HealthManagement
Promoting Management and Leadership

Expert Tips on Outdated IT Security

It's time to say goodbye to outdated security tools (and beliefs) and shift to a "new era of security". For example, flat networks, compliance-only security and SOC-less security are amongst the items in the "security graveyard".

Healthcare security is in constant flux. One of the biggest ways to shift into this new era of security involves the relationships within the organisation. While most healthcare organisations are aware that involving multiple departments in the security discussion is important, often security work was designated to just one or two people in the past.

This shift requires "series" management, or the need for CISOs to work closely with the operations department, according to Karl West, Salt Lake City-Intermountain Healthcare CISO.

“The relationship with operations is critical to the success of any CISO,” said West. “I create relationships to make security work. Five years ago, this didn’t exist. The security person has never been asked to meet with the CSO or the management community. And today that happens all the time.”

See Also: **Cloud Security Toughest Role for HIT to Fill**

He explained that involves knowing what executives do and do not understand about the technical aspects of security risks.

“If I can explain to them in a few minutes in language they understand,” he continued, “we can be successful at getting funding.”

In addition, West cited the need for organisations to replace some of the outdated security tools used in healthcare, including:

Simple passwords: Passwords like ‘MD’ or ‘1234’ have gone by the wayside. Passwords (hopefully) have increased in complexity, like 8 to 12 characters and special symbols.

Password only: The single password mentality is no longer appropriate. West recommended multi-factor authentication, as passwords and PINs are no longer secure.

Flat networks: Flat networks where everything is connected can facilitate a breach, West pointed out. With the amount of people coming through our system and across the environment, networks need to be segmented.

Cloudless security: Connected devices like unsecured peripherals and medical devices require an increase in security with the use of cloud security to cover all devices.

Compliance "only" security: Reliance on compliance to secure an organisation's network is ineffective. Security is more than checking a box. West stressed the need for encryption and the use of analytics to secure all elements.

SOC-less security: In 2012, Security Operations Centres were optional. Today, however, a SOC is critical. Because of the analytics and rich data Intermountain harvested, events are detected within two to five minutes. Before, it could take up to five months to discover.

Source: Healthcare IT News
Image Credit: Healthcare Informatics

Published on : Mon, 12 Dec 2016