WHAT CAN HEALTHCARE ORGANIZATIONS LEARN FROM THE ACCENTURE 2016 HIGH PERFORMANCE SECURITY RESEARCH?

VIDEO TRANSCRIPT
KEVIN RICHARDS
MANAGING DIRECTOR, ACCENTURE STRATEGY SECURITY,
NORTH AMERICA LEAD

So Accenture interviewed 2,000 companies in 12 industries in 15 countries to understand their security capabilities and their security program. The big takeaways from this research is really pretty interesting. First, there was huge amounts of confidence – well over 75, 76% of the respondents felt confident that their cyber security program could protect their critical data assets. And further, would be able to provide significant business value to the enterprise. And then if you drove a little bit deeper, it was in the upper-70s that also said that they had integrated cyber security into the core culture of their enterprise.

So we saw significant confidence. And then we dug a little bit deeper. It’s like, well how well is it actually doing? And what we found is that on average, one out of three focused targeted attacks actually was successful. And when we look at the aggregate over the course of the year, and we average them out, it was basically two to three successful breaches a month. Then if we started looking at the math underneath that... So if the average breach is around $4 million, and I’m having two to three of them a month, the average large enterprise is losing someplace between $8 and $12 million a month due to cyber breaches.

And when we look at these numbers compared to the confidence, obviously we are at different ends of the spectrum. Then we look at it a little bit further, and we ask the question, “Do you have the tools and capabilities to detect a breach and be able to track it as it traverses your enterprise?” Almost two-thirds said they had no tools to actually track a breach once it got through the hard outside layer. So again, we start seeing this big shift, and we call it the conundrum of, “I feel confident.” But the statistics say it’s just not anywhere close.