accentureconsulting

ACCENTURE 2018 HEALTHCARE WORKFORCE SURVEY ON CYBERSECURITY

VIDEO TRANSCRIPT

JOHN SCHOEW
MANAGING DIRECTOR, HEALTHCARE SECURITY

The Accenture 2018 Healthcare Workforce Survey on Cybersecurity is about understanding the beliefs, behaviors at attitudes of healthcare employees in US and Canada for both payer and providers. The top three takeaways of the survey were one, we have a major problem. There's a large number of employees that are willing to compromise patient's medical data. Two, training's not enough. We see that training is happening, but it's not being effective. And three, we see an opportunity for healthcare organizations to deploy better and more focused technologies to protect patient data.

Payers and providers should do three things that counter this threat we uncovered in the survey. One, optimize training. Invest in training that's most effective for their organization and their needs. Number two, use multiple techniques to protect data whether it's micro segmentation, tokenization, better privileged access management. These are the things that can improve security and counter the insider threat. Three, constantly monitor and respond to anomalous and suspicious behavior.

These findings point to a significant threat. We know that around 80% of successful attacks in any industry are perpetrated through compromised login credentials. So when we learn that healthcare employees are willing to sell theirs to an unauthorized third party, it's a cause of great concern. So we, in many cases, organizations are constantly looking at the external threat, which is still important. But in healthcare specifically, this survey shows us the insider threat is massively important and one that we must focus on with our training and our technology investments.