https://channellife.com.au/story/gchq-deputy-director-cybersecurity-vendors-need-quit-their-scaremongering/
GCHQ deputy director - "Cybersecurity vendors need to quit their scaremongering"
07/06/16

Ashton Young
June 07, 2017 6AM

We were at the recent NetEvents European Spotlight held in London where the opening keynote was held by three heavyweights in the cybersecurity sector, representing GCHQ, MI6 and Israeli Intelligence.

There were some incredible revelations throughout the keynote about where we currently are in cybersecurity, and what we need to do to move forward.

Without beating about the bush, Brian Lord, OBE and former GCHQ deputy director for Intelligence and Cyber Operations, stated we are far behind where we need to be and it's simply too easy for cybercriminals.

"Criminals are operating in an online sense of being able to walk into the equivalent of a town centre, where everybody's doors are open, windows are open, tills are open, safes are open, cars are left there with the doors open and the keys in and no one is watching," says Lord.

"That is the environment, that's the criminal environment that exists at the moment. So anybody with a basic set of skills can carry out a criminal act. "

Lord asserts there are a few main reasons for the current environment - and why it's not progressing any time soon.

"The IT security industry, information security industry, are all extremely good at saying they have the solution," Lord says.

"Everybody has a shiny box which always is the cyber silver bullet to all cyber problems, but there is no one solution to this problem and there never will be one single solution to this problem."

According to Lord, the constant peppering from vendors asserting they have the 'be all, end all' solution has significantly affected the industry.

"I think it is always worth the IT security industry remembering that there are still a lot of elements of industry, particularly industry who remember 1999, when they were told that planes would fall out of the sky, satellites would spin off into space, screens would go blank and the world would end as we know it," says Lord.

"That didn't happen. So as a consequence, the perception of advice, information from the IT security industry is jaundiced by history. Selling by fear never works."

Lord says every outbreak means big money for cybersecurity vendors - they made an absolute fortune in 1999, and Lord is confident they will again following the recent attacks.

"So what we are looking at now, what we are looking at now, is an environment where nobody really understands what they have to protect themselves from, nobody really understands why they are at threat or from whom," says Lord.

"So as a consequence, we end up with decision-making stasis, decision-making stasis at industry level, where organisations don't know what to buy, CEOs, CFOs don't know what to believe and so as a consequence, nobody invests in anything."

Lord says the solution is clear reporting and concise reporting of what enterprises are actually in threat of, and the simple things they need to do to protect themselves - starting with the basics.

"All we need is a responsible IT security market to sell basic tools, advise on basic control measures and basic education and in effect, the vast majority of that problem will go away and it will leave," says Lord.

"Do the basics right and a business' risks go down by about 80-90 percent."