Public-private survey: US cybercrime on the rise

May 28 2014, by Martha Mendoza

The hackers are winning, according to a survey of 500 executives of U.S. businesses, law enforcement services and government agencies released Wednesday.

The 12th annual survey of cybercrime trends found that online attackers determined to break into computers, steal information and interfere with business are more technologically advanced than those trying to stop them.

The survey was co-sponsored by San Jose, California-based business consulting firm PwC, the U.S. Secret Service, the CERT Division of Carnegie Mellon University's Software Engineering Institute and CSO security news magazine.

Three out of four respondents said they had detected a security breach in the past year, and the average number of security intrusions was 135 per organization, the survey found.

"Despite substantial investments in cybersecurity technologies, cyber criminals continue to find ways to circumvent these technologies in order to obtain sensitive information that they can monetize," Ed Lowery, who heads the U.S. Secret Service's criminal investigative division, said in a written statement.

Lowery said companies and the government need to take "a radically different approach to cybersecurity," which goes beyond antivirus

software, training employees, working closely with contractors and setting up tighter processes.

The top five cyberattack methods reported in the survey were malware, phishing, network interruption, spyware and denial-of-service attacks. And 28 percent of respondents said the attackers were insiders, either contractors or current and former employees or service providers, according to the survey.