Survey Finds That 85 Percent of Workers Know It's Illegal to Steal Corporate Data, Yet Many Are Willing to Risk the Consequences

November 23, 2009 4:38 AM ET

*Research Shows 41 Percent of Workers Admit to Taking Sensitive Data with Them to a New Employer, While a Quarter Would Steal Information to Help a Friend Get a Job*NEWTON, Mass. - November 23, 2009 - Stealing employer data has become endemic in our culture. According to a survey conducted with 300 office workers in New York City examining the impact of the recession on ethics and security, 85 percent of the respondents admitted to knowing that downloading corporate information from their employer was illegal, yet a quarter of those surveyed would take the data regardless of the penalties. In fact, 41 percent of respondents have already taken sensitive data with them to a new position, while 26 percent would pass on company information if it proved useful in getting friends or family a job.The second annual "Global Recession and Its Effect on Work Ethics"transatlantic survey also polled 300 office workers in London, asking the same set of questions for comparison. What's clear in the US data is that the recession has shaken employees' confidence, with a quarter of total respondents admitting to feeling less loyal toward their employer. Despite this, only 40 percent of respondents are worried about losing their jobs, compared to 52 percent in 2008. The survey was sponsored by Cyber-Ark SoftwareÂ®, the Privileged Account Management specialists.Corporate Data Protection Continues to Lag: Sensitive Data is Easy to Access, Easy to ShareProtection of corporate data continues to lag, with 60 percent of those surveyed admitting that it is easy to take sensitive information from under their bosses noses - with the primary tool of choice remaining a portable storage device like a memory stick, USB flash drive or CD, followed by email and then paper coming in a close third.The survey found that 26 percent of the respondents admit that if they were fired tomorrow they would take company information with them, and 24 percent of people would download company/competitive information if there were rumors that their job was at risk. Of those who plan to take competitive or sensitive corporate information:

- 52 percent admit they would do so "just in case" the data were to prove useful or advantageous in the future
- 28 percent would use the data to negotiate their new position
- 28 percent plan to use the data as a tool in their new job

Tops on the hit list of information that people like to download is customer and contact details (23 percent), followed by access and password codes (11 percent). Other information that is coveted includes product information, plans and proposals. This is particularly worrying as, without the proper identity and access management solutions in place, many ex-employees can still get into the network to access content and download information long after they've left the building.Lack of Job Security Leads to Risks and CompromiseWith remaining concern about job security, 23 percent of respondents revealed that they would do their utmost to sneak a look at the "lay-off list" to find out if their name was on it, with a whopping 70 percent using their own IT access rights to snoop around the network to find additional information. If they couldn't find out the information on their own, 24 percent would approach a colleague in IT to get the inside information. Eleven percent of respondents indicated they would consider bribing human resources to reveal if their jobs were on the line.Respondents were also asked what steps they would take to keep their jobs. According to the survey:

- 50 percent of US respondents would take a salary cut to keep their jobs, compared to 20 percent of UK respondents
- 25 percent of UK respondents indicated they would work up to 80 hours a week to keep their jobs, compared to just 12 percent of US respondents

"While we are seeing glimmers of hope in the US economy, clearly employee confidence has been rocked. This survey shows that many workers are willing to do practically anything to ensure job security or make themselves more marketable - including committing a crime," Adam Bosnian, vice president of products and strategy, Cyber-Ark Software. "While there is no excuse for employees who are willing to compromise their ethics to save their job, much of the responsibility for protecting sensitive proprietary data falls on the employer. Organizations must be willing to make improvements to how they monitor and control access to databases, networks and systems - even by those privileged

users who have legitimate rights. Additional protection can be added with simple steps like frequently changing passwords and only granting access to certain information on-demand."Note to editors: The "Global Recession and Its Effect on Work Ethics" survey was conducted for a second year by Cyber-Ark Software during November 2009 among 300 office workers in Canary Wharf, London and 300 office workers on New York City's Wall Street by independent researchers.**About Cyber-Ark**Cyber-ArkÂ® Software is a global information security company that specializes in protecting and managing privileged users, applications and highly-sensitive information to improve compliance, productivity and protect organizations against insider threats. With its award-winning Privileged Identity Management (PIM) and Highly-Sensitive Information Management software, organizations can more effectively manage and govern application access while demonstrating returns on security investments. Cyber-Ark works with 600 global customers, including more than 35 percent of the Fortune 50. Headquartered in Newton, Mass., Cyber-Ark has offices and authorized partners in North America, Europe and Asia Pacific. For more information, visit www.cyberark.com.

Monday, November 23, 2009 - 13:30