CyberArk Global Survey Shows External Cyber-Security Risks Will Surpass Insider Threats

April 14, 2011 3:36 PM ET

57 Percent of C-Level Executives Agree That Cyber-Crime Will Eclipse Insider Security Risks Within Three Years

NEWTON, Mass. and LONDON -- April 14, 2011 Results of CyberArkÂ® Software's fifth annual â€œTrust, Security and Passwordsâ€™survey show that 57 percent of global C-level executives agree that in the next one-to-three years, external threats such as cyber-criminals will become a greater security risk than insider threats. In addition to the growth of external threats, 16 percent of C-level respondents believe that competitors may have received highly sensitive information or intellectual property including customer lists, product information and marketing plans from sources within their own organization. Of note, this response doesn't take into account other external forces, beyond the competitive threat, that may also be motivated to seek access to similar information, such as IP thieves, sabotage or targeted , sophisticated APT type attacks..

CyberArk's fifth annual â€œTrust, Security and Passwordsâ€™global report is the result of online surveys conducted in the Spring of 2011 with 1422 IT managers and C-level professionals across North America and EMEA, primarily from enterprise-class companies. This is the first year CyberArk extended the survey to the C-suite. The overall expanded sample set impacts benchmarking against previous years' data, but provides a broader view of industry trends to track in future reports.

â€œThe increased awareness that attack vectors can and do originate from both external and internal sources can be attributed in large part to the spectacular external-born breaches that drew headlines in the past year, including the NASDAQ and Gawker breaches. Regardless of the attack vector, the targets inside an enterprise remain the same - highly sensitive intellectual, financial and customer information,â€™said Adam Bosnian, executive vice president Americas and corporate development, CyberArk Software. â€œPrivileged accounts are the key tool that external attackers and insiders leverage to access and exfiltrate an organization's sensitive information. While the survey shows a greater awareness around protecting these targets from attacks from any vector, it's concerning that nearly 1 in 5 of C-level respondent believe that their corporations sensitive information may be being used against them in the market. Security teams need to start with improving the protection of these key internal targets - not simply building bigger walls around the enterprise.â€™

The Temptation to Snoop Remains: Examining North American and EMEA Habits
With recent high-profile breaches that took advantage of privileged accounts and passwords, like RSA SecurID, awareness and a sense of urgency will continue to increase around the need to better monitor and control those powerful accounts. Specific results from global IT managers surveyed found that:

- More than half (64 percent) said their use of privileged accounts is currently being monitored.
- Of those with privileged account monitoring, 40 percent of respondents said they could get around controls that monitor privileged access.
- Nearly one in five (18 percent) agreed that they had cases of insider sabotage or IT security fraud at their workplace.

The following results compare â€œsnoopingâ€™habits of IT managers around the world:

- When asked if they had ever accessed information on a system that was not relevant to their role, 28 percent of North American respondents admitted to snooping, while an even greater number in EMEA, 44 percent, admitted to the same behavior.
- Similarly, 20 percent of North American respondents and 31 percent of EMEA respondents said that they or

one of their colleagues had used an administrative password to access information that was otherwise confidential or sensitive.

A response that has remained fairly constant over the years is identifying the departments most likely to snoop around the network to look at confidential information. With their broad reach and responsibility for managing various networks, systems and applications, 48 percent of all global respondents chose the IT department as the most likely to snoop. Respondents said that managers were the next most likely (10 percent) followed by human resources (7 percent).

The Impact of Data Breach Laws and Regulations on Privileged Account Perceptions
A new question added to this year's survey focused on measuring how respondents' perception of privileged account security has changed in light of data breach notification laws. According to the results, 77 percent of North American IT managers said their perceptions have changed, while much fewer in EMEA, 24 percent, felt the same way.

â€œWe expected some differences between North American and EMEA respondents, and thought this gap was noteworthy in that it speaks to differences between the regions in terms of how data breach notifications are enforced - either by law in places like the U.S., or as a regulation in the U.K. Regardless, several recent reports have cited escalating fines associated with breaches, so it will be interesting to watch how perceptions change over time,â said Bosnian.

Managing Privileges in the Cloud
In another newly-added survey question, CyberArk found that 57 percent of global C-level respondents currently utilize a virtualized or cloud-based computing environment. When asked if they had technologies in place to mange administrative access to the databases and systems in those environments, the majority said yes, though approaches varied. Solutions included Security Information and Event Management (SIEM) and Digital Asset Management (DAM) tools or VMware.

Note to editors:
This online survey was conducted with 1422 IT managers and C-level professionals across North America and EMEA. For the most part, the C-level responses were in-line with their colleagues, though it will be interesting to track where differences of opinion grow, especially related to securing new virtualization technologies and being held liable for data breach reporting and increasing fines. To view a detailed report of the survey results, please download datasheet.

About CyberArk

CyberArkÂ® Software is a global information security company that specializes in protecting and managing privileged users, applications and sensitive information to improve compliance, productivity and protect organizations against insider threats and advanced external threats. With its award-winning Privileged Identity Management, Sensitive Information Management and Privileged Session Management Suites, organizations can more effectively manage and govern data center access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments. CyberArk works with more than 850 global customers, including more than 35 percent of the Fortune 100. Headquartered in Newton, Mass., CyberArk has offices and authorized partners in North America, Europe and Asia Pacific. For more information, visit www.cyberark.com.

Thursday, April 14, 2011 - 14:00