PUBLICATION

Ransomware Imminently Expected to Target Medical Devices

Authors: Thomas H. Barnard
May 17, 2017

As a wave of devastating ransomware-based attacks spread across the globe last week, it became abundantly clear that the medical industry at large was ill-prepared for the threat despite years of warnings. The virus hit medical systems as large as the National Health Service in England, various hospital systems in more than 150 different countries and countless providers particularly hard.

Last week's events illustrated the importance of dedicating resources to ensure that a provider's systems and procedures are up-to-date with the latest security patches, adequate antivirus measures, regular and secure data back-up systems, and security incident response plans – as those reasonable precautions alone may have been enough to mitigate the most recent threat. The attack was also a reminder that there is no substitute for preparedness and reliable information in the event of an attack.

Medical Devices are at Risk

Complicating this cybersecurity risk in health care is the looming threat to medical devices. More and more, medical devices have Internet connectivity in order to allow providers to monitor patients remotely and enable better patient outcomes, but the risks created by that trend are poorly understood by manufacturers, designers, prescribers and end-users. Most notably, medical devices do not run antivirus software, are not easily patchable and therefore are not generally updated timely, and while they are generally protected by passwords, those passwords are often easily discoverable in device documentation. Devices and other medical equipment are also commonly subject to failures to appropriately wipe localized data from user to user.

This confluence of factors makes Internet-enabled medical devices a security nightmare. The threat to end-users is very real and already here. Most estimates say that tens of millions of breaches have already occurred and patient health data has already been successfully exfiltrated by malicious actors. While the focus of the known attacks on Internet-connected devices to date has been compromising patient data for the purpose of identity theft, the Food and Drug Administration (FDA) has been warning for years that criminals could use ransomware-based attacks targeting medical devices such as insulin pumps or pacemakers in order to literally hold someone's life for ransom – while incurring almost zero risk of getting caught. It is also important to note that even devices that do not connect directly to the Internet, but that share a network with Internet-connected resources, are at risk; there have already been significant data breaches involving magnetic resonance imaging (MRI) machines and other similar devices.

In August of 2015, we previously reported that the FDA issued a warning that the Hospira Symbiq Infusion System, a widely-used insulin pump, was extremely vulnerable to a potentially life-threatening cyber-attack. Johnson & Johnson was forced to issue a similar alert concerning its Animas OneTouch Ping only last year. In September of 2015, the FBI warned broadly of the coming threat of ransomware specifically aimed at medical devices. In a recent article in a Belgian Medical Journal, an investigation found ten Implantable Medical Devices already on the market with exploitable security problems that made them susceptible to a ransomware-based attack that could directly threaten a patient's life. McAfee Labs' 2017 Threats Predictions contained the dire warning that "[w]e are certain that ransomware will readily migrate to IoT (Internet of Things, a common way of referring to Internet-enabled devices), as it has proven to be a relatively easy way for

criminals to make money." Despite the various warnings over the years, however, vulnerabilities remain. In fact, the U.S. Department of Health and Human Services (HHS) recently reported that it has already received anecdotal notices of medical device ransomware infections.

Last week proved that ransomware could dramatically impact the medical industry, even when only data was at stake. Health care practitioners must seriously consider that the risk posed by ransomware goes beyond loss of data and may threaten the actual health and safety of patients' lives. Steps must be taken by all facilities to prepare for these attacks and manufacturers must account for these risks in designing their devices.

FDA's Public Workshop – Cybersecurity of Medical Devices

One way to arm yourself is to get involved. FDA, in association with National Science Foundation (NSF) and Department of Homeland Security, Science and Technology (DHS, S&T) is holding a public workshop entitled "Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis." The purpose of this workshop is to examine opportunities for FDA engagement with new and ongoing research, catalyze collaboration among Health Care and Public Health (HPH), stakeholders to identify regulatory science challenges, discuss innovative strategies to address those challenges and encourage proactive development of analytical tools, processes and best practices by the stakeholder community to strengthen medical device cybersecurity.

This meeting will be held May 18 – 19, beginning at 8:00 a.m. – 5:00 p.m. at the following location:

FDA White Oak Campus
10903 New Hampshire Avenue
Bldg. 31, Room 1503
Silver Spring, MD, 20993

How to Reduce Risks and Prepare for Attack

We recommend you take the following steps to help reduce the risk of and damage from an attack:

- **Arm yourself with knowledge: Get familiar with the reliable informational resources that are available to you.** Find the most up-to-date information from the U.S. government and stay abreast of updates via email alerts.

- **Train and frequently remind your workforce not to click on unreliable links and attachments.**

- **Authenticate the identity of any person wanting access to your IT systems.** Train your staff not to fall for scams such as callers claiming to be from Microsoft and asking for access to the network or a medical device to fix a problem. Multi-step authentication of identity should become a routine part of workforce procedures.

- **Hope for the best but prepare for the worst.**
  - **Know where your data is and where it is flowing.** Your data security program is only as good

as your data map and information governance programs. Data destruction in accordance with a regimented plan is critical to managing risk.

- **Dust off your data security incident plan** and make sure it includes up-to-date procedures relating to medical devices and contact information (with cell phone numbers) for your cyber liability attorney and response vendors. Your security incident plan should be linked with your emergency management plan. Consider contracting with your favorite data response/breach attorney and vendors to help ensure quick response at reasonable prices in the event of another national or international crisis. Data incident plans should include procedures for notifying and working with device manufacturers and various governmental entities – when applicable.
- **Review your cyber liability insurance coverage to ensure adequacy**. Make sure your insurance policy panels allow you to work with attorneys and vendors you trust.
- **Run a tabletop exercise on a ransomware attack.** Immediate response and strong downtime procedures are key to surviving any attack. Be sure any practice exercises include simulating the use of backup systems – including paper-based procedures.
- **Your risk assessment and risk management plans should factor in medical devices as risks that must be managed.**
- **Perform due diligence on all device vendors and business associates.**
- **Do not house/manage your workforce emergency communications systems on the same IT platform as your other medical records and devices systems.**
- **Be sure to review and implement the most recent manufacturer guidelines for data security and data wiping of medical devices between users.**

Baker Donelson's Data Protection, Privacy and Cybersecurity Team was recently recognized as a member of the "Honor Roll of Cybersecurity Law Firms" in the United States as determined by The BTI Consulting Group. Recognition as a member of the Honor Roll reflects corporate counsel's view of the Baker Donelson team as strong cybersecurity performers. To link to the Baker Donelson series on ransomware, please click here.

If you have any questions about ransomware, please reach out to Thomas Barnard or any of the 36 members of Baker Donelson's Data Protection, Privacy and Cybersecurity Group which includes nine attorneys who have a CIPP/US certification, one attorney with a CISSP certification and the former General Counsel of Homeland Security.