http://www.itweb.co.za/index.php?option=com_content&view=article&id=137961:Cyber-security-a-CEO-concern-&catid=234

Cyber security 'a CEO concern'

Portugal, 26 Sep 2014

Company CEOs should be just as concerned about bolstering cyber security as CIOs if telcos are to build a truly robust framework for their businesses.

IT security should be a concern for all top management, say NetEvents speakers.

This is the view held by Jan Guldentops, a researcher and security consultant at Belgium-based BA Test Labs, who was addressing delegates at the NetEvents Press and ServiceProvider Summit in Portugal.

While strong IT security measures are important for any telco's success in its core business, added Guldentops, top management should turn away from the tendency to assign the company's security strategy to a small section of its leadership. He said security should be as important a strategy as decisions taken collectively by management.

"There is only one real security product – that is common sense. Many companies have attitudes looking at giving [responsibility] to someone else, particularly specialists like CIOs, while CEOs don't have to think about it, but this is not how it should be.

"At times, tech companies most arrogant about security measures are the ones that have the biggest holes and get hacked for something as simple as trivial passwords for their systems."

Guldentops added that a proactive approach means consistently revisiting existing frameworks and framing thinking around "should I be hacked" to "when I get hacked" in a bid for companies to stay ahead of the curve.

Plugging holes

Jordi Gascon, senior director at CA Technologies, says swiftly recovering from security breaches involves as much pre-hacking preparation as the measures taken afterwards. "If you don't fully understand the detailed technical nature of your breach, you will be fixing problems without properly addressing their root cause.

"Without knowing what was the exact state of your environment or servers before the breach, you are setting yourself up for more problems in the long-run."

Guldentops added that a lack of sophisticated intrusion detectors "paralyses" organisations as they struggle to define whether they are free from attacks. Having the right personnel and knowledge in-house can also place a burden on operational costs, he said.