HealthManagement
Promoting Management and Leadership

Only Half of Healthcare Leaders Feel Cyberattack Protected

Eighty-one percent of healthcare executives say their information technology has been compromised by cyberattacks during the past two years, according to a recent survey by KPMG. In addition, only half of those executives say they are ready to defend against future attacks. These attacks may put sensitive patient data at risk of exposure, the KPMG report said.

Compared with previous KPMG polls, the new survey showed that the number of attacks on healthcare IT systems has increased, with 13 percent of respondents saying they are targeted by external hack attempts about once a day and another 12 percent reporting about two or more attacks per week.

"More concerning, 16 percent of healthcare organisations said they cannot detect in real time if their systems are compromised," the report said.

The 2015 KPMG Healthcare Cybersecurity Survey covered 223 U.S.-based CIOs, CTOs, chief security officers and chief compliance officers at healthcare providers and health plans.

The respondents said the main threats to their systems are malware (67 percent) and HIPAA violations (57 percent). The areas with the greatest vulnerabilities within an organisation include external attackers (65 percent), sharing data with third parties (48 percent), employee breaches/theft (35 percent), wireless computing (35 percent) and inadequate firewalls (27 percent).

"The vulnerability of patient data at the nation's health plans and approximately 5,000 hospitals is on the rise and healthcare executives are struggling to safeguard patient records," said Michael Ebert, who runs KPMG's Healthcare & Life Sciences Cyber Practice. "Patient records are far more valuable than credit card information for people who plan to commit fraud, since the personal information cannot be easily changed."

The KPMG report listed five key reasons healthcare organisations are facing increased security threats:

- The adoption of digital patient records and the automation of clinical systems.
- The use of antiquated electronic medical records (EMRs) and clinical applications that are not designed to securely operate in today's networked environment — and software vendors who push that problem to the provider.
- The ease of distributing electronic personal health information both internally (via laptops, mobile devices, thumb drives) and externally (third-party firms and cloud services).
- The heterogeneous nature of networked systems and applications (ie, network-enabled respirator pumps on the same network as registration systems that can browse the internet).
- The evolving threat landscape, where cyberattacks today are more sophisticated and well-funded, given the increased value of the compromised data on the black market.

Source: KPMG
Image credit: Flickr.com

Published on : Sun, 6 Sep 2015