EIN PRESSWIRE

Cyber security breaches can go undetected, IT Governance’s Cyber Watch Boardroom survey finds

36% of respondents who took part in the Boardroom Cyber Watch survey believe that their company could have suffered an undetected cyber attack in the past year.

ELY, CAMBRIDGESHIRE, UK, July 8, 2014 /EINPresswire.com/ -- 36% of the respondents who took part in the Boardroom Cyber Watch 2014 survey believe that their company could have suffered an undetected cyber attack in the past year, and almost 20% didn’t know. This means that more than 56% of the respondents though it possible for their company to have suffered a breach without it being detected.

This is a key finding of the Boardroom Cyber Watch 2014 Survey, the second annual international survey of senior executive opinion conducted by IT Governance, a global cyber security provider and CREST member.

The above findings are complemented by the results from another survey - the Mandiant M-Trends® Report 2014 - which found that the average number of days that attacks were present on a victim’s network before being discovered was 229 – more than seven months.

Alan Calder, Founder and Executive Chairman of IT Governance says, “For breaches to go undetected for months is a very dangerous matter. In the worst of scenarios it may mean the end for an organisation. In June, we saw Code Spaces forced out of business due to a targeted cyber attack, while more than 190 customers of a European bank have been robbed by cyber thieves who operated in a very sophisticated manner and deleted all evidence leading to them.”

Cyber criminals are indiscriminate, and all Internet-facing organisations are potential victims. Yet, the Boardroom Cyber Watch 2014 Survey revealed that 73% of the respondents believe that their current information security defences are effective at repelling cyber attacks.

Calder explains, “The high level of complacency, compared to the high level of uncertainty over whether or not an organisation has been breached, shows that in many cases, the organisations’ belief that they are secure against attack is likely to be unfounded. It can and will expose them to the sort of existential threat that forced Code Spaces out of business.”

While organisations should ensure that they have a well-practiced and proven recovery plan in place, they should also conduct penetration testing on their networks and web applications to identify any security gaps and vulnerabilities. This will also give organisations better confidence that they are able to detect and protect themselves from cyber attacks.

Geraint Williams, QSA and Senior Consultant at IT Governance, says, “Organisations are at a significant risk from attacks through automated botnets and automated scanning tools that test the ‘attack surface’ to see if there are any vulnerabilities that can be exploited. Any successful attack will incur significant remediation costs, loss of productivity and reputational damage. ‘Not testing’ could be a very costly process.”

More information on IT Governance’s penetration testing packages is available here: www.itgovernance.co.uk/penetration-testing-packages.aspx.

A copy of the full Boardroom Cyber Watch 2014 report is available here: www.itgovernance.co.uk/boardroom-cyber-watch.aspx.

Desislava Aleksandrova
IT Governance Ltd
00448450701750
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.

© 1995-2018 IPD Group, Inc. All Right Reserved.