Chapter 1
An Analysis of Industry 4.0

ABSTRACT

Chapter 1 sets the scene by providing an overview of the Industry 4.0 concept that is conjoining a number of different technologies, with various levels of maturity, in order to provide an end-to-end capability. This case study is a good exemplar to tease out many pertinent socio-technical topics where the main contexts will be elaborated on throughout the remainder of the book. In short, a case is made that cyber security is first and foremost a human problem, but also highlights the importance of regulation, standards, and bodies to underpin cyber security. Examples of the opposing forces are covered here that together if unmitigated will contrive to undermine the cyber resilience of the 21st century.

INTRODUCTION

It has been more than 30 years since the public Internet was born. Society continues to transform towards an online-centric world. This utopia has been significantly tainted by the continually evolving threat landscape and the level of capability that potentially could gain unauthorized access to users' data. It is not just about the external attackers and targeted users, which in fact catch most of the press attention. It is the holistic cyber security considerations for the protection of computer-based systems that should be the preserve of many practitioners. Considerations range from software developers and programmers, system designers and solutions architects, system administrators, and system support managers (Bird & Curry, 2018). There is no better

DOI: 10.4018/978-1-7998-3979-8.ch001

protagonist to start this journey into the cyber security challenges of the 21st Century than Industry 4.0. Berting, Mills, & Wintersberger (1980) first coined the term Fourth Industrial Revolution in 1980, and it is now developing with such a technological trajectory (Swahb, 2016) that it has culminated in the coming together of various disparate technologies for a common purpose. This intersection brings an amalgamated risk from the ICT domain interfacing with Operational Technology (OT), OT interoperability with the Internet of Things (IoT), and the use of Artificial Intelligence (AI) to process big data sets. Both IoT and AI have been designated as being critical to the United Kingdom on the road to digital transformation that is engulfing the second decade of the new millennium (Violino, 2018).

BACKGROUND

Whilst it is not possible to cover every cyber security issue in one chapter, this case study will provide a compendium of general topical issues, some of which the author will explore further in this book. Many of the security principles covered here are pertinent to OT, IoT, and AI systems today because they have not only become increasingly interconnected, but most of them are also managed via ICT. This is a very large subject area that transcends private Local Area Networks (LAN), distributed wide-area networks across the Internet and Cloud Service Provider (CSP) infrastructure. Therefore, Industry 4.0 serves as a ideal paradigm to highlight the diversity of key cyber security challenges facing civilization. The remainder of the book then elaborates on many common themes and discusses how society should go about resolving them.

INDUSTRY 4.0

Information Communications Technology

Computing technology has progressed quickly from the First-Generation valve / vacuum tube-based computers to the Second Generation, which consisted of transistors, around the mid-20th century. The Third Generation consisted of integrated circuits and the Very Large-Scale Integration microprocessors of the Fourth Generation carried us forward into the 21st century (Fiegenbaum