HealthManagement
Promoting Management and Leadership

Lack of Resources Frustrates Healthcare IT Security

Electronic health records (EHRs) and digital clinical systems have widely been deployed in healthcare without strategic data and IT infrastructure security planning, a report by HIMSS Analytics and Symantec Corporation has said.

“As a result, chief information security officers (CISOs) frequently have limited authority, sparse staffing and tight budgets. Data security spending in healthcare lags behind other top cybercrime targets such as financial services,” the report said.

The research also revealed stolen patient data fetches up to 50 times more than a Social Security or credit card number and criminal attacks on healthcare information systems have increased 125 percent in the past five years.

Last month a Hollywood hospital paid $17, 000 in order to regain access to data after hackers released malware into its IT systems. Hackers from Turkey subsequently claimed responsibility for the attack for political reasons. Shortly afterwards, a ransomware thread was found in computers of the Los Angeles County Department of Health Services although the malware did not spread.

HIMSS16 has put security in the spotlight at its Las Vegas congress this week with panels addressing readiness in the face of a healthcare cyber attack.

The HIMSS and Symantec report brought to light disturbing facts about how healthcare approaches IT security.

In spite of the fact that healthcare is flooded with patient data, out of 115 hospital IT and security personnel polled, only a handful dedicate a significant part of their budget to data security. Other findings were:

See Also: IT Security Complacency High

The majority devote less than 6 percent of IT budgets to data security;

More than fifty percent of polled organisations allocated 3 percent or less of their total IT budget to security last year;

Seventy-two percent of respondents said they have five or fewer IT employees allocated to data security.

Most organisations conduct IT security risk assessments just once a annually;

Only 23 percent have an ongoing, consistent risk-management program;

Most organizations do not provide cyber security awareness employee training and education;

Many security bosses only have occasional interactions with top-level leadership.

“Adding more security products to an enterprise is not the solution. And managing data security with after-the-fact tactical responses instead of proactive strategies to prevent incidents contributes to the enormous financial consequences of each privacy breach,” the report said.

“Chief Information Security Officers have to understand the business, know what the leaders are aiming to accomplish and put together a business plan for security that ties into those business goals,” Mac McMillan

Chairman HIMSS Privacy & Security Policy Task Force said. “The irony is that Information technology and data in healthcare are clearly critical to the mission of providing care, yet data security is an afterthought.”

Source: HIMSS Symantec
Image Credit: Pixelbay

Published on : Thu, 3 Mar 2016