Report on Patient Privacy Volume 19, Number 3. March 06, 2019

Legacy Systems Pose Under-the-Radar Threat to Security, HIMSS Survey Finds

By Jane Anderson

Email phishing is the most obvious risk facing health care entities as they seek to prevent breaches of protected health information (PHI), but legacy systems still in use are a covert—yet substantial—risk factor.

That's the word from the 2019 HIMSS Cybersecurity Survey, which found that significant security incidents are a "near universal experience" in U.S. health care organizations. The survey also found that provider organizations are making gains in addressing these threats, says Lorren Pettit, vice president for research at HIMSS.

The survey found that health care organizations continue to experience significant security incidents: only 22% of health care organizations did not experience a breach over the last 12 months, similar to previous surveys the society has done ("Privacy Briefs," *RPP* 15, no. 7). The majority of these incidents involved bad actors, and phishing and other email compromise schemes were the most prevalent threats.

However, Pettit warns that phishing may overshadow the threat posed by the expansive use of legacy platforms. "Not only do most organizations have at least one legacy system still in operation, but many organizations are resigned to the fact that they are dependent on these systems because they don't have the resources to replace [them]," he tells *RPP*.

Organizations may operate legacy systems for several reasons: there may be no other alternative for the applications involved, workflows might get disrupted during a transition, and upgrading may be extremely costly, Pettit says.

HIMSS found that 86% of hospital respondents had at least one legacy system in place, Pettit says, adding that "this finding is significant as it illuminates the tension between the need to patch and upgrade systems—if they can be patched or upgraded—and the reality that many organizations remain dependent on legacy devices."

These platforms may still perform their primary function "perfectly within expectations," Pettit says, but may require additional security controls, such as isolation on their own networks or network segments. The problem isn't necessarily the fault of security staff, he says. "Rather, it is a cost-benefit analysis and—likely—a wish for the health care organizations not to disrupt patient care and/or protocol."