1. Record Nr. UNINA9910299201803321

Autore	Refsdal Atle
Titolo	Cyber-Risk Management / / by Atle Refsdal, Bjørnar Solhaug, Ketil Stølen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-23570-2
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (146 p.)
Collana	SpringerBriefs in Computer Science, , 2191-5768
Disciplina	331.7610058
Soggetti	Computer security Quality control Reliability Industrial safety Management information systems Computer science Mathematical statistics Management Industrial management Systems and Data Security Quality Control, Reliability, Safety and Risk Management of Computing and Information Systems Probability and Statistics in Computer Science Innovation/Technology Management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	1 Introduction -- Part I Conceptual Introduction -- 2 Risk Management -- 3 Cyber-systems -- 4 Cybersecurity -- 5 Cyber-risk Management -- Part II Cyber-risk Assessment Exemplified -- 6 Context Establishment -- 7 Risk Identification -- 8 Risk Analysis -- 9 Risk Evaluation -- 10 Risk Treatment -- Part III Known Challenges and How to Address Them in Practice -- 11 Which Measure of Risk Level to Use? - 12 What Scales Are Best Suited Under What Conditions?- 13 How to

Deal with Uncertainty?- 14 High-consequence Risk with Low Likelihood -- 15 Conclusion -- Glossary -- References -- Index.

Sommario/riassunto

This book provides a brief and general introduction to cybersecurity and cyber-risk assessment. Not limited to a specific approach or technique, its focus is highly pragmatic and is based on established international standards (including ISO 31000) as well as industrial best practices. It explains how cyber-risk assessment should be conducted, which techniques should be used when, what the typical challenges and problems are, and how they should be addressed. The content is divided into three parts. First, part I provides a conceptual introduction to the topic of risk management in general and to cybersecurity and cyber-risk management in particular. Next, part II presents the main stages of cyber-risk assessment from context establishment to risk treatment and acceptance, each illustrated by a running example. Finally, part III details four important challenges and how to reasonably deal with them in practice: risk measurement, risk scales, uncertainty, and low-frequency risks with high consequence. The target audience is mainly practitioners and students who are interested in the fundamentals and basic principles and techniques of security risk assessment, as well as lecturers seeking teaching material. The book provides an overview of the cyber-risk assessment process, the tasks involved, and how to complete them in practice.