

MKS provides one-stop shopping with substantial cost savings...



The Threat Within: Employees Pose The Biggest Security Risk

The No. 1 tactical security priority for U.S. companies in 2007, according to 37% of respondents, is creating and enhancing user awareness of policies. But this is down from 42% in 2006.

By Larry Greenemeier, [InformationWeek](#)

July 16, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=201001449>

Put simply, the end user is the biggest issue when it comes to IT security, says Mark Loveless, white-hat [hacker](#) who goes by the handle "Simple Nomad."

It's a concern echoed throughout *InformationWeek* Research's [10th annual Global Information Security survey](#), conducted with consulting firm Accenture. Survey results indicate that simply educating employees and partners about a company's security policies isn't sufficient to keep generally honest people from letting customer information leak out through e-mails, instant messages, and [peer-to-peer](#) networks. While the [No. 1 tactical security priority](#) for U.S. companies in 2007, according to 37% of respondents, is creating and enhancing user awareness of policies, this is down from 42% in 2006.

"They'll click on anything, and if anything slows them down, they'll short cut it," said Loveless, whose day job is as a senior security researcher with [network security](#) provider Vernier Networks, in an interview. "End users are given massively complex systems with a happy [interface](#) over it, and to make it easy for them to do their job, a lot of the controls are disabled or nonexistent."

"The problem is that you have a sophisticated attack vector, Windows, that they're all using, so you have commonality," he said. "From an attacker's standpoint, it's great. If I develop a Windows [exploit](#) all I have to do is get one of these users to click on it."

And, even when users aren't making such obvious mistakes, they're still sitting ducks for attackers looking to exploit the user's lack of knowledge of how their computers work. Loveless once worked for a company that brought most of its employees to attend a major software conference. "Because it was such a big deal, some of the people were issued loaner laptops to use so they could work at the show," he said. "Unfortunately, some of these loaner laptops were missing security upgrades. When the users logged on to the public [IP](#) addresses with these under-patched machines, we were seeing three or four attacks against them simultaneously. We're talking active attempts to run an exploit against these systems. One of the laptops was owned within 10 minutes."

Loveless and his team were able to kick off the attackers and then hastily erect a [firewall](#) to protect the laptops. But it was a classic example of an end user not realizing the security dangers they faced in a hostile environment like a hotel network.

Of course, Loveless said, it's not always the end user's fault, not even in the example he provided. Users are being handed a piece of equipment that wields tremendous power and, at the same time, has tremendous vulnerabilities and lots of enemies. "The upper hand belongs entirely to the bad guys," he said. "They have unlimited time and unlimited resources to do these things."

Unfortunately, there's no easy way to keep users from becoming their own worst enemy. Loveless suggested starting off small when it comes to user security training and moving slowly. "One thing to do is teach the user one thing per year. Spend your budget teaching (and reminding) them to write good passwords and to protect those passwords. The next year, focus on [e-](#)

[mail](#) attachments."

Of the U.S. respondents who say their companies monitor employee activities, 51% monitor e-mail use, 40% monitor Web use, and 35% monitor phone use, roughly consistent with last year's findings. However, other sources of data leakage are given less attention: Only 29% [monitor instant messaging](#) use, 22% the opening of e-mail attachments, and 20% the contents of outbound e-mail messages. And only a handful keep a close eye on the use of portable storage devices.

Only 19% of respondents say that security technology and policy training will have a significant impact on alleviating employee-based security breaches, the same percentage as last year.

Behind the scenes, IT security pros need to make sure security measures are automated and proactive, Loveless said. Don't rely on the users to protect themselves. And never forget, "whenever a box pops up on the screen, a user will click 'OK' because the makes the box goes away," he added. It's this kind of mentality that ensures security pros will always have a job.

A blue banner advertisement for SAS. On the left, there is a computer monitor displaying a green line graph on a grid. The main text in the center reads "Are You Using BI Best Practices?" in large white font, followed by "Free research summary shows current BI trends." in smaller white font. Below this is a yellow button with the text "DOWNLOAD NOW" in blue. On the right side of the banner is the SAS logo in white.

Are You Using BI Best Practices?
Free research summary shows current BI trends.
DOWNLOAD NOW



Copyright © 2007 [CMP Media LLC](#)