ARMIS CENSUSWIDE SURVEY DATA ANALYSIS

Methodology:

Censuswide conducted a survey on behalf of Armis of 400 IT professionals working in healthcare institutions in the US, and 2,030 general respondents in various industries from across the United States in October 2021.

Key Findings:

Increased cyber risk: Eighty-five percent of IT professional respondents agreed they have seen increased cyber risk over the past 12 months.

Ransomware on the rise: Ransomware alone has hit organizations hard, with 58 percent of IT pros in healthcare stating that their organization has been hit with ransomware.

Potential patients are not paying attention: The data also shows that while patients are concerned about security, and acknowledge the impact that an attack could have on their care — there is a shocking unawareness about recent cyberattacks. Despite major media headlines around vulnerabilities in pneumatic tubes, technologies used in HVAC systems, to vulnerabilities in two types of B. Braun infusion pumps to REvil attacks on healthcare organizations, 61% of potential patients stated they had not heard of any cyberattacks in the healthcare industry in the past 24 months.

Potential patients are Being Impacted: 33 percent of potential patients stated that they have been the victim of a healthcare cybersecurity attack.

Breaches guide potential patient decisions: This lack of awareness is striking, given almost half (49%) of potential patients said that they would change hospitals if their healthcare organization was hit by a ransomware attack.

IT Pros are most concerned about data breaches: Data breaches resulting in loss of confidential patient information was a top concern for healthcare IT pros (52%), followed by attacks on hospital operations (23%), and ransomware attacks (13%)

Critical infrastructure attacks were seen as the riskiest: Security risks in a hospital's infrastructure topped the list of the biggest risks (49%), followed by the risk of inputting information into an online portal (31%) and staying in a hospital room with connected devices (17%)

Building systems were seen as the riskiest devices: Healthcare IT professionals said building systems such as HVAC, electrical, etc. (54%), Imagine machines (43%), Medication dispensing equipment (40%), Kiosks for check-in (39%), and vital sign monitoring equipment (33%) were the riskiest devices.

Potential patients concerned about impact of security on quality of care: An overwhelming majority (73%) of potential patients surveyed recognize that an attack could impact their quality of care. Privacy issues associated with online portals (37%) topped the list of concerns for potential patients, and 52% said they were worried about an attack shutting down hospital operations and potentially affecting patient care.

Potential patients trust their best friend more than their healthcare provider: Sixty-six percent of potential patients believe their healthcare provider is doing enough to protect their personal information. In fact, 30% of U.S. patients trust their best friends more with their sensitive healthcare information than they do healthcare organizations (23%)

Healthcare organizations are taking steps toward a more secure environment: 85 percent of respondents stated that their organization has a CISO, and 95% of IT healthcare professionals believe their organization's connected devices are up-to-date with the latest software.

Recent attacks are a catalyst for change: 75% of IT healthcare professionals agree that recent attacks have had a strong influence on decision-making at their health organization

Organizations are putting their money where their mouth is: 52% of IT healthcare professionals believe their healthcare organization is allocating more than sufficient funds to secure its IT systems

But there is still a long way to go: 63% of IT healthcare professionals said that their organization has had to submit a cyber insurance claim.