RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 204 – 15 October 2019

Healthcare: A Critical Information Infrastructure

By Pauline C. Reich

SYNOPSIS

As we rely more and more on networked data and devices with the advent of the 5G networks, there are more Internet-connected devices entering the medical marketplace worldwide. What are the cybersecurity risks to the healthcare sector?

COMMENTARY

YEARS AGO, in the film "The Net", terrorists arranged to kill a diabetic patient by remotely changing the insulin dose in his IV drip. Today such attacks are possible in reality through remote access to network-connected health devices.

According to the 2019 Health Canada advisory, a cybersecurity vulnerability could allow an attacker to access the settings of some Medtronic insulin pumps and tamper with the amount of insulin delivered to the patient. We have also seen ransomware attacks against hospitals, and major hacks of health insurance and patient electronic health records in some countries, including Singapore.

Emerging Trend

According to a Zion Market Research report, the Asia-Pacific cybersecurity in healthcare market is projected to show a high growth rate in the years ahead. This rapid growth is also attributed to the presence of research and development centres of the medical device and pharmaceutical industry and several MNC headquarters. "These organisations are highly vulnerable to cyberattacks from malicious insiders, state and non-state agents, and external hackers," says the report.

According to the 2019 IBM Security and Ponemon *Cost of a Data Breach Report*, the highest industry average cost of a data breach found in their global survey was $6.45 million in the healthcare category.

A survey by Carbon Black entitled *Healthcare Cyber Heists in 2019* conducted with CISOs from the healthcare industry worldwide indicates that two thirds (66%) of the surveyed healthcare organisations had encountered attacks in which the primary motivation was destruction of data; and two thirds (66%) reported that their organisation was targeted by a ransomware attack.

Clearly the healthcare sector needs strong regulation and guidelines to help secure healthcare data and network-connected medical devices as elements of critical information infrastructure.

What is "Critical Information Infrastructure"?

There is no one definition of a Critical Information Infrastructure. Each country decides what its own critical sectors are. In Asia, only Singapore, Bangladesh, China, Japan, Malaysia, The Philippines, and Sri Lanka include public health and safety or medical and health services in their definitions.

Under Singapore's Cybersecurity Act of 2018, the Commissioner may "designate a computer or computer system as a critical information infrastructure … issue or approve one or more codes of practice or standards of performance for the regulation of the owners of critical information infrastructure with respect to measures to be taken by them to ensure the cybersecurity of the critical information infrastructure".

Singapore's Guidelines

Since network-connected medical devices are part of the critical information infrastructure, some of the standards, legislation and best practices applicable to their cybersecurity are as follows:

The Health Sciences Authority (HSA) reviews connected medical devices (wireless-enabled, Internet-connected and network connected) and specifies that medical device cybersecurity is a shared responsibility between stakeholders (i.e. the health care facilities, patients, providers, and the Product Owner of the medical devices).

The HAS also specifies that information to support the cybersecurity of these devices shall be provided. This will include, but is not limited to:

(i) Cybersecurity vulnerabilities and risk management approach for the device, including validation reports where necessary;

(ii) Cybersecurity controls measures;

(iii) On-going plans for surveillance, timely detection and management of the cybersecurity related threats during the useful life of the device, especially when a breach has been detected.

The Cybersecurity guidelines for healthcare institutions are published by the Singapore Standards Council. They provide guidelines for institutions on how to mitigate cybersecurity risks in the procurement of new connected medical devices, and day-to-day operations of existing connected medical devices.

International Standards

The ISO/IEC 80001-2-2 standard is a voluntary technical control standard for 'Application of risk management for IT-networks incorporating medical devices' and presents a unified and amalgamated approach to the safety of medical devices connected to IT networks.

USA – NIST

The National Institute of Standards and Technology, US Department of Commerce is a major source of standards used in the Information Security industry. In July 2018 it issued Special Publication 1-800-1, entitled Securing Electronic Health Records on Mobile Devices.

European Union

In May 2020, the EU will have a new Medical Device Regulation in effect.

More Collaboration Needed

The standards exist, but they must be applied and enforced. The safety of new and existing network-connected medical devices is of great concern to the medical community worldwide, but doctors cannot do it alone without the help of technologists and enforcement by regulators. Vigilant regulators like HSA and Health Canada are needed to help keep unsafe connected medical devices away from the market.

Industry is focused on profits; government agencies and medical institutions worldwide suffer from the shortage of trained and certified cybersecurity experts; and there are not enough university programmes in healthcare cybersecurity issues that incorporate law, policy, and medical issues. Greater collaboration across disciplines is needed, to ensure that patients do not die due to hacking of connected medical devices.

Pauline C. Reich is a Senior Fellow at the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.