COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 4. April 09, 2020 Privacy Briefs: April 2020

By Jane Anderson

◆ **Health care organizations in the United States, Europe and other world regions are seeing a stark uptick in the number of hacking attempts in the midst of the COVID-19 pandemic**, *Bloomberg News* reports.[1] Some incidents may be related to COVID-19 research or patient care. For example, bad actors broke into computers at Hammersmith Medicines Research, a London-based company that carries out clinical trials for new vaccines just as the company was in talks with other firms for potentially testing a COVID-19 vaccine. The hackers encrypted thousands of patient records and promised to publish them online if a ransom wasn't paid, but the company was able to work with police and its own IT staff to mitigate the damage. Europol, the European Union's law enforcement agency, has received reports of intensifying cyberattacks in almost all of its 27 member countries, and experts say several of the attacks appear to be the work of an organized crime syndicate that uses a strain of ransomware known as Maze. In the U.S., multiple health care providers, such as hospitals, medical laboratories, doctor's offices and urgent care centers, have been hit by ransomware during the crisis.

◆ **As hackers dialed up their attacks on health care entities during the COVID-19 crisis, the Department of Health and Human Services (HHS) was breached by hackers**. Few details were revealed, but a spokesperson for HHS subsequently told *The Hill* that the agency "became aware of a significant increase in activity on HHS cyber infrastructure and are fully operational as we actively investigate the matter."[2] HHS Secretary Alex Azar played down the incident further, saying at a White House news conference that there was "no penetration into our networks" and "no degradation of our ability to function or serve our important mission here."

◆ **A report from Palo Alto Networks reveals that 83% of medical imaging devices are running on unsupported operating systems.**[3] This reflects a 56% jump from 2018 due to the Windows 7 operating system reaching its end of life, and leaves hospital organization vulnerable to attacks that can disrupt care or expose sensitive medical information. The report also uncovered several other threats. For example, it found that 98% of all Internet-of-Things (IoT) device traffic at health care organizations is unencrypted, exposing personal and confidential data on the network and allowing attackers the ability to listen to unencrypted network traffic, collect personal or confidential information, and then exploit those data for profit on the dark web. In addition, 51% of threats for health care organizations involve imaging devices, disrupting the quality of care and allowing attackers to exfiltrate patient data stored on IoT devices. Finally, 72% of health care virtual local area networks mix IoT and information technology assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network. "Threats continue to evolve and target IoT devices using new sophisticated and evasive techniques, such as peer-to-peer command and control communications and worm-like features for self-propagation," the Palo Alto Networks study says. "Coupled with a weak device and network security posture, attackers have ample opportunity to compromise IoT systems." Some 57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT "the low-hanging fruit for attackers," the report says. In addition, 41% of attacks exploit device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses, the report says. "We found that, while the vulnerability of IoT devices make them easy targets, they are most often used as a stepping stone for lateral movement to attack other systems on the network," the report authors wrote, noting that password-related attacks on IoT devices are prevalent due to weak manufacturer-set passwords and poor password security practices. Finally, "we're also

witnessing a shift away from attackers' primary motivation of running botnets to conduct [distributed denial of service] attacks via IoT devices to malware spreading across the network via worm-like features, enabling attackers to run malicious code to conduct a large variety of new attacks."