HealthManagement.org
Promoting Management and Leadership

Valuable and Vulnerable: Healthcare Data Breach Forecast

The second annual data breach forecast published by Experian warns of an ongoing threat against data privacy and safety for healthcare organisations in 2015. Technological developments designed to increase efficiency and consumer involvement — such as record digitisation, cloud storage and wearable health monitoring devices — make healthcare data more vulnerable to cyber attacks due to the higher number of data access points. The data also have economic value for those engaging in fraudulent activity.

Healthcare Data Are Vulnerable

Compared to other sectors, the healthcare industry lags behind in cyber security. According to the Identity Theft Resource Center, 42 percent of major data breaches in 2014 involved healthcare industry data; one such breach exposed the medical records of 4.5 million patients from 206 hospitals. In response, many companies are adopting cyber insurance, and are communicating directly with clients about the role individuals can play in protecting themselves against fraud.

A surprising component of data vulnerability at the individual level is breach fatigue, whereby consumers who receive multiple notices of breach incidents fail to take any action. According to a 2014 report by the Ponemon Institute, 32 percent of consumers do not respond when notified of a data breach. Cyber criminals can exploit breach fatigue by stepping up attacks, secure in the knowledge that not every violation will be noticed, reported or pursued by law enforcement agencies. Meanwhile, consumers continue to expect organisations to provide identity theft and credit monitoring services, according to the Ponemon Institute study.

Confidence among healthcare providers is low, with only 28 percent of organisations reporting that they are confident in the privacy and security of patient data, according to the Ponemon Institute. Surprisingly, it is not only external threats which risk data exposure in healthcare systems. In 2015, the leading cause of data security breaches may be employees and negligence within an organisation.

Healthcare Data Are Valuable

There are several reasons why healthcare data might be attractive to cyber criminals. In the US, a person's Medicare card contains his or her Social Security number, which can be used to open or access financial accounts. The black market value of healthcare data is consistently high. The problem is made worse by the volume and complexity of healthcare data being generated, and the lack of resources available to smaller clinics, doctors' offices and hospitals.

The upcoming deadline for adoption of "Chip and PIN" security requirements for payment systems in the US could prompt cyber criminals to increase point-of-sale (POS) attacks before the window for compliance closes in October 2015. Payment breaches are therefore likely to increase in the near-term while POS malware may still be effective, according to the Experian report. However, it would be a mistake for consumers and providers to believe that thieves are not currently identifying vulnerabilities in new infrastructures.

The threat of data breaches not only jeopardises patient privacy and safety, but puts healthcare organisations at risk for federal and state scrutiny. In the US, there is no national breach law as of yet, although state regulators are increasingly vigilant about engaging companies on data breach response. Currently, each state has its own requirements for breach notifications, which complicates things for companies whose customer base is drawn from multiple states.

Source: Experian Data Breach Resolution

Image Credit: Pixabay

Published on : Tue, 6 Jan 2015