Cyber-Ark Asks: What's Changed in IT Security Since the Terry Childs Network Lockout Incident?

July 20, 2009 3:23 AM ET

Recent High-Profile Insider Breach at Goldman Sachs Highlights the Continued Struggle with Monitoring and Controlling Privileged Accounts

NEWTON, Mass - July 20, 2009 - One year after former San Francisco IT administrator Terry Childs was charged with using a privileged account to lock down the city's network, organizations are still struggling to monitor and control privileged accounts. Recent high-profile, insider-related incidents, including the Goldman Sachs employee who allegedly stole proprietary trading software, and the Quantum Technology Partners employee who was sentenced to jail for using an administrative password to breach the company's network and shut down its servers, serve as harsh reminders of the security vulnerabilities organizations continue to face despite elevated awareness.

These cautionary tales underscore the need for management to effectively take ownership of privileged accounts and identities that provide access to critical networks, systems and applications to prevent similar damaging and costly breaches from happening within their own companies. Cyber-Ark addresses the problematic trend of insider breaches attributed to mismanagement of privileged accounts and identities, such shared administrative accounts and embedded application passwords, and how companies can better manage and monitor the power they provide to administrative users.

"The Terry Childs case served as a wake-up call on the power a privileged user wields in an organization. Unfortunately, many companies still don't believe they have an issue, or simply haven't taken the steps to address the underlying problems," said Adam Bosnian, vice president of products and strategy at Cyber-Ark Software. "Too often, we look at these incidents through the prism of the rogue employee, when, in fact, the vast majority of IT administrators are trustworthy. The continued prevalence of privilege-related breaches can be attributed to the failure of organizations to uphold their responsibility to manage, control and monitor the power they provide to their employees."

Insiders Remain a Pervasive Threat
Despite a sharp rise in data breaches and increased media awareness on the subject, many organizations still fail to protect privileged accounts and identities that provide access to their most sensitive files, devices and databases. In fact, Cyber-Ark's third annual "Trust, Security & Passwords" survey revealed that 35 percent of IT workers now admit to accessing corporate information without authorization.

The root cause of this internal threat is that privileged accounts convey broad and deep access privileges that cannot be traced to a specific person. They 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 and rarely changed. The mismanagement of shared administrative accounts and embedded passwords is also one of the main reasons why companies fail compliance audits.

To better protect against insider threats, organizations must ensure that administrative and application identities and passwords are changed regularly, highly guarded from unauthorized use and closely monitored, including full activity capture and recording. By automating these tasks, passwords are automatically refreshed at regular intervals, and they are disabled immediately when an employee leaves the company. Cyber-Ark's 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.

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.

Monday, July 20, 2009 - 13:15