HealthManagement
Promoting Management and Leadership

People: From Security Threat to Line of Defence

Employees are regarded as the lifeblood of an organisation, yet they can also be its greatest cybersecurity threat. Breach reports from IBM and Verizon, as well as other similar surveys, have indicated that people are the greatest vulnerability statistically, according to a technology expert.

See Also: Uptick in Health Data Breaches

“Most of these breaches start by an inside user making a mistake. But 45 percent of all the breaches in the IBM breach report were malicious insiders. The solution is much more holistic than the industry currently thinks, and until we wrap our hands around the people problem, there is no amount of technology that is going to make a dent in breaches," said Kurt Long, founder and CEO of FairWarning, a cybersecurity firm that protects patient information in more than 8,000 healthcare facilities globally.

Fortunately, there are reliable steps that healthcare organisations can take to tackle the people problem:

Vet your next hire. “Vetting can go deep into background checks, making sure people are not on any of the federal fraud lists,” Long said.

Govern and train employees. Ensure the workforce has signed and is aware of the policies of acceptable use for the provider organisation. As for training, this means the workforce is not just trained on acceptable use but also trained to report suspected incidents. It's with this kind of training that workforces "can be transformed to help become a line of defence,” Long pointed out.

Monitor your team. “Monitoring is a trust but verify matter,” Long said. Healthcare workers have access to important data and should be monitored for various scenarios. "For example, you want to statistically monitor is this person well outside the boundaries of what they should normally be accessing," he added.

Identify, track and correlate users. “Organisations have many different applications that touch PHI, and those applications could be legacy systems that they’ve had for a long time, so they don’t have modern user management controls,” Long said. “Or they could have acquired different group practices and brought in different users they have never seen before. Or in the past they simply could have had poor information practices. It all adds up to poor identification, poor governance and poorly trained users; all those users accessing the PHI, organisations don’t really know much about them at all.”

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 9 May 2017