

28 August 2008

By: Denisa Ilascu, Internet / SEO News Editor



IT professionals are not the honest persons we believe they are  
sfx.ac

## **IT Professionals Snoop Around Employees' Personal Information**

### *And would use confidential data after being dismissed*

According to a survey conducted by Cyber-Ark Software among 300 IT security professionals, 88% of them would take sensitive information with them if they were to be fired from their jobs. Only the remaining 12% of them said that they would not take advantage of the security breaches made possible by the companies that don't cut the access of former employees to the internal network of the company. Some of the information to which IT professionals still have access after being dismissed is related to privileged and regular passwords (the former granting access to all the information within the network), customer databases, research, development, merger or acquisition plans or financial reports.

Although rather naive in their approach to protecting their servers from what a former employee, who was either fired or willingly quit, would do, companies fear industrial espionage and data leakage. In fact, one third of the respondents believes that these threats are abundant nowadays. However, the same percentage of current employees in charge with the security system of an enterprise makes a habit out of writing privileged passwords on post-its, which is the least secure of all methods to store sensitive information. Other intriguing findings of Cyber-Ark Software are related to the way IT professionals send confidential data. 35% of them do it by email, which is known to be one of the means most targeted by hijackers. Yet another 35% send the encrypted data by courier, while 4% of the respondents use the postal mail system to deliver it. All these are very likely to contain security flaws that would allow third parties to intercept and use internal information for malicious purposes. One third of the people queried admitted to poking their nose into the affairs of other employees, thus reading personal emails, finding out salary details, and so on and so forth. "You can install the best security systems in the world, but if your staff does not respect the information they are entrusted with, then the information will most definitely go astray - just as the findings of this survey have illustrated," says Udi Mokady, president and CEO of Cyber-Ark. "That's why we recommend companies secure their privileged identities and sensitive information in a digital vault - only giving individuals access to the information they actually need, when they need it while also keeping a log of who has accessed what and when." Same thing goes for the people who don't work in the company anymore, whose access to the network should be completely denied.

&nbsp;