J Med Syst (2017) 41: 104
DOI 10.1007/s10916-017-0752-1

WannaCry, Cybersecurity and Health Information Technology: A Time to Act

Jesse M. Ehrenfeld[1]

Published online: 24 May 2017

On Friday, May 12, 2017 a large cyber-attack was launched using WannaCry (or WannaCrypt). In a few days, this ransomware virus targeting Microsoft Windows systems infected more than 230,000 computers in 150 countries. Once activated, the virus demanded ransom payments in order to unlock the infected system.

The widespread attack affected endless sectors – energy, transportation, shipping, telecommunications, and of course health care. Britain's National Health Service (NHS) reported that computers, MRI scanners, blood-storage refrigerators and operating room equipment may have all been impacted. Patient care was reportedly hindered and at the height of the attack, NHS was unable to care for non-critical emergencies and resorted to diversion of care from impacted facilities.

While daunting to recover from, the entire situation was entirely preventable. A "critical" patch had been released by Microsoft on March 14, 2017. Once applied, this patch removed any vulnerability to the virus. However, hundreds of organizations running thousands of systems had failed to apply the patch in the first 59 days it had been released.

This entire situation highlights a critical need to reexamine how we maintain our health information systems. Equally important is a need to rethink how organizations sunset older, unsupported operating systems, to ensure that security risks are minimized. For example, in 2016, the NHS was reported to have thousands of computers still running Windows XP – a version no longer supported or maintained by Microsoft.

There is no question that this will happen again. However, health organizations can mitigate future risk by ensuring best security practices are adhered to.

✉ Jesse M. Ehrenfeld
jesse.ehrenfeld@Vanderbilt.Edu

[1] Vanderbilt University, Nashville, TN, USA