International Journal of Cyber-Physical Systems
Volume 3 • Issue 1

Shared Cybersecurity Risk Management in the Industry of Medical Devices

Maria Lai-Ling Lam, Anderson University, Anderson, USA*
Kei-Wing Wong, Lord Aeck Sargent Planning and Design, Inc., USA

ABSTRACT

The cybersecurity capabilities of Class 1 medical devices must be seriously addressed when the industry moves toward Industry 4.0. Many U.S. 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 attitudes toward vulnerability disclosure, and reap quick benefits from the low-trust level among stakeholders and the 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 that can elevate the security practices of entire global supply chain of Class 1 devices. Many small and medium-sized enterprises inside and outside the U.S. need to be equipped to co-foster cybersecurity values with large manufacturers through the coordination between government and industry regulations and the support of international organizations and local government policies.

KEYWORDS

Cybersecurity Guidelines, Ecology of Medical Devices Industry, Food and Drug Administration, Government and Industry Regulations, Internet of Medical Things (IoMT), Interoperable Governance Mechanism

INTRODUCTION

The promises of having more patient-centric, accessible, and cost effective health care can only be realized through the well-governance of cybersecurity infrastructures, policies, and practices in the global supply chain of medical devices (Bartlett, Somauroo, Zerbi, 2021; Chiu et al., 2017; Deloitte Center for health solutions, 2018; Food and Drug Administration [FDA], 2016; Fu, 2014; General Electric, 2021; Loffler & Tschiesner, 2013; National Institute of Standards and Technology [NIST], 2017; The Economist, 2017; Schwartz, 2016; Siemens, 2020; Sogeti, 2017; Woodside Capital Partners, 2017). Cybersecurity risk management is regarded as a shared responsibility among stakeholders, including manufacturers, users, information technology vendors, and health care delivery organizations (Healthcare & Public Health Sector Coordinating Councils, 2019). Manufacturers are expected to respect industry-self-regulations which monitor the cybersecurity of the entire smart product life-cycle process (FDA, 2016). However, there is a gap between the expected behavior of U.S. medical devices manufacturers and their actual practices in designing and implementing a secure embedded system

DOI: 10.4018/IJCPS.2021010103 *Corresponding Author

(Cooper, 2016; Ponemon Institute, 2017). Medical devices manufacturers are expected by government regulators to 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, para.3). These manufacturers must monitor the performance of their smart products in the hand of health care providers, be willing to take predictive maintenance, and assess the vulnerability of the devices when they are installed in the system of health care providers (Kobes, 2014; Schwartz, 2016). Unfortunately, cybersecurity is not treated as the first-priority in the design process of many manufacturers of medical devices (Cooper, 2016) in the existing social and legal systems (Doehmann, 2016). Previous empirical studies found that many leading U.S. medical devices manufacturers do not want to pay for the cost of managing cybersecurity risk, and may attempt to shift the cost to small and medium distributors outside of the USA (Lam & Wong, 2018).

The few global medical devices manufacturers that have developed their strategies toward Industry 4.0 (i.e., the fourth industry revolution that is driven by the internet of medical things [IoMT], big data, artificial intelligence [AI], mobile applications, robotics, and advanced sensors) tend to focus on the cybersecurity of their smart production process rather than the entire product life-cycle of the smart products (General Electric, 2021; Siemens 2021). They can easily ignore the fact that one medical device can keep its function while being used to break down the users' operating system. For example, Class 1 products, which are exempted from FDA approval, can be an entry point of a cyberattack (Wellington, 2014). Given the stated problematics, the authors of this paper explore the social conditions for better cybersecurity risk management in entire global supply chain of Class I medical devices and recommend specific solutions and future research to enhance the cybersecurity capabilities of the entire global supply chain. Three essential research questions guide the study: (1) What factors lead these U.S. manufactures of medical devices not to invest in cybersecurity management? (2) Under what conditions will U.S. medical devices manufacturers develop their cybersecurity capabilities? (3) How can small and medium-sized enterprises outside of the U.S. (e.g., OEM) contribute to the cybersecurity risk management in an increasingly integrated global supply chain? This article proceeds with four sections. The first section describes the complexity of the medical device ecology and cybersecurity risk management; the second section describes the methodology. The third section answers the research questions. The fourth section proposes future research, and the fifth section concludes with contributions and recommendations.

THE INDUSTRY OF MEDICAL DEVICES AND CYBERSECURITY RISK MANAGEMENT

The medical device industry is highly regulated, concentrated, and diversified in terms of channel members' relationships. Thirty percent of multinational medical device firms control 70% of the global market share. The U.S. medical device market (i.e., $156 billion) accounts for 40% of the global market in 2017 and is expected to grow to $208 billion by 2023. U.S. export of medical devices exceeded $ 43 billion in 2018 (SelectUSA, 2021). There are more than 6500 medical device manufacturers in the U.S., and many of which are small and medium-sized enterprises. There are more than 500,000 medical devices in the industry. They are intrinsically diverse in their design, usage, implementation, and application. The industry is diversified and ranges from simple cotton to complicated implantable cardioverter defibrillators. The product life cycle of each device can be significantly different other medical device. The following section will review the definitions and classifications of medical devices, FDA cybersecurity risk management, and the opportunities and challenges of manufacturers in the cybersecurity risk management in Industry 4.0.

Definitions and Classifications of Medical Devices

World Health Organization [WHO] (2017) defines medical devices as "an article, instrument, apparatus or machine that is used in the prevention, diagnosis or treatment of illness or disease, or