Holding the Line: Events that Shaped Healthcare Cybersecurity

Stephen Grimes and Axel Wirth

1982 The first computer virus is released into the wild by high school student Rich Skrenta. Called "Elk Cloner," this mostly harmless program displays a poem on Apple II computers.

1999 **Sept.** The Food and Drug Administration (FDA) issues *Guidance for Industry on Compliance of Off-the-Shelf Software Use in Medical Devices*.

2001 **July.** AAMI and the American College of Clinical Engineering (ACCE) hold a conference on medical device security and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

2002 **Nov.** Beth Israel Deaconess Medical Center in Boston experiences a massive, multiday network failure that includes medical devices.

2003 **Feb.** The final HIPAA Security Rule is published, which is intended to protect electronic protected health information.

2004 **May.** ACCE and the ECRI Institute publish *Information Security for Biomedical Technology: A HIPAA Compliance Guide*.

Nov. The Healthcare Information and Management Systems Society (HIMSS) releases the *Manufacturers Disclosure Statement for Medical Device Security* (MDS2) form, which provides medical device manufacturers with the means to disclose security-related features of medical devices to healthcare providers.

2005 **Jan.** The FDA publishes the guidance *Cybersecurity for Networked Medical Devices for Containing Off-the-Shelf (OTS) Software*.

2008 **March.** Researchers uncover vulnerabilities in implantable cardiac defibrillators to software radio attacks.

Feb. The U.S. Supreme Court rules on the case of *Riegel versus Medtronic, Inc.* The decision in favor of Medtronic meant that the medical device amendment to the Food, Drug, and Cosmetic Act preempts state common law claims for defective medical devices that meet federal requirements.

2009 **Feb.** The Health Information Technology for Economic and Clinical Health (HITECH) Act is signed into law. The law provides incentive to increase the use of electronic health record systems, as well as widens protections (including security) under HIPAA.

2010 The Medical Device Innovation, Safety & Security Consortium (MDISS) and the National Health Information Sharing and Analysis Center (NH-ISAC) are founded.

Oct. ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT Networks incorporating medical devices—Part 1: Roles, responsibilities and activities* is published. This standard helps ensure that information assets (i.e., data and systems associated with medical devices) are reasonably protected from compromises to confidentiality, integrity, and availability.

2011

Feb. Baylor Health notifies the Department of Health & Human Services and more than 8,000 patients of a data breach caused by the theft of an ultrasound imaging device.

Aug. Researcher Jay Radcliffe demonstrates at the Black Hat security conference that insulin pumps can be controlled remotely and are open to attack. The work was built upon by Barnaby Jack.

2012

MDISS launches MDRAP (Medical Device Risk Assessment Platform) to help healthcare delivery organizations (HDOs) and medical device manufacturers understand and mitigate the cybersecurity risks of their medical devices.

July. The first parts of ANSI/AAMI/IEC technical information report (TIR) 80001-2 (including guidance for the disclosure and communication of medical device security needs, risks, and controls) are published.

Aug. The Government Accountability Office issues a report to Congress, *FDA Should Expand Its Considerations of Information Security for Certain Types of Devices*.

Dec. The Showtime series *Homeland* depicts the assassination of a politician conducted by wirelessly hacking an implanted medical device.

2013

Oct. The first major revision to the original MDS2 form is published as MDS2 HIMSS/National Electrical Manufacturers Association HN-1 2013, *Manufacturer Disclosure Statement for Medical Device Security*. The updated form aligns with the ANSI/AAMI/IEC 80001-1 standard and its supplementary guidances.

2014

Feb. NIST publishes the first version of *Framework for Improving Critical Infrastructure Cybersecurity*. This guidance describes what industries and organizations associated with the nation's critical infrastructure (which includes healthcare) should be doing to protect the elements over which they have control. A revised version is scheduled for publication in 2017.

April. The Federal Bureau of Investigation issues the industry notification, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusion for Financial Gain*.

April. The hacker group Anonymous targets the website of Boston Children's Hospital with a distributed denial-of-service attack in order to protest a Massachusetts child custody decision.

June. AAMI and the ECRI Institute issue a report on cybersecurity and other hazards, *Executive Insights on Healthcare Technology Safety*.

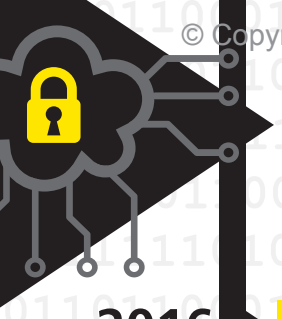
Oct. The FDA releases *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. It provides guidance for manufacturers on the cybersecurity factors to include in their quality system and premarket submissions.

2015

Feb. More than 78 million customer records are stolen in a breach of insurance company Anthem.

May. TrapX Labs publishes the white paper *Anatomy of an Attack: MedJack (Medical Device Hijack)*.

Aug. The FDA issues a cybersecurity alert following the discovery of cybersecurity flaws in Hospira infusion pumps by Billy Rios.



2016

Feb. Hollywood Presbyterian Medical Center in Los Angeles pays out a $17,000 ransom to ransomware hackers after its computers are locked down.

July. AAMI publishes TIR57, *Principles for medical device security—Risk management*. The TIR provides guidance on methods to perform security risk management for connected medical devices.

Aug. Cybersecurity firm MedSec publishes a report with Muddy Waters Research that claims St. Jude Medical pacemakers are vulnerable to cyberattack. St. Jude, now owned by Abbott, disputes the report.

Dec. The FDA publishes final guidance on *Postmarket Management of Cybersecurity in Medical Devices*. This guidance encourages medical device manufacturers to report known vulnerabilities and associated mitigations to an information sharing and analysis organization (ISAO) or center (ISAC).

2017

Jan. The Medical Device Vulnerability Intelligence Program for Evaluation and Response is introduced by the FDA, MDISS, and NH-ISAC. The program guides the reporting of vulnerabilities to ISAO or ISAC.

Feb. AAMI's Device Security Working Group is approved to begin development of AAMI SW96/Ed. 1, *Medical devices—Application of security risk management to medical devices* based on the guidance document AAMI TIR57.

April. The Windows OS exploit EternalBlue is leaked online. It is reported to have been developed by the National Security Agency.

May. The WannaCry ransomware worm attacks unpatched Windows computers and medical devices worldwide in what is considered to be one of the most impactful cyberattacks in history. Several HDOs and the British National Health System are affected. This attack takes advantage of the leaked EternalBlue exploit.

May. The FDA, National Science Foundation, and the Department of Homeland Security convene a public cybersecurity workshop, *Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis*, to highlight cybersecurity regulatory gaps. The workshop brings together the academic community, third-party experts, federal agencies, HDOs, and manufacturers.

June. A 21-member task force concludes that "healthcare cybersecurity is in critical condition" in the Department of Health and Human Services' *Report on Improving Cybersecurity in the Healthcare Industry*.

June. Medical device cybersecurity takes center stage at the AAMI 2017 Conference & Expo in Austin, TX, where cybersecurity expert Kevin Fu delivers the keynote address.

June. The Petya ransomware and its variants ExPetr and NotPetya attack pharmaceutical, advertising, shipping, and energy companies worldwide. Ukraine is disproportionately affected. Some variants of Petya use an exploit similar to WannaCry.

Aug. The FDA issues a voluntary recall of affected Abbott (formerly St. Jude Medical) pacemakers due to their vulnerability to cyberattack. The corrective action affects 465,000 implanted devices.