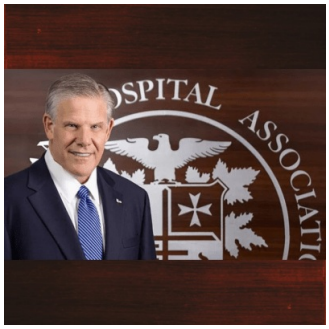
HealthManagement
Promoting Management and Leadership

Impact and Aftermath of the Change Healthcare Cyberattack: Insights from the AHA



Rick Pollack, President and CEO, AHA

Rick Pollack, the president and CEO of the American Hospital Association, addressed the Change Healthcare cyberattack at the Hospital + Healthcare Association of Pennsylvania Leadership Summit. The cyberattack, which was first reported on February 21, has been labelled by the American Hospital Association as the most significant cyberattack ever against the healthcare industry. A survey conducted by the AHA indicated that a staggering 94% of hospitals experienced a financial impact due to this attack. Furthermore, nearly 60% of these hospitals reported daily revenue losses exceeding $1 million.

Uncertainty regarding leaked data

The cyberattack has been attributed to the "Blackcat" ransomware gang by UnitedHealth Group, the parent company of Change Healthcare. However, the full scope and specifics of the data breach remain shrouded in uncertainty. Pollack highlighted the fact that it's still unknown what kind of private health data was compromised by the ransomware group and the precise number of hospitals affected. According to federal regulations, organisations must report data breaches affecting more than 500 individuals to the U.S. Department of Health & Human Services within 60 days. As of the time of Pollack's statement, there had been no such report filed regarding this cyberattack.

UnitedHealth Group's financial response and criticisms

In response to the attack, UnitedHealth Group has distributed over $3.3 billion in payments to healthcare providers and hospitals impacted by the breach. Change Healthcare, known for processing a vast number of healthcare transactions and managing patient records, faced significant disruptions in its services following the attack. Initially, the assistance and support offers extended by UnitedHealth to affected hospitals were heavily criticized. Many hospitals found the terms of the offers to be inadequate and burdensome. However, Pollack acknowledged that UnitedHealth has since improved its responsiveness to the concerns raised by hospitals.

Concerns around data consolidation trends

Despite the challenges faced by UnitedHealth and Change Healthcare, Pollack stressed that UnitedHealth is a victim of the ransomware attack and not the entity responsible for it. He issued a warning about the increasing threat posed by sophisticated cyberattacks orchestrated by nation-states or groups affiliated with them. The federal government has taken action by launching an investigation into the Change Healthcare cyberattack. Pollack also referenced the American Hospital Association's previous opposition to UnitedHealth Group's acquisition of Change Healthcare. The association had expressed concerns about the potential consolidation of private health data, and Pollack indicated that this breach underscores those concerns.

Pollack emphasised the necessity for the government to play an active role in bolstering cybersecurity measures for critical infrastructure, including healthcare. While he welcomed the federal government's initiative to establish cybersecurity goals for hospital organisations, he cautioned against imposing financial penalties for breaches. Pollack argued that penalising hospitals for breaches involving third-party vendors or partners doesn't address the core issue. Instead, he advocated for the adoption of voluntary cybersecurity standards as a more effective approach to enhancing cybersecurity in the healthcare sector.

Source: **HAP's Annual Leadership Summit**

Image Credit: **AHA**

Published on : Thu, 4 Apr 2024