

27 August 2008

By: Denisa Ilascu, Internet / SEO News Editor



IT professional fear  
external threats  
spitcomp

## [IT Professionals Fear Job Loss Caused by Security Breaches](#)

### *Shows a survey*

A recent survey performed by market research firm Opine Consulting showed that 86% of the respondents, all IT professionals, considered that the most pressing security matter that concerned them was controlling the access to the internal network. Although, usually, such a thing would also translate into the adoption of actions meant to defend from a possible attack, 45% of those who had been questioned answered that they were not entirely sure about all the devices that connected to their networks. This means that possibly dangerous endpoints could get confidential information or damage the system without the administrators even being aware of it. Almost the same percentage of IT professionals said that they were not confident in the measures their companies usually took to block external threats. In case something unexpected, like a hacking attack, happens, network engineers or administrators are usually the ones to be brought to book. The survey conducted by Opine Consulting showed that they were more than aware of the situation. 51% of the respondents expressed their fear of the possibility of losing their jobs in case of a security breach. "In analyzing the responses, it's clear that controlling network access is one of the highest priorities in all organizations," said Sheila Baker of Opine Consulting. "But deploying the appropriate technology is being hindered to some extent by a lack of focus on policy, and is often being driven by operations or security departments and not by the business units. Despite organizational obstacles, the recognized need is highlighting a gap in most security architectures where network access control solutions could be filling that gap." Massive investments in security solutions could be the answer to quench the fears of IT employees. Even more, in order to overcome them, Mirage Networks, the company that contacted the research firm for the survey, is advising organizations to use its own Network Access Control (NAC) technology. "Organizations across all industries are recognizing the greatest threat to the network is the endpoint that connects to the interior. Once inside, endpoints of all types become conduits for web-based threats and other malware to propagate within the network. Customers around the world are deploying Mirage's patented NAC solution to enable their networks to thrive in the midst of these challenges." says Trent Fitz, vice-president of Marketing for the company.

&nbsp;