IN VIVO
CITELINE COMMERCIAL

18 May 2017 | **Opinion**

WannaCry Cybersecurity Alert Shows Medtech Software Must Look Beyond Quick Fixes

by Ashley Yeo

Preventing cyberattacks on medical technology occupies the waking thoughts of device software manufacturers, but the global ransomware episode in mid-May shows that companies must also be alive to threat posed to their provider customers.

The WannaCry (WanaCrypt0r 2.0, WCry) ransomware attack that affected over 200,000 systems globally on Friday May 12 locked users out of their IT systems and demanded a relatively small bitcoin ransom to let them resume access.

Most of the headlines focused on the relatively large effect on systems used by the NHS England, where 40 trusts reported that they had been hacked. Eleven Scottish Health Boards were also affected. Patient data were not affected: files were not compromised, simply inaccessible. Clinical care was affected and logistics disrupted.

This was a problem largely of the national UK health provider's own making – the persistent use of unsupported systems using outdated Windows XP systems, and failure in some cases to upload security update patches when prompted to do so or in time.

NHS Digital counters that the vast majority of NHS organizations are running contemporary IT systems, but attributing blame to provider systems' inadequate budgets is a pointless exercise after the fact. The lessons are there to be learned at provider systems around the world, which will be aware that the hacking could have been much more damaging. They should use the incident to protect their own systems from risk of compromise.

For their part, medical device industry suppliers were quick to help providers restore operations and protect systems from further risk of attack. Microsoft issued a patch to users a few days after

the attack, but some NHS IT developers are recommending the health service reduce its reliance on Microsoft.

> *For the device industry branches most affected by the hack – digital pathology, and CT and MRI imaging, the solution is not as easy as simply applying a patch at will.*

The exploitability of any such vulnerability depends on the configuration and deployment environment of each product. For the device industry branches most affected by the hack – digital pathology, and CT and MRI imaging, the solution is not as easy as simply applying a patch at will. That reality is explained by AXREM, the UK trade association representing suppliers of diagnostic medical imaging, radiotherapy, health care IT and care equipment, in a release issued on May 18.

Medical imaging systems differ from standard personal computers and server systems that can often receive cumulative updates or patches promptly. But medical imaging system software products are medical devices, and the strict regulatory needs mean that suppliers must do rigorous tests on each and every software update to ensure that functionality and safety are not compromised.

"For this reason, the reliance on the provision of clinical product software patches for defending against malware attacks is not a sustainable option, given that this would mean a new regulatory-approved and clinically-tested software release for multiple assets on as much as a daily or weekly basis to keep pace with evolving malware," says AXREM.

Suppliers are having to balance their obligation and responsibility to validate patches and software updates, as well as provide additional network security provisions, with the requirement to promptly apply appropriate protective measures in addition to those applied within customers' own networks.

The significance of the May 12 incident is that it is a health care first in terms of its scale and impact. At the same time, few could deny the was a pervading sense of the inevitability of such an episode. Cybersecurity has rapidly become a top priority in the device industry; in March 2017, day two of the International Medical Device Regulators Forum (IMDRF) meeting put a major focus on the theme of understanding and tackling the cyber threat to the medical device

industry.

Late last year, DITTA, the Global Diagnostic Imaging, Healthcare IT, and Radiation Therapy Trade Association (DITTA), released a *white paper* on cybersecurity needs. "Cybersecurity of Medical Imaging Equipment" set the tone for what will be this industry sector's major talking point for the whole of 2017 and beyond.

Post WannaCry, NHS Digital provided more guidance on protection against cyberattacks, but manufacturers know that the ball is in their court and they must devise solutions with the regulatory constraints they live under not just for their own products but for their downstream customers.