Security vendors are 'mis-selling' technology - security reseller

Roundtable discussions hear vendors need to earn credibility back for the security sector

Tom Wright

23 November 2016

Cybersecurity vendors need to be more honest about the limitations of their products to help bring credibility back into the security sector, according to security reseller Cognition.

At a cybersecurity roundtable discussion in Dublin, executives from vendors and channel firms waded through the biggest issues in the security market, as high-profile breaches continue to hit mainstream news and a flurry of new VC-backed vendors continue to emerge.

Carl Gottlieb, founder and CTO at reseller Cognition, claimed that it is becoming more and more difficult for resellers to piece together a full security solution for clients because of fragmentation in the market.

"People are buying jigsaws with pieces missing," he said. "People are being mis-sold technology because no vendor will admit where its flaws are. That's the same in anything, whether it be technology [or] buying a house - you don't necessarily say there's a loud road behind the house if you can't see it.

"We need to get credibility back in the industry and we need more vendors to say ‘don't trust us, trust yourself, do more testing'. Try and get away from the sales guy pushing technology onto you."

Gottlieb went on to explain that clients are becoming frustrated when it comes to renewing their security products, to the point where some are losing trust in the channel, and choosing to make their own decisions independently and without the support of vendors and resellers.

In response, the vendors in the roundtable discussion claimed that more often than not security issues stem from end-users themselves, not always maliciously, but because IT managers not qualified in security are being asked to maintain entire networks and cannot always interpret the data.

"Best practices are just not being followed in the industry and we have a problem with just gettin the basics right," said Cylance sales engineering director Lloyd Webb. "We're flogging a dead hors if we think our users are doing the right thing."

"They are constantly doing the wrong thing and I think we have to empower them with some technology to really help them prevent some of these things from taking place.

"You cannot rely on the user to do the right thing - obviously education and awareness is important - but never expect them to the right thing. They'll do the wrong thing and we cannot blame them for that."

The focus quickly shifted to the well-publicised skills gap in the security and wider IT sector, with the government taking criticism for its recently announced $1.9bn security pledge - particularly over its lack of detail on how the funding will be used to address the skills gap.

Anton Grashion, director at Cylance, said the industry itself is partly to blame for the skills shortage because of its constant shift in focus over the last few years.

"We're victims of our industry in some ways because we've chased detail into the network," he said.

"If you think of cybersecurity as the boat - there used to be protection, prevention [on one side]; detection and response [on the other].

"Because protection got worse and worse, we've chased everything over to the other side of the boat so detection and response has tilted over.

"We've actually exacerbated the skills gap by doing that because then we have to hire more people who can actually go and do the detection and response."