Report on Patient Privacy Volume 21, Number 8. August 12, 2021 Privacy Briefs: August 2021

By Jane Anderson

◆ **IBM Security reported that the total cost of a data breach increased by nearly 10% year-over-year in 2021, the largest single-year cost increase in the last seven years.**[1] In its annual *Cost of a Data Breach* report, IBM and the Ponemon Institute said that remote working and digital transformation due to the COVID-19 pandemic increased the average total cost of a data breach. There was a $1.07 million cost difference in breaches where remote work was a factor in causing the breach, the report said. The percentage of companies where remote work was a factor in the breach was 17.5%. Additionally, organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50% or less working remotely. Information technology (IT) changes "such as cloud migration and remote work increased costs, yet organizations that did not implement any digital transformation changes as a result of COVID-19 experienced $750,000 higher costs compared to the global average, a difference of 16.6%," the study said. In total, data breach costs rose from $3.86 million in 2020 to $4.24 million in 2021, the highest average total cost in the history of the IBM report. The health care sector had by far the highest average total cost of a data breach by industry, more than $9.23 million, up from $7.13 million in 2020. "Costs were significantly lower for some of the organizations with a more mature security posture, and higher for organizations that lagged in areas such as security AI [artificial intelligence] and automation, zero trust and cloud security," the report said. Lost business represented the largest share of breach costs, at an average total cost of $1.59 million, and customer personally identifiable information was the costliest record type, at $180 per lost or stolen record. Compromised credentials were responsible for 20% of data breaches, the IBM report found. Business email compromise was responsible for only 4% of breaches, but had the highest average total cost of the 10 initial attack vectors in the study, at $5.01 million. The second costliest was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million) and compromised credentials ($4.37 million). Organizations with a high level of system complexity had an average cost of a breach that was $2.15 million higher than those that had low levels of complexity, the study found. The presence of a high level of compliance failure was associated with breach costs that were $2.3 million higher than breach costs at organizations without this factor present, according to the report.