Chapter 100
Embracing Cybersecurity Risk Management in the Industry of Medical Devices

Maria Lai-Ling Lam
AJ-Great Limited, China

Kei Wing Wong
Calvin College, USA

ABSTRACT

The promises of Industry 4.0 in the medical device industry needs to be built on sound cybersecurity infrastructures, polices, and practices. During 2011-2017, the authors interviewed many manufacturers of medical devices in China, Germany, Israel, Japan, Taiwan, and U.S. about their attitude towards cybersecurity. Many manufacturers are not committed to cybersecurity risk management because they pursue lower cost and shorter product life cycles; do not have sufficient knowledge of operating environments of hospitals; have defensive attitude toward vulnerability disclosure; and reap quick benefits from the low-trust level among stakeholders and unequal power between manufacturers and distributors. Only a few large U.S. manufacturers of medical devices have set up robust secure platforms and interoperable optimal standards which benefit the users. As cybersecurity is a shared responsibility, many small and medium-sized enterprises need to be empowered through the support of international organizations and local government policies.

INTRODUCTION

Industry 4.0, the fourth industry revolution, allows intelligent data gathering, data storage, data distribution, and real-time responses through many heterogeneous cyber-physical systems and internet of things [IoT] (General Electric, 2017; Siemens, 2016). Some promising examples of industry 4.0 in the medical device industry are robotics in health care, fitness apps, tele-medicine, smart home care, and real-time processing through data analytic and data mining. Industry 4.0 empowers but also disrupts the current

DOI: 10.4018/978-1-7998-8954-0.ch100

manufacturing sector of medical devices. Manufacturers not only can digitally manage the entire lifecycle of products and production processes through the IoT, cyber-physical systems, powerful sensors and big-data analytics, but also predict the maintenance of their smart products (Chiu et al., 2017; Loffler & Tschiesner, 2013; Sogeti, 2017). When an operating system and an information technology system are integrated in the manufacturing process, cyber security is an on-going significant challenge in the heterogeneous environments constructed by industry 4.0 (Woodside Capital Partners, 2017). The manufacturers must comprehend the complexity of managing cybersecurity of diverse devices and systems when new medical devices are added to the existing system of health care providers. They are called to design their new devices with the in-depth knowledge of the users' operation system and be open to any vulnerability report from the community (Food and Drug Administration [FDA], 2016; Fu, 2014; National Institute of Standards and Technology [NIST], 2017; Schwartz, 2016).

The promise of industry 4.0 in the medical device industry needs to be built on sound cybersecurity infrastructures, policies, and practices. Manufacturers must know how to design and implement a secure embedded system *that typically must provide multiple functions, security features, and real-time guarantees at a minimum cost* (Sadeghi et al., 2015). When they want to realize the benefits of industry 4.0, they must assure the cybersecurity of their own systems and also the systems that support the health care providers and other stakeholders. These manufacturers must monitor the performance of their smart products in the hand of health care providers and are willing to take predictive maintenance and the assessment of the vulnerability of the devices when they are installed in the system of health care providers (Kobes, 2014; Schwartz, 2016). Unfortunately, cyber security is not treated as the first priority in the design process of many manufacturers of medical devices (Cooper, 2016). The practice of industry 4.0 in the entire medical device industry also challenges our existing social and legal systems (Doehmann, 2016). Its impact may become greater in our existing embedded health care systems and networks which are not equipped with updated software.

Cybersecurity risk management is regarded as shared responsibility among stakeholders, including manufacturers, users, information technology vendors, and health care delivery organizations. Manufacturers are expected to have industry-self-regulations which monitor the cybersecurity of the entire smart product life-cycle process (FDA, 2016). The entire medical device ecology is described by a key representative of FDA as very complex, complicated, uncertain, intensive, diverse, and evolving rapidly (Schwartz, 2016). Many manufacturers of American medical devices are criticized for lagging behind other industries in terms of cybersecurity management and standard setting (Cooper, 2016). A recent survey of about 242 medical device manufacturers finds that even though these manufacturers, an average, spend approximately U.S. $4 million in the security of their devices, only 34% of respondents follow the FDA published Secure Development Life Cycle process for medical devices (Ponemon Institute, 2017). Many small and medium enterprises are expected to comply with FDA cybersecurity guidelines much less than those respondents. Why do many companies not comply with the FDA cybersecurity guidelines? Are FDA cybersecurity guidelines not effective?

A few global American manufacturers have developed their strategies toward 4.0 and tend to focus on the cybersecurity of their smart production process rather than the entire product life-cycle of the smart products (General Electric, 2017). They can easily ignore the fact that one medical device can still function but can be used to break down the users' operating system. For example, Class 1 products which are exempted from the FDA approval, can be the entry point of cyberattack (Wellington, 2014). As the authors see it, there are two essential research questions: (1) What factors led these manufactures not to invest in cybersecurity management? (2) Under what conditions will these manufacturers develop