COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 3. March 10, 2022 Privacy Briefs: March 2022

By Jane Anderson

◆ **HHS said in early March that it was not aware of any specific threat to U.S. health care organizations stemming from the Russian invasion of Ukraine.** "However, in the interest of being proactive and vigilant, we are briefly reviewing the cyber capabilities of Russia and its allies and specifically two malware variants most likely to be utilized in any collateral attacks which may impact [the U.S. Healthcare and Public Health Sector] in this campaign," the HHS Cybersecurity Program Office of Information Security said in a March 1 analyst note.[1] There are three potential threat groups, the note said: organizations that are part of the Russian government, cybercriminal groups based in Russia and neighboring states, and organizations that are part of the Belarussian government. In addition, there are two malware variants that have been observed in significant use against Ukraine in the last two months: HermeticWiper and WhisperGate, the note said. HermeticWiper comes in the form of an executable file that will damage the master boot record of the infected computer, rendering it inoperable, the analysis said. WhisperGate is a new form of disk-wiping malware that is believed to operate in three stages: a bootloader that corrupts detected local disks, a Discord-based downloader and a file wiper, the note said. HHS recommended that health care entities become familiar with these malware variants and that organizations review guidance from the Cybersecurity and Infrastructure Security Agency on defense and mitigation.

◆ **Significant security incidents continue to plague health care organizations of all types and sizes, according to the 2021 Healthcare Information and Management Systems Society (HIMSS) *Healthcare Cybersecurity Survey*.**[2] Phishing remains the most common health care sector security incident, with 45% of respondents saying a phishing attack was involved in their most serious security incident in 2021. Ransomware attacks represented the most serious incidents for 17% of survey respondents. Still, it's possible that insider threats were underreported, because many health care organizations do not have robust insider threat management programs, HIMSS noted. Financial information was the main target of hackers in 52% of the attacks, the survey revealed. Hackers targeted employee information and patient information in 43% and 39% of the most serious incidents, respectively, HIMSS said. Intellectual property, confidential business information and biometric information also were targets, according to the survey. The most typical impact of an incident is disruption, with 32% of those surveyed saying that their most serious incident resulted in disruption of systems and/or devices impacting business operations. Still, 44% of those surveyed reported that their incident had no impact or negligible impact on the organization, the survey found. Cybersecurity budgets are still tight, with 6% or less of the information technology budget typically allocated for cybersecurity, the survey found. In addition, many basic security controls are not fully implemented, although some organizations are implementing advanced security controls. The survey reflects the responses of 167 health care cybersecurity professionals, the majority of whom had primary responsibility over health care cybersecurity programs at their organizations.