Cyber-Ark Addresses Special Challenges Facing Government Agencies as They Work to Combat Insider IT Security Threats

May 20, 2009 3:27 AM ET

Newton, MA - 20th May 2009 - High profile insider breach incidents, such as the arrest of a former Federal Reserve Bank of New York IT employee accused of identity theft, and the rogue Fannie Mae employee who allegedly implanted a logic bomb on the company's network, highlight increasing security vulnerabilities in the public sector. To better protect highly sensitive information against internal and external threats, Cyber-Ark recommends government agencies more closely examine how powerful privileged accounts, those with carte blanche access to critical networks, systems and applications, are being monitored and controlled.

Up to 80 percent of system breaches are caused by internal users, including privileged administrators and power users who accidentally or deliberately damage IT systems or release confidential data assets, according to a Cyber-Ark survey. These accounts are often neglected and session activities are difficult to monitor due to their anonymous nature, while privileged passwords can be hard coded inside applications, scripts and parameter files, leaving them unsecured, rarely changed and visible to the world.

The risk of internal data misuse can be significantly mitigated by implementing policies and technologies that provide special treatment for privileged identities. In accordance with newly-proposed Consensus Audit Guidelines, which suggest automated and continuous control of administrative privileges, Cyber-Ark helps government agencies successfully address the security threat of privileged accounts and related audit challenges.

"Mismanagement of privileged identities poses serious risks to organizations - in both the public and private sectors - leaving them vulnerable to threats that can be nefarious in nature, or simply caused by human error," said Udi Mokady, president and CEO of Cyber-Ark Software. "Additionally, these privileged accounts are increasingly scrutinized by auditors, and are becoming one of the key reasons that many organizations fail compliance audits. Therefore, agencies must demonstrate more effective control over who has access to powerful privileged accounts and what activities occur during those privileged sessions."

Cyber-Ark's products were recently added to the US Government Services Administration (GSA) Schedule. Through its agreement with government distribution partner DLT Solutions, Inc., Cyber-Ark's award-winning Privileged Identity Management Suite v5.0 and Managed File Transfer solutions are now broadly available to federal, state and local agencies. Cyber-Ark's recently released Privileged Identity Management Suite v5.0 is the industry's most comprehensive solution for securing, managing and monitoring all activities associated with powerful privileged accounts, including both administrative and application identities. It features the Privileged Session ManagerÃ¯Â¿Â½ that provides sensitive session monitoring and recording with DVR-like playback.

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, May 20, 2009 - 13:00