

Preface

Information and communication technologies (ICT) have over several decades brought significant benefits to enterprises, individuals, and society as a whole. This is clearly evident when considering the wide and profound impact of the Internet in a great many parts of our daily lives. The Internet, and more broadly cyberspace, has become a cornerstone for a broad range of services and activities that today we take for granted. Due to cyberspace and its underlying infrastructure, people and organizations have access to more and better services than ever before. This is the case within several domains of society, including banking and finance, communication, entertainment, health, power supply, social interactions, transportation, trade, and social participation. As a result, our daily lives, fundamental rights, economies, and social security depend on ICT working seamlessly.

At the same time, cyberspace has introduced, and continues to introduce, numerous new threats and vulnerabilities. Stakeholders are exposed to cybersecurity incidents of many different kinds and degrees of severity. These include information theft, disruption of services, privacy and identity abuse, fraud, espionage, and sabotage. At a larger scale, societies are threatened by possible attacks on critical infrastructures via cyberspace, as well as the potential for cyber-terrorism and even cyber-warfare. In addition to the many possibilities for cyber-crime and malicious attacks come all the accidental and other non-malicious threats that may lead to cybersecurity incidents. In fact, the ubiquity of cyberspace has brought societies to a point where a very large number of the risks that we traditionally have been exposed to in the physical world today arise in cyberspace and have become cyber-risks.

In order to ensure a satisfactory level of cybersecurity, stakeholders need to understand the nature of cyber-risk and what distinguishes cyber-risk from other kinds of risk, and they need adequate methods and techniques for cyber-risk management. Our main objective with this book is to give a short introduction to risk management, focusing on cybersecurity and cyber-risk assessment. We introduce the reader to the underlying terminology, we present and explain the processes of cyber-risk management, and we provide guidance and hands-on examples on how to conduct cyber-risk assessment in practice. We moreover address many of the typical challenges that risk assessors face, and we give advice on how to tackle them.

There are many different techniques, tools, modeling languages, and documentation formats that are available to support cyber-risk assessment. This book is oblivious to any such specific approach; while we have based the contents on established standards and industry best practices, we present the risk assessment process and the examples in a format that can be instantiated by any specific approach that complies with the ISO 31000 risk management standard. The intended target audience is practitioners, as well as graduate and undergraduate students, in particular within the ICT domain. We also aim to provide lecturers with teaching material on the fundamentals of cyber-risk management and the basic principles and techniques of cyber-risk assessment. We moreover believe that the book illuminates and clarifies many aspects and underlying concepts of the domain of cybersecurity. The book can therefore be useful also for researchers and standardization bodies that have activities related to cybersecurity.

Our own knowledge about and experience of cybersecurity and cyber-risk management, and therefore also the contents of this book, largely stem from academic research and empirical studies that we have conducted jointly with colleagues and with collaborators from industry. We express our acknowledgments to all of those who in different ways have helped out in the work on this book.

We owe many thanks to our close colleagues Gencer Erdogan, Yan Li, Aida Omerovic, and Fredrik Seehusen for their many and valuable comments and suggestions on several parts of this book. We are very grateful to Kristian Beckers, Karin Bernsmed, Aslak Wegner Eide, Marika Lüders, and Ragnhild Kobro Runde for reviewing the manuscript and providing good and helpful feedback.

Prior to and during the work on this book we have benefited greatly from collaboration with people from academia and industry on several research projects. These include Jürgen Großmann, Maritta Heisel, Fabio Martinelli, Wolter Pieters, Alexander Pretschner, Christian W. Probst, and Aristotelis Tzafalias.

Some of the research activities that the work on this book has benefited from have partly been funded by the Research Council of Norway, in particular through the projects Diamonds and AGRA. Relevant research activities have also been funded by the European Commission, in particular through the projects RASEN and NES-SOS, but also through CONCERTO.

Oslo, Norway
July 2015

*Atle Refsdal
Bjørnar Solhaug
Ketil Stølen*

Cyber-Risk Management

Refsdal, A.; Solhaug, B.; Stolen, K.

2015, XI, 145 p. 32 illus., Softcover

ISBN: 978-3-319-23569-1