Making the board buy-in for security

Security breaches happen all the time. In fact, barely a day goes by without a story in the news about new victims, whether it's a bank, retailer or publishing house.

©goodluz via 123RF

In addition, surprisingly, most company's boards are not included in the decision processes and strategies controlling IT security, risk and privacy, says Lutz Blaeser, MD of Intact Software Distribution. "The majority of the time, these decisions are left to the CIO, as security is viewed as being purely technical, and an issue that be resolved merely by having the right products and solutions in place. Security issues are dropped in the CIOs lap and the board assumes there is no further need for its involvement."

It's not just a technical issue

Unfortunately, he says this pretty basic misconception can carry with it catastrophic ramifications. "C-level executives must be made to understand that information security risks cannot be solely under the purview of the CISO or CIO. These issues affect the entire organisation as a whole, and the implications are enterprise-wide. The issues involved here are far beyond technical alone. Particularly where advanced threats are concerned, it can take hundreds of days to realise that a breach has occurred and the network has been compromised."

Usually, by the time a breach has been discovered, the attackers have been lurking on the network, scoping out the scene for weeks, and have already exfiltrated the data they were after. "Remember too, that the fallout from an attack goes far further than data alone - loss of reputation, loss of customer confidence and similar, could have far reaching and disastrous consequences for the business," Blaeser says.

Making executives understand

No company in its right mind can seriously contend that these sort of issues do not affect the board or the shareholders, he adds. "However, many technical heads will tell you that bringing the C-level executives in to a meeting to discuss the broader security strategies is an enormous mission itself, as these individuals are always busy and preoccupied with their own business initiatives. We need to make the executives understand that the business plan, investment strategy and the overarching information security strategy align. We need to make them acknowledge that they play a pivotal role in the security strategy as they do in any other large technology strategy or investment."

To do this, he advises posing several questions to them. "What is our appetite for risk? Do we need just enough security to be compliant, or do we want the best in place to prevent attackers from breaching our networks? How much security is enough?"

In addition, Blaeser says the executives must be made to understand the threat landscape, and how quickly it is evolving in terms of both threats and their sophistication. "Make them realise that a determined enough attacker will eventually get in. Breaches are inevitable, so ensure that the majority of security efforts are focussed on the most valuable data assets."

Arguing for security

There are not only compromised systems at play here; the financial implications should a breach occur and the company be found non-compliant are massive, often resulting in a company name taking a beating it cannot recover from. "This is compounded with legal risks from regulatory non-compliance and customers leaving in droves, so make sure these points are central to your argument."

Today, discussions around business risk must include conversations about information security and cyber risks. "They cannot be viewed in isolation of each other. They are not separate issues, and companies who treat them this way are in for a nasty surprise. Executives must be involved in cyber security policy, and must grasp enough about their company's security and the threat landscape as a whole, to get shareholders' buy in," Blaeser concludes.