sagentia

Holding medical devices hostage

As medical devices become increasingly connected, security is emerging as a major issue, prompting device companies and healthcare providers to take action. Risk mitigation is critical to prevent security breaches that would not only tarnish company reputation but also cripple the global medical connectivity industry.

From mobile apps to insulin pumps, medical devices are becoming smarter. Forecasts suggest that by 2020, Internet-connected healthcare products are expected to be worth an estimated $285 billion in economic value. However with the potential vulnerability to hackers and criminals this connectivity does come at a price.

Beyond the security of individual devices, hospitals may also find themselves vulnerable, as demonstrated in February 2016 when hackers held the internal computer system ransom of a hospital in Hollywood.

¬ Risk mitigation for connected devices

Medical device manufacturers and healthcare organisations are under mounting scrutiny to better secure and protect patient care equipment and systems from security threats. It became clear that medical devices are vulnerable to hacking, in 2015, following a government warning that an infusion pump could be modified remotely to deliver a fatal dose of medication. As medical devices make more and more use of wireless communication and Internet connectivity, it is not hard to imagine that without suitable countermeasures, more data breaches and even malicious attacks threatening the lives of patients could result.

A consistent approach to managing cyber security when developing devices is surely required.

While well-established risk management frameworks, (such as NIST 800-30) exist in conventional IT systems, it is widely recognised that little guidance is available for managing cyber security risks for medical devices.

¬ A new framework

On that subject, the Association for the Advancement of Medical Instrumentation (AAMI) took a welcome step forward in moving medical device manufacturers towards a coherent security risk management framework. The Association's report *TIR57:2016 Principles for medical device security – risk management* provides guidance for medical device manufacturers about how to manage the risks associated with security threats and the impact of these risks on data, confidentiality, integrity and device availability.

¬ A new way of thinking

The recommendation is that manufacturers establish a companion security risk management process alongside their existing ANSI/AAMI/ISO 14971-based safety risk management process. This should not be too cumbersome as Medical Manufacturers are already familiar with ISO 14971, however the approach taken to safety and security risk may need to differ. Safety risk involves evaluating the probability and severity of a hazard leading to harm. Security risk on the other hand assesses the likelihood that a threat will successfully exploit a device vulnerability, an event that could compromise system confidentiality, integrity, and/or availability.

Organizations should exercise caution when attempting to quantify the likelihood of a future adverse impact in purely traditional probabilistic terms. Instead, they should focus on the skills and motivations of an attacker, and whether the effort required to exploit a vulnerability is less than the perceived gain the attacker will achieve by compromising the system. As many a good Hollywood movie has told us over the years, this isn't necessarily as straightforward an evaluation as one might hope.