nationalistic tendencies within the USA and Europe” is included, even though the phenomenon has nothing to do with the scope of the book. And since within this book we find numerous examples of countries with leftist governments, which are also sources of cybercrime.

The second part (Chapters 2-4) is focused on the relationships between cybercrime and three types of companies: startups (very important especially in IT), small and medium-sized (SME) companies.

The third one (Chapters 5-8) covers the problem of cyber security when companies try to use different strategies for their development: mergers, acquisitions, joint ventures, partnerships, subsidiaries, franchising, intellectual property protection, licensing and outsourcing. Each Chapter is constructed in almost the same manner, presenting business insights on strategy, inner and external threats, possible ways to mitigate the existing risk of cybercrime.

The last part presents conclusions with a summary.

This book contains plenty of case studies, examples, interesting presentations which provide very well researched supplementary materials to each chapter. And this convinces us that this book is, in general, very valuable, interesting and without any doubt can be recommended to anyone, who is interested in the big picture of the problems of cybercrime, especially in business. Let us note, that it

takes time to properly recognize the criminal threat involved with new technologies, and put forth the necessary measures to combat them; for example, firearms were known to mankind for more than 800 years and today we fully understand just how dangerous they can be in the wrong hands. However, computers and IT were not nearly as common 20 years ago as they are now and we only begin to understand how they can be a threat. There is a lot of work to be done in this field and the book does a great job explaining those issues. The contents of the book may disappoint professional computer engineers because it does not cover the technical issues in great detail, but it does provide the necessary language connections between business and IT and cyber security communities.

I have also found typos in the text, for example: Window XP instead of Windows XP. Another shortcoming was the small number of figures which end up explaining rather straightforward relationships, which can actually be understood without these figures. There is no statistical data about cybercrime, breaches, financial losses etc. presented in tables or figures. But these small flaws by no means discredit the amount of good work poured into this book by S. L. Moskowitz.

Dominik Strzałka