



2009 Trust, Security & Passwords Survey Research Brief

June 10, 2009

Research Brief

2009 Trust, Security & Passwords Survey

This global “snooping” survey is the third in a series of benchmark studies focused on identifying security and privacy trends among IT workers. Results are intended to raise awareness about the risks associated with powerful, and often unmanaged, privileged users and passwords. While seemingly innocuous, these accounts provide workers with “keys to the kingdom,” allowing them to access critically sensitive information, no matter where it resides. This unauthorized access to information such as customer credit card data, private personnel information, internal financial reports and R&D plans can leave a company vulnerable to a severe data leak; risks include financial or regulatory exposure, and damage to the organization’s brand or competitive positioning. The survey of more than 400 senior IT professionals, mainly from enterprise class companies, was conducted at Infosecurity Europe 2009 and RSA USA 2009.

Key Findings

Sensitive Data in Danger with More Jobs in Jeopardy

Despite a sharp rise in data breaches and increased media awareness on the subject, the third annual Cyber-Ark survey reveals that 35 percent (see Figure 1) of IT workers admit to accessing corporate information without authorization. This number is up from 33 percent in 2008.

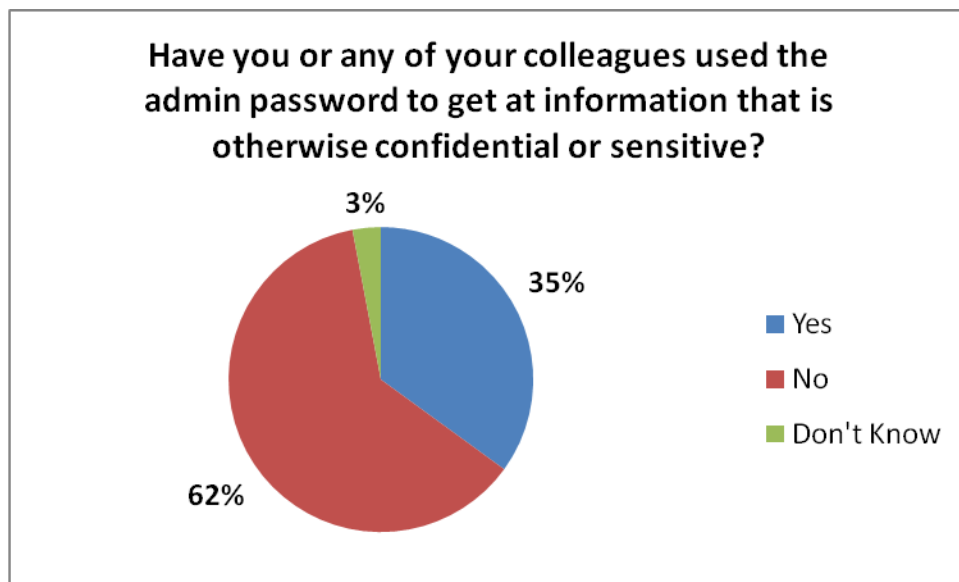


Figure 1

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. In fact, 74 percent of respondents stated that they could circumvent the controls currently in place to prevent access to internal information.

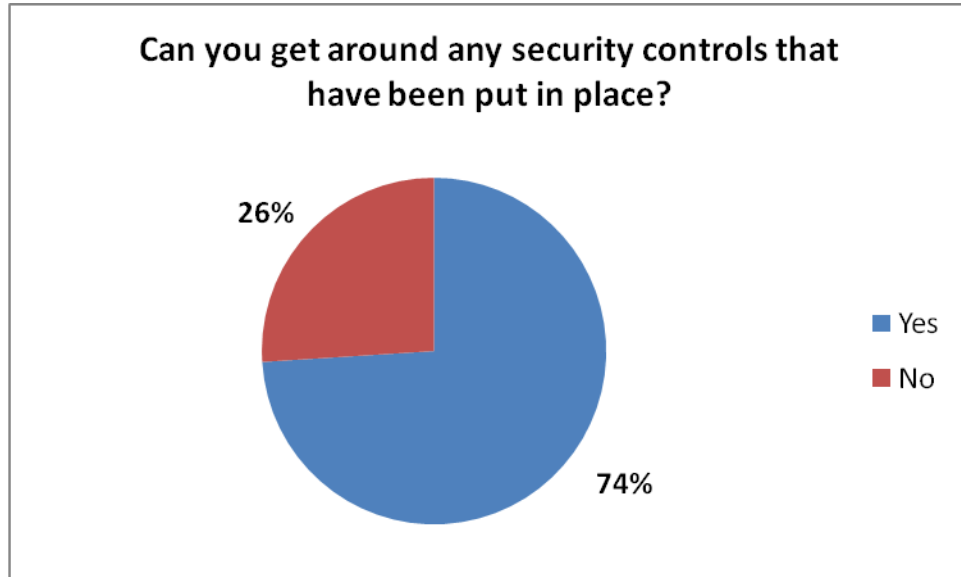


Figure 2

The following graphic (Figure 3) details the types of information that are commonly being accessed using admin passwords. HR records and the customer database were the most popular.

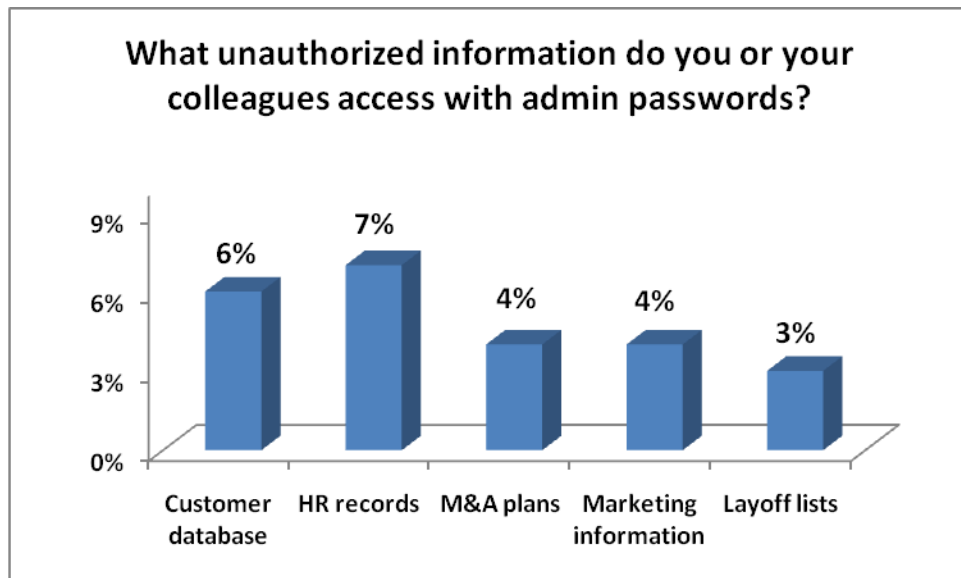


Figure 3

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.

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%

Figure 4

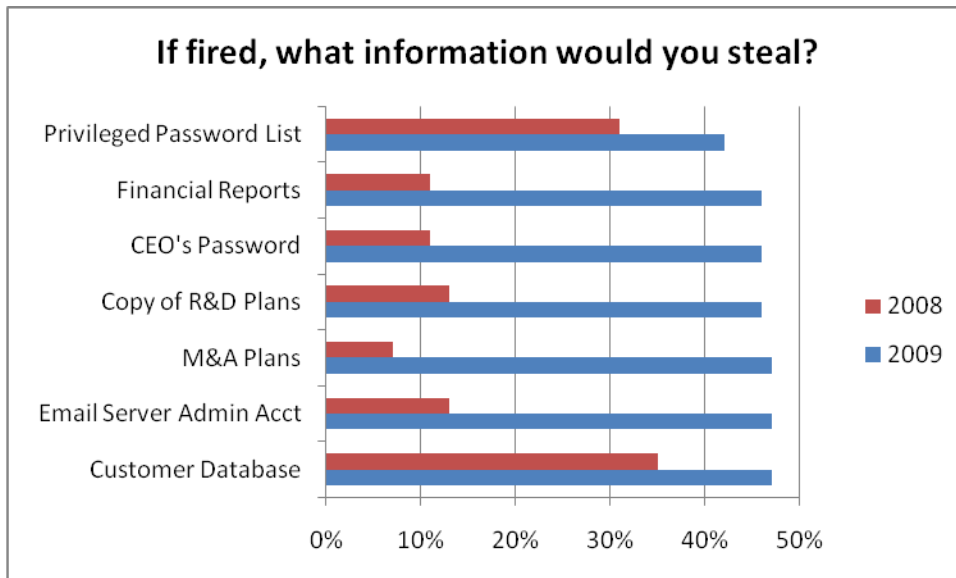


Figure 5

Additionally, 1 in 5 companies admit having experienced cases of insider sabotage or IT security fraud (Figure 6). Of those companies, 36 percent suspect that their competitors have received their company's highly sensitive information or intellectual property (Figure 7).



Figure 6

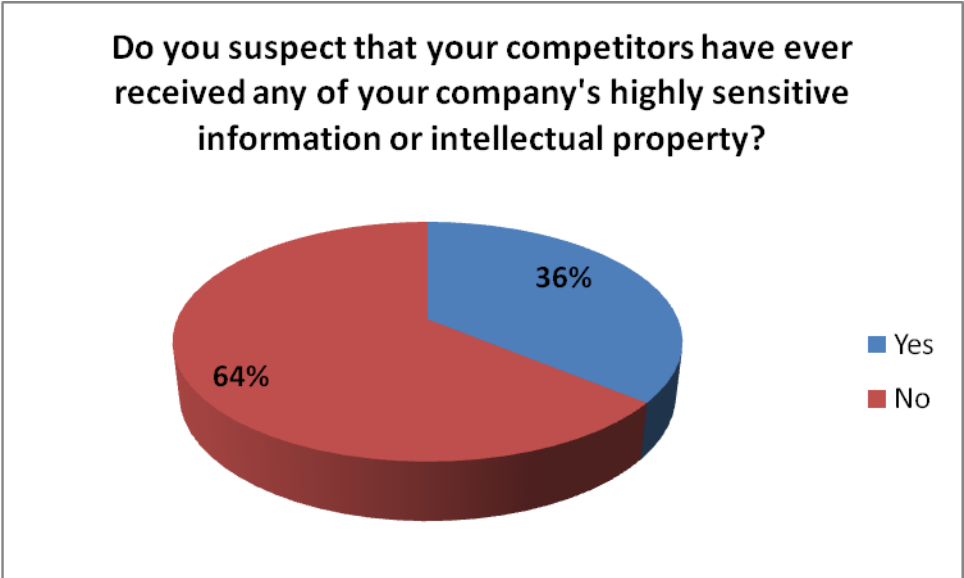


Figure 7

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.”

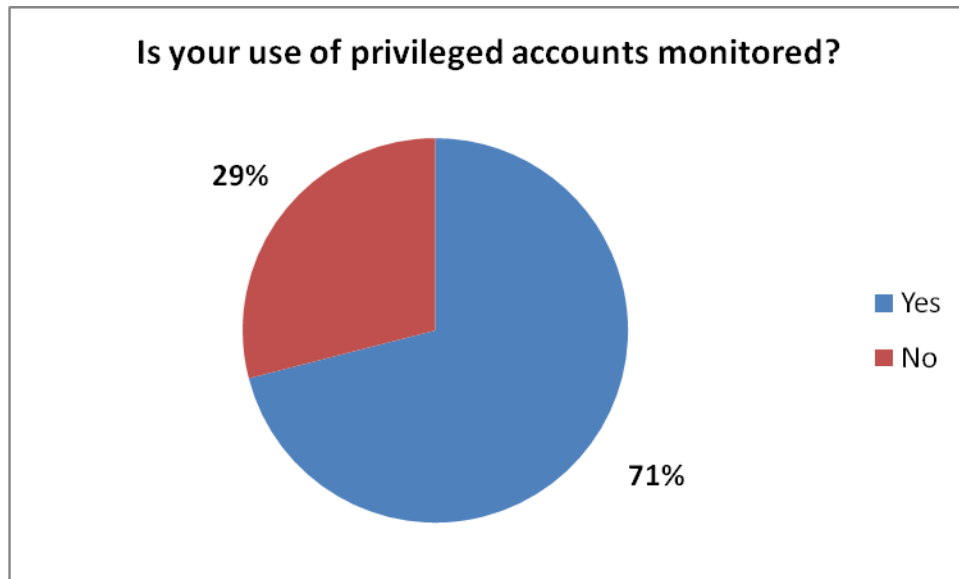


Figure 8

Other Notable Findings

When asked if respondents had systems in place to allow them to send large or sensitive files, 80 percent said yes. The most popular systems were FTP (43 percent), Secure email (32 percent) and Email (20 percent).

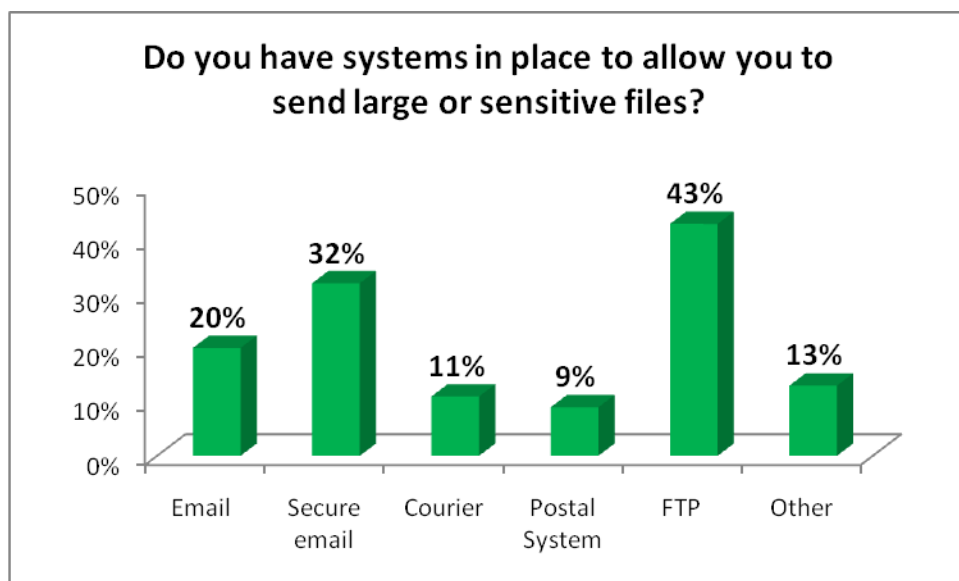


Figure 9

About Cyber-Ark

[Cyber-Ark® Software](#) is a global information security company that specializes in protecting highly-sensitive enterprise data, restricted user and application accounts 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 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.cyber-ark.com.