Supported Lifetimes Request for Information

As cybersecurity threats to the health care sector have grown, the Energy and Commerce Committee's attention has grown in parallel. Over the course of dozens of hearings, letters, roundtables, briefings, and more, the Committee has examined health care cybersecurity issues to identify common factors and potential strategies for addressing them. While health care cybersecurity is a complex, nuanced challenge with many different contributing factors, the use of legacy technologies, which are typically more insecure than their modern counterparts, continues to be a root cause of many incidents. The health care sector and medical technologies face the same challenge that has vexed the information technology (IT) industry for decades; digital technologies age faster and less gracefully than their physical counterparts.

This fact was illustrated in May 2017, when a flaw in a 30-year-old software protocol led to the global infection of hundreds of thousands of devices by the WannaCry ransomware.[1] The United States health care sector escaped the worst of the danger due to the timely intervention of an independent security researcher.[2] However, the existence of this severely outdated protocol throughout modern medical networks—including within devices such as MRIs and X-Ray machines, in addition to traditional desktops—alerted stakeholders to the pervasiveness and severity of the legacy problem in health care.[3] The WannaCry outbreak occurred primarily because of one protocol embedded within dozens of unique medical technologies. In the aftermath of the outbreak, health care stakeholders were faced with a troubling question: how many other potential "WannaCrys" lurk within their environments?

Exacerbating this situation, finding and fixing vulnerabilities like the one leveraged by WannaCry is costly. Though hard data about the exact costs are difficult to determine, one cybersecurity professional estimated that fixing a single vulnerability may cost an organization anywhere from $400 to $4,000.[4] Considering the fact that many popular medical technologies leverage software and hardware with hundreds to thousands of known vulnerabilities, let alone unknown ones, vulnerability identification and management can quickly become a daunting

---

[1] Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED (Mar. 12, 2017), https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.
[2] Lily Hay Newman, *How An Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack*, WIRED (May 13, 2017), https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.
[3] *INFORMATION TECHNOLOGY ADVISORY - "WannaCry" Ransomware*, BAYER (last updated May 24, 2017), https://webcache.googleusercontent.com/search?q=cache:CZo9_qnMQNIJ:https://radiology.bayer.com/products-and-services/product-security/wannacry-ransomware+&cd=3&hl=en&ct=clnk&gl=us; *Customer Information on WannaCry Malware for Siemens Healthineers Imaging and Diagnostics Products*, SIEMENS last updated June 14, 2017), https://www.siemens.com/cert/pool/cert/siemens_security_bulletin_ssb-421479.pdf; *Product security service bulletin for "WannaCry" ransomware*, BD (last visited Jan. 25, 2018), http://www.bd.com/en-us/support/product-security-and-privacy/product-security-bulletin-for-wannacry-ransomware.
[4] Kelly Jackson Higgins, *The Cost of Fixing An Application Vulnerability*, DARKREADING (May 11, 2009), https://www.darkreading.com/risk/the-cost-of-fixing-an-application-vulnerability/d/d-id/1131049.

task.[5] This leads to a cost-benefit analysis between the value provided to an organization through the use of a given piece of technology, the costs of keeping it patched and updated, and the risks posed by using technologies which may be too expensive in terms of time and resources to update.

Often, the first piece of advice given to organizations looking to manage these challenges is deceptively simple: organizations should replace technologies as their benefit to cost ratio shifts, as—in theory—new technologies have learned from the mistakes of their ancestors and are less susceptible to the same weaknesses. While this is certainly an accepted and recommended practice in the IT industry, where technologies are routinely declared "end-of-life" and support is discontinued in favor of more modern software and hardware, its application in the health care sector is more complicated.

Medical technologies are, in many cases, significantly more specialized than traditional IT products. There may be only two or three products available that can perform vital medical treatments or diagnostics, and those products may have been built using software and hardware that were considered cutting-edge at the time of manufacture but are now considered legacy. For some of these products, replacements or alternatives may not be available, or they may be affected by similar vulnerabilities, leaving organizations with few, if any, good options.

In addition, medical technologies typically are vastly more expensive than consumer or enterprise IT. Many hospitals operate on thin or nonexistent margins and replacing technologies may mean foregoing additional staff or patient care needs. As a result, organizations may reason that replacing technologies to address intangible and often esoteric cybersecurity vulnerabilities, especially in machines that may still exhibit acceptable physical operation, does not provide enough benefits to offset the costs. Why, if a device can still meet its intended use, should it be replaced at the expense of other organizational needs?

Given the significant costs of replacing legacy technologies, some argue that, rather than replace the technology, manufacturers and developers of medical technologies should be required to support these technologies as long as they are still in circulation. But this is an equally troublesome proposition for many reasons. It is sometimes inefficient or impractical to fix vulnerabilities, as doing so may mean entirely rearchitecting or rewriting the chipsets, operating systems, or applications on which a technology relies. This is an expensive undertaking not just in terms of funding, but in terms of time and expertise. Further, technologies are often heavily interdependent, and fixing a vulnerability in one product may give rise to numerous others in reliant products.

---

[5] *Windows Xp: Security Vulnerabilities*, CVE DETAILS (last visited Jan. 29, 2018), https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-739/Microsoft-Windows-Xp.html; *Linux Kernel: Security Vulnerabilities*, CVE DETAILS (last visited Jan. 29, 2018), https://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/Linux-Linux-Kernel.html; *Openssl: Security Vulnerabilities*, CVE DETAILS (last visited Jan. 29, 2018), https://www.cvedetails.com/vulnerability-list/vendor_id-217/product_id-383/Openssl-Openssl.html.

Policies that would require manufacturers to support legacy technologies indefinitely would therefore likely have significant impacts on their ability to provide new and innovative technologies, as their resources would necessarily have to be spent maintaining their legacy products. This would likely lead to a decrease in the invention and development of new, advanced treatments and procedures that might otherwise help meet the health care sector's primary motivation: the health and well-being of patients.

The challenges created by legacy technologies are, by definition, decades in the making. They implicate dozens of diverse stakeholders with different and at times competing equities, and they have no clear solutions. While the issues described so far have been some of the most common encountered by the Committee as we've explored this topic, much information-gathering remains to be done. To understand the full scope of the challenge and potential paths to address it, we require insight from stakeholders of all sizes, from all parts of the health care sector.

Collecting these issues under the heading "Supported Lifetimes," the Committee today requests information regarding legacy technology challenges, opportunities, considerations, and suggestions in the health care sector. The Committee welcomes the public's input and feedback to supportedlifetimes@mail.house.gov by May 31, 2018. Please be advised that submissions sent to supportedlifetimes@mail.house.gov will be made publicly available to help further the discussion around how best to approach supported lifetimes and legacy technologies. We thank you for participating.