MediTechSafe

Whitepaper

NEED HOLISTIC APPROACH TO CYBERSECURITY OF MEDICAL DEVICES AND NETWORKS

Reinforcement from WannaCry attacks!

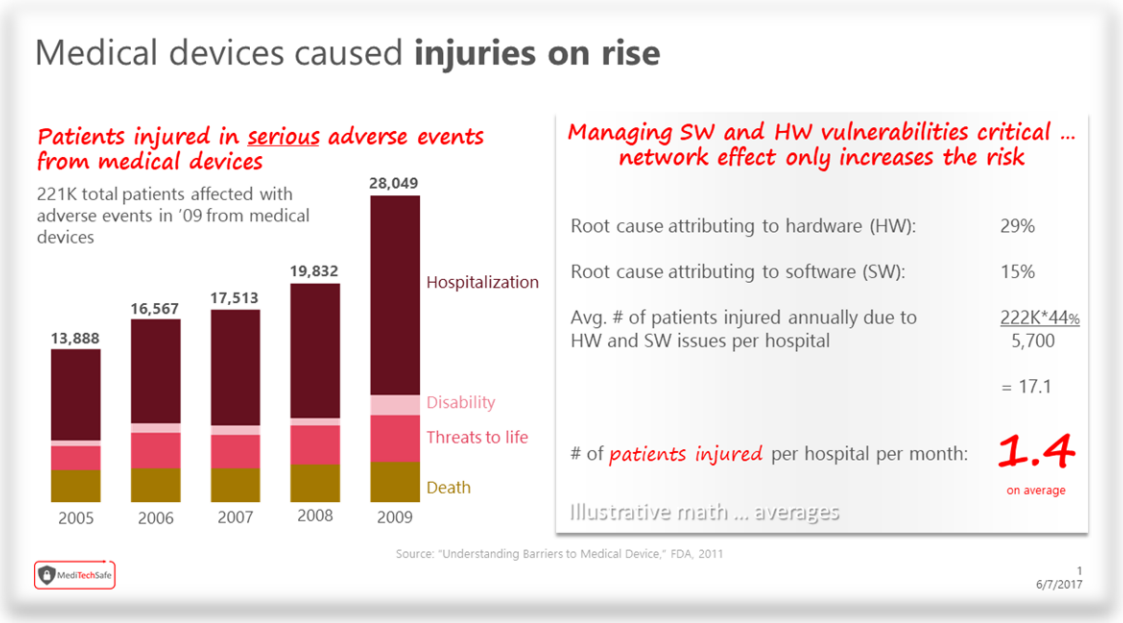
Need Holistic Approach to Cybersecurity of Medical Devices and Networks … reinforcement from WannaCry attacks!

The aftermath of WannaCry ransomware attacks have left many healthcare CIOs, CSOs and medical device manufacturers more concerned about **device security** than ever. The healthcare community, however, has been aware of potential cybersecurity related vulnerabilities and threats to their medical devices for some time now. In fact, many publications, experiments and actual events have tried to surface these risks:

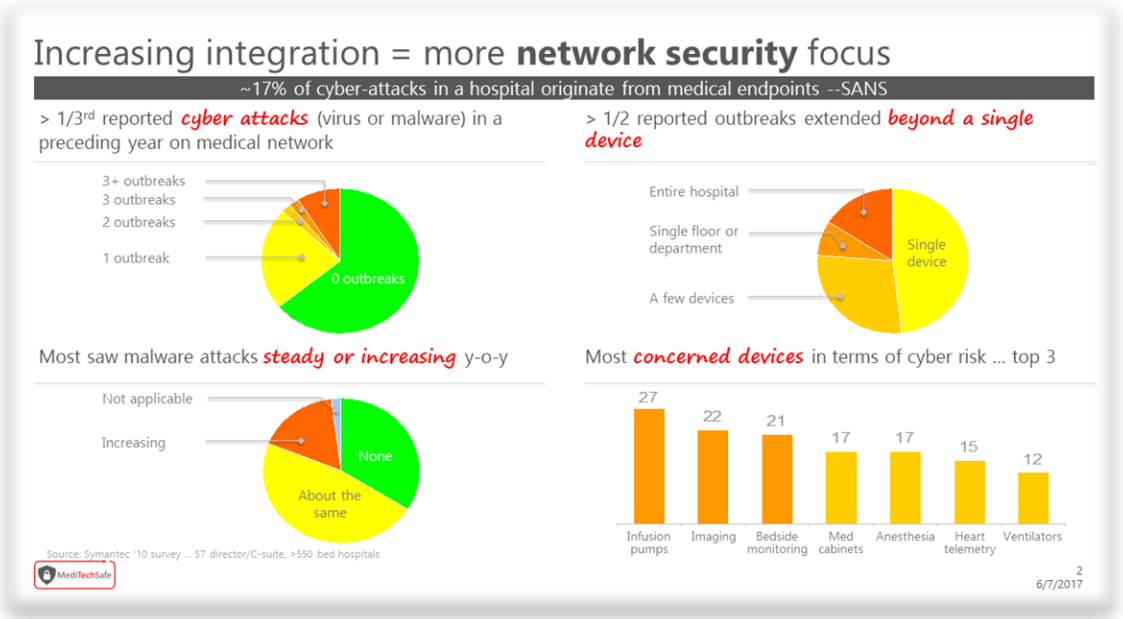
- In **2011**, a security expert hacked into an insulin pump at the Black Hat security conference, showing how the device could be accessed remotely with the ability to increase the dose of insulin.
- In **2012**, Jack Barnaby demonstrated a serious medical device cybersecurity vulnerability when, at a conference in Melbourne, he demonstrated that he could remotely cause an implanted pacemaker to deliver an 830V shock.
- In **2014**, the FBI released a warning to hospitals to discontinue use of a certain line of infusion pumps from medical device maker Hospira due to security flaws that could potentially allow an unauthorized user to remotely change medication dosages dispensed by the pumps.
- In **2015**, students at the University of Alabama hacked the pacemaker implanted in an iStan (a robotic dummy patient used to train medical students) and were able to speed up its heart rate.
- In **2016**, Johnson & Johnson warned diabetic patients that some of its insulin pumps are vulnerable to hacking.
- In Jan **2017**, FDA confirmed that St. Jude's cardiac devices can be hacked.
- In May **2017**, WannaCry ransomware infected one of Bayer's medical products, whereas Siemens warned that some of its products are also vulnerable.

Clearly, experts have been pointing to potential threats for many years. However, it seems that the industry has been waiting for actual attacks to get fully concerned about protecting medical devices and networks!

Medical devices are often the direct interfaces with patients. Consequently, malfunctioning of medical devices from exploitation of their vulnerabilities could lead to serious patient safety concerns. To illustrate this point, we could look at the patient injuries due to adverse events from medical devices in the figure below. On average, almost **1.4 patients get affected monthly in a hospital due to malfunctioning of medical devices**! It is interesting to note that 44% of those were due to vulnerabilities in Software (SW) and Hardware (HW), arising from design and post-production change phases. It isn't unimaginable to think that ill intending cyber attackers could potentially directly or indirectly exploit these vulnerabilities in the installed base of these devices.



Cyberattacks targeting medical devices and networks could not only get Patient Health Information (PHI), but could also cause harm to patients. **Reports indicate that major cyberattacks on healthcare grew 63% in 2016; about 17% of cyberattacks in a hospital originate from medical endpoints according to a SANS Institute report.** Increasing integration of medical devices into a clinical network with Internet of Things (IoT) trend only increases the risk. A survey done by a security company shows that **outbreaks often extends beyond a single device** due to the integration. Till 2012, only about 8% of medical devices were connected to a network; that number is in range of 30%+ today and only increasing!



Holistic Approach to Cybersecurity and Risk Management

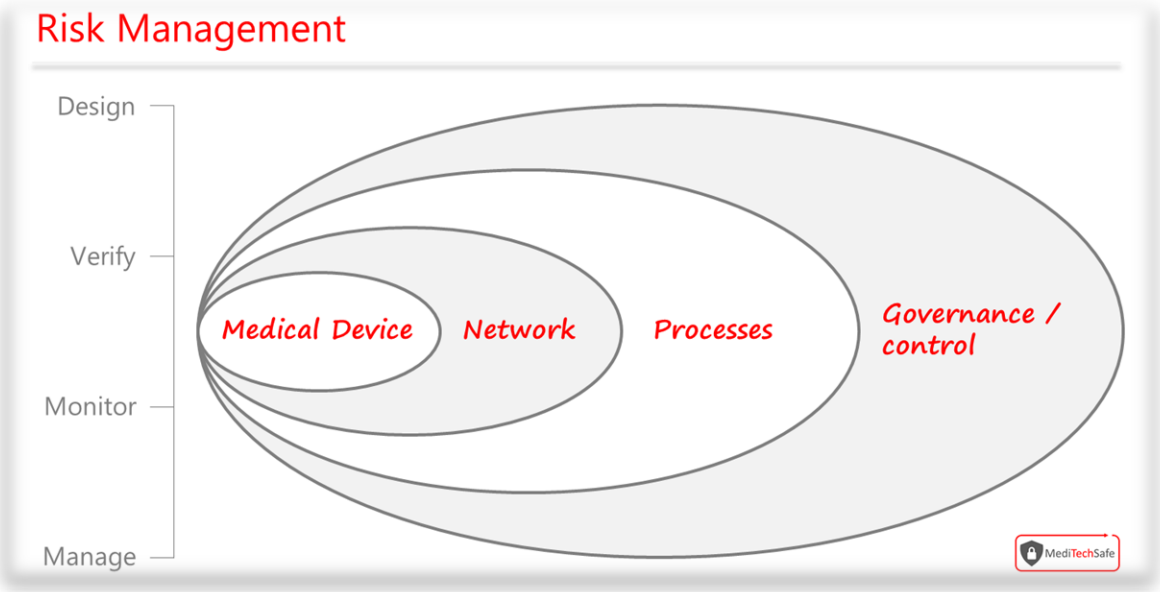
While complete risk avoidance may not be practically feasible, a holistic approach could help reduce risk tremendously. It, however, requires engagement from medical device manufactures, IT equipment manufacturers, and multiple parties from healthcare provider organizations such as biomedical engineering, IT, clinical and compliance teams. Each party has a specific and critical role to play in ensuring cybersecurity of medical devices and clinical networks.

Medical devices sit at the center; the device manufacturers (OEMs, also referred as MDMs in some literature) have to start implementing *Design for Security* practices if not already undertaken. The practices could include design for fail-safe, patient centric risks and associated *alerts* based on key system parameters, built-in protection around various USB ports, etc. Medical device OEMs have to prioritize patch *verification* and validation activities to release them in timely fashion. The IT gear manufacturers are expected to do the same in addition to releasing specs and failure mode information of their products for the healthcare provider's IT teams to design robust medical IT networks.

Stakeholders	Accountability
Medical device OEMs	• Design for security • Patch release with clinical validation
IT gear OEMs	• Design for security • Patch validation and release • Specs for network design
Healthcare providers	
Biomed engineering	• Device level patch validation and installation
IT	• Clinical network design for security • Patch validation in network
Clinicians	• Clinical inputs for risk management in design of clinical network for security
Compliance	• Process development, training, governance and control for cybersecurity

Within a hospital, biomed engineering team is expected to have the most knowledge about medical devices, their operations, maintenance and related compliance matters. Consequently, they are expected to manage OEM approved modifications and relevant tests as per specifications and instructions, including patching of devices, in hospitals. They are also expected to provide device operations knowledge to the IT team, as part of a cross-functional team, in designing, remediating and managing medical IT networks and associated test protocols. The IT and security teams are expected to employ *Design for Security* methodologies in designing, deploying, validating and managing these **networks,** considering risks to patients and the enterprise. Clinicians' inputs are vital in designing and developing *verification & validation* test protocols for cybersecurity of these networks; they are the most knowledgeable about patients' health safety implications from performance of the medical devices and networks. For example, only clinicians should define if 5 seconds or 5 minutes delay in achieving a specific alert about a patient's health is adequate, based on the complication and condition of the patient; if a cyberattack were to cause signal jamming, is there a built-in redundancy in the network to deliver the alert in specified time to ensure patient safety? Is there a built-in feature for remotely *monitoring* the performance of the medical IT network to ensure appropriate

actions when cyberattacks happen? Hospital compliance team is expected to help build **processes** and network design as well as testing features to identify, protect, detect, respond and recover from cyberattacks to minimize risk … call it *management* responses. They should also lead development of cybersecurity training programs targeted towards medical devices and networks with help from biomed, IT and clinical teams. **Governance and control** is essential to maintain vitality of the processes and policies. It also allows comfort to the hospital Boards about management's proactive approach to cybersecurity!



Clearly, a holistic approach to cybersecurity of medical devices requires focus not only on medical devices but also on the associated medical IT networks, processes and governance and control methods. There are elements of design, verification, monitoring and management efforts at each level. **When clinical data flow bi-directionally through a network, that clinical network should be treated like a Class I medical device** requiring associated clinical verification and validation processes. Because individual hospitals are going to have converged medical IT networks with the increasing trend of connected medical devices, the responsibility of clinical verification and validation will rest on hospitals' shoulders; this is not a muscle that most hospitals have fully developed yet. Overall potential risk from cyberattacks is so large that it isn't fair to only hold CISO and/or CIO accountable for cybersecurity of medical assets. **It must be a strategic priority from the top of an organization, requiring focus from the Board, CEO, CMIO, CIO, CISO, COO and CFO**.

Though the approach to cybersecurity of devices in a hospital may certainly look overwhelming, the consequences of cyberattacks on the medical assets could potentially be far worse!

MediTechSafe has developed a **proprietary solution** to help hospitals manage their cybersecurity related risks from medical devices and clinical networks. If you are a healthcare

provider (or a biomed services provider) interested in learning more about **MediTechSafe**'s solution, you could reach us at info@meditechsafe.com.