Global IT Security Survey Finds Insider Snooping on the Rise

June 10, 2009 3:26 AM ET

Recession Sees More Than a Third of IT Staff Admit to Abusing Admin Rights to Look at Confidential Information; 74 Percent Able to 'Get Around' Controls Designed to Protect Sensitive Data

Newton, Mass. and LONDON - June 10, 2009 - Twelve months after the Cyber-Ark "Trust, Security & Passwords" survey discovered that 33 percent of IT staff used their IT administration rights to snoop around networks to access privileged, corporate information such as HR records, layoff lists, customer databases and M&A plans, a repeat of the survey has discovered that the situation has escalated. Despite a sharp rise in data breaches and increased media awareness on the subject, the third annual Cyber-Ark survey reveals that 35 percent of IT workers now admit to accessing corporate information without authorization, while 74 percent of respondents stated that they could circumvent the controls currently in place to prevent access to internal information.

Cyber-Ark's "Trust, Security & Passwords" is a global survey of more than 400 senior IT professionals both in the US and UK, mainly from enterprise class companies.

Sensitive Data in Danger with More Jobs in Jeopardy

One of the most revealing aspects of the survey was found in the types and quantity of information employees would take with them if they were fired. As the economic climate has worsened, the survey found a sharp increase in the number of respondents who say they would take proprietary data and information that is critical to maintaining competitive advantage and corporate security. When asked this year "What would you take with you," the survey found a six-fold increase in staff who said they would take financial reports or merger and acquisition plans, and a four-fold increase in those who would take CEO passwords and research and development plans. Of the information targeted, respondents indicated they would be most likely to steal the following types of information:

Type of Information	2009	2008
Customer Database	47%	35%
Email Server Admin Account	47%	13%
M&A Plans	47%	7%
Copy of R&D Plans	46%	13%
CEO's Password	46%	11%
Financial Reports	46%	11%
Privileged Password List	42%	31%

Ominously, 1 in 5 companies admit having experienced cases of insider sabotage or IT security fraud. Of those companies, 36 percent suspect that their competitors have received their company's highly sensitive information or intellectual property.

Current Privileged Account Controls Deemed Ineffective

Organizations are increasingly aware of the need to monitor privileged account access and activity, with 71 percent of respondents indicating that privileged accounts are partially monitored, while 91 percent of those who are monitored admitting they are "okay with their employer's monitoring activities." Despite these efforts, 74 percent of respondents revealed that even with the controls being put in place to monitor them, they could still get around them, making current controls ineffectual.

Highlighting the ineffectiveness of current controls and access policies, 35 percent of IT administrators admitted they were using their administration rights to snoop around the network to access confidential or sensitive information. The most common areas respondents indicated they access are HR records, followed by customer databases, M&A plans, layoff lists and lastly, marketing information.

"This survey shows that while most employees claim that access to privileged accounts is currently monitored and an overwhelming majority support additional monitoring practices, employee snooping on sensitive information continues unabated. Unauthorized access to information such as customer credit card data, private personnel information, internal financial reports and R&D plans leaves a company vulnerable to a severe data leak with the risk of financial or regulatory exposure and damage to its brand, or competitors obtaining critically important competitive information," said Udi Mokady, CEO of Cyber-Ark. "Cyber-Ark is committed to raising awareness around the risk of unmanaged privileged accounts. While seemingly innocuous, these accounts provide workers with the 'keys to the kingdom,' allowing them to access critically sensitive information, no matter where it resides. Businesses must wake up and realize that trust is not a security policy; they have an organizational responsibility to lock down sensitive data and systems, while monitoring all activity even when legitimate access is granted."

Note to editors:
This survey was conducted with more than 400 IT administrators at Infosecurity Europe 2009 and RSA USA 2009. To download a PDF of the findings, please visit: www.cyberark.com

For more information about this survey or to interview Cyber-Ark on their findings, contact Yvonne Eskenzi at +44(0)20 71832 832 or email Yvonne@eskenzipr.com.

About Cyber-Ark

Cyber-ArkÂ® Software is a global information security company that specializes in protecting highly-sensitive enterprise data and restricting access to privileged accounts and applications to improve compliance, productivity and guard against insider threats. With its 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 to the C-suite. Cyber-Ark's award-winning technology is deployed by more than 500 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.

Wednesday, June 10, 2009 - 13:15