1. Record Nr. UNINA9910392740103321

Autore	Corradini Isabella
Titolo	Building a Cybersecurity Culture in Organizations : How to Bridge the Gap Between People and Digital Technology / / by Isabella Corradini
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-43999-2
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (144 pages)
Collana	Studies in Systems, Decision and Control, , 2198-4182 ; ; 284
Disciplina	005.8
Soggetti	Quality control Reliability Industrial safety Psychology, Industrial Employee health promotion Computer crimes Quality Control, Reliability, Safety and Risk Industrial and Organizational Psychology Employee Health and Wellbeing Cybercrime
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- The scenario -- Security: Human nature and behavior -- Redefining the approach to cybersecurity -- Building Cybersecurity Culture -- Communication is not optional -- Developing cybersecurity awareness -- Training methods -- Conclusions.
Sommario/riassunto	This book offers a practice-oriented guide to developing an effective cybersecurity culture in organizations. It provides a psychosocial perspective on common cyberthreats affecting organizations, and presents practical solutions for leveraging employees' attitudes and behaviours in order to improve security. Cybersecurity, as well as the solutions used to achieve it, has largely been associated with technologies. In contrast, this book argues that cybersecurity begins with improving the connections between people and digital

technologies. By presenting a comprehensive analysis of the current cybersecurity landscape, the author discusses, based on literature and her personal experience, human weaknesses in relation to security and the advantages of pursuing a holistic approach to cybersecurity, and suggests how to develop cybersecurity culture in practice. Organizations can improve their cyber resilience by adequately training their staff. Accordingly, the book also describes a set of training methods and tools. Further, ongoing education programmes and effective communication within organizations are considered, showing that they can become key drivers for successful cybersecurity awareness initiatives. When properly trained and actively involved, human beings can become the true first line of defence for every organization. .