# COMPLIANCE VS. SECURITY: WHAT ARE THE DIFFERENCES BETWEEN THESE CYBERSECURITY APPROACHES?

## REZA CHAPMAN
## MANAGING DIRECTOR, CYBERSECURITY, ACCENTURE HEALTH

Healthcare executives, when surveyed, indicated that their confident in their program's ability to provide protections from legal and regulatory downsides. And so the challenge with a program that's designed to deal with those — which we call a compliance-driven program — is it does not provide for the outcome of actual security on the patient or member data that we're talking about.

To me, the difference between a compliance-driven security strategy and security-driven security strategies and the outcome. When we talk about compliance driven programs, we're talking about programs that don't stand up to the test of the attackers. When we talk about a security-driven program, we talk about a program that is designed to deal with the attackers and the threats that they pose to our organizations.

Providers can do a number of things to transition from a compliance-based mindset to a security-based mindset. I think first and foremost, it's to think out of the box. Let's get

Away from worrying about the internal checklists and worrying if this control is in process or not and more focused on what are the risks that we're dealing with? What's important to our organization? Where is our patient data? Where does it live and where is it stored, and what are the protections on that data? And are those protections sufficient?

Payers can transition themselves to a security-focused program from compliance in much the same way as any of the other industry players can do. One of the things I know from a payer perspective, is they've invested tremendous amount of capital over the past number of years since high-profile incidents have taken place, is to make sure that the technologies they've put in place to deal with the risks — so the technical controls that they've purchased, the technologies — are fully supported, fully deployed across their entire enterprise, and not in limited capacities or in some cases, not in unmonitored situations.