# Report on Patient Privacy Volume 18, Number 5. May 31, 2018 Privacy Briefs: May 2018

By HCCA Staff

◆ Hiring more people does not necessarily lead to better security unless companies also fix their broken patching processes, according to a study from ServiceNow, Inc. The study, which included a survey of nearly 3,000 security professionals in nine countries, found that firms struggle with patching because they use manual processes and can't prioritize what needs to be patched first. More than half of those surveyed said they spent more time navigating manual processes than responding to vulnerabilities, and 61% said manual processes put them at a disadvantage. A majority of security professionals say they were breached because of a vulnerability for which a patch was already available. View the survey at https://bit.ly/2q4MwGi.

◆ An employee at a Charlotte, North Carolina, provider office shared about 100 patients' information with identity theft suspects, according to a police report. Police investigating the theft at Carolina Digestive Health Associates' University Endoscopy Center found names, birth dates and Social Security numbers on the employee's phone in January. Police were investigating because the employee had texted with someone who was indicted on federal fraud charges in Charlotte in December. Read the story at https://bit.ly/2HIvg19.