Foreword

Companies can gain a decisive market advantage through information and communication technology (ICT). Clouds providing central computing services, mobile access, networking, and machine-to-machine communication are the basis for processing high volumes of business-relevant data, and are at the core of new business concepts and greater performance in existing ones. ICT is used in almost all businesses to automate business processes and increase speed and quality. This "digitalization" has two major consequences. Firstly, enterprises, authorities and even consumers are much more dependent on ICT. The value of the data being processed is going up and up, while adversaries, including hostile hackers, organized crime and industrial spies, are unfortunately highly motivated and active as well. Secondly, ICT is now a ubiquitous part of everyday life. This increases the attack surfaces that adversaries can, and do, exploit.

ICT infrastructures and applications are attacked effectively and both enterprises and consumers suffer considerable losses. Though managers and officials know that they have to invest in protecting their ICT, many stakeholders still consider appropriate security to be inconvenient and expensive. At the end of the day, it is about "which party must do what."

Technology, business models and trends in the economy lead to an immense centralization of computing power mastered by large-scale IT production. Cost pressure and other customer demands in turn reinforce the need to deliver ICT services in an industrialized manner. User organizations are increasingly using ICT services from ICT service providers instead of producing these services in-house themselves. They demand reliability and seek trustworthy, dependable suppliers offering secure ICT services: A sufficient level of security is an essential and intrinsic element for the successful digitalization of industries, administration, and our society as a whole. The word "intrinsic" is important here. Users demand reliable ICT services and want to concentrate on making the most of them in their business, requiring the security to be integrated "almost invisibly" and "with ease." Nonetheless, it is up to the user to demand and reimburse the appropriate protection of ICT. In fact, every party in the supply chain must make their contribution to security, since the chain is only as strong as its weakest link. However, this cannot be taken as a given but must be arranged systematically.

This 2nd, updated and extended edition of the book presents methods and measures for dealing with information security in today's IT industry that were developed and proven in our corporation, with our customers, and with suppliers and partners. This book is intended to help the reader to implement security measures throughout a complex ICT delivery infrastructure in organizations, pro-

cesses and technology, from design to service management, while taking into consideration effectiveness as regards customer requirements, and efficiency relating to costs. The book should also help user organizations to understand the security aspects of ICT provision and to select the correct provider and the correct services in terms of information security. In this way, the workable architecture presented here aims to find a balance between buyers and providers: requirements and deliverables must correspond. *Secure ICT Service Provisioning for Cloud, Mobile and Beyond* is of utmost concern to both parties.

Reinhard Clemens

Member of the Board of Management at Deutsche Telekom

CEO of T-Systems

Preface

The task of making ICT services secure is important and mission critical for any ICT service provider paid to deliver secure ICT services for cloud, mobile and beyond. Such providers are challenged to turn requirements into real material security in a way that is verifiable for customers. This puts leading ICT service providers in a very specific and (does it come as a surprise?) very complicated and truly complex situation. The reasons are easy to see. The provider is facing an almost unmanageable multitude of different sets of requirements that are all to be met by its single ICT service delivery infrastructure. Moreover, the provider must produce the ICT services efficiently, which in turn requires as much standardizing and harmonizing as possible.

In the past, security was managed in "customer silos." However, security requirements have increased dramatically in number, coverage and depth in recent years. At the same time, the customers of the ICT service provider demand a significant cost reduction while retaining or even enhancing performance and flexibility, and at the same time being provided with more security transparency and assurance.

This situation was the starting point some years ago when a number of security managers from T-Systems sat down together with the authors of this book to discuss precisely the issues described above. We decided to take a big step forward. We invented the idea of "industrializing security" or adapting ICT security to an industrialized ICT provision method. That was the birth of ESARIS, the subject of this book. That approach, and its realization, have proven to be very successful. We decided to publish large parts of the work in order to contribute to *Secure ICT Service Provisioning for Cloud, Mobile and Beyond*. At the same time, we wanted to encourage customers and a wider audience to discuss the concepts and to adopt useful ideas. In this way, the industry should be able to progress in balancing the requirements of user organizations and the measures that are provided by ICT service providers.

With the 1st edition of this book, major concepts of ESARIS were published at the beginning of 2013. Since then, our corporation has gained more experience in applying the new methods and measures in practice, and has also developed new ones. Four years later, this 2nd, updated and extended edition presents an even more complete set of concepts, methods and measures. It provides deeper insight, improved rationales and more background information. T-Systems' Board of Management decided to implement ESARIS in our corporation and initiated a longer-lasting program for introducing it in all subsidiaries around the world. This book reports on real-world experience from this Transformation program. Moreover, it considers feedback from our customers as well as experience gained from using

ESARIS while managing numerous big and complex deals throughout their IT outsourcing phases, including Sales, Manage the Deal, Transition and Transformation, and Operations. Recently, T-Systems initiated the foundation of the Zero Outage Industry Standard association in which technology leaders are aiming to provide the highest quality and security against outages of IT infrastructure. The work in this association and other examples show that ESARIS closed a substantial gap in the literature about information security. ESARIS "takes operational requirements into account and focuses on user requirements, thus facing the reality in the market economy." It addresses efficiency, standardization and quality in the realm of security; and it helps to manage security in large-scale IT production characterized by a high degree of division of labor and specialization. I consider this book an essential contribution to the successful industrialization of ICT: Users require ICT services that are secure, at an affordable cost.

Heike Bayerl

Vice President of international Security, Compliance & Quality Management

T-Systems, IT Division

http://www.springer.com/978-3-658-16481-2

Secure ICT Service Provisioning for Cloud, Mobile and Beyond
ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers
von Faber, E.; Behnsen, W.
2017, XIV, 369 p. 159 illus. in color., Hardcover
ISBN: 978-3-658-16481-2