

■ Windows Grabs Lion's Share Of 2010 OS Market

Led by Microsoft, global operating system revenue reached \$30.4 billion last year, climbing 7.8% from the previous year, according to Gartner. Overall, client OSes outperformed server OSes, Gartner states, growing 9.3% vs. 5.7%. Windows' global OS market share grew to 78.6% in 2010, totaling about \$23.8 billion, up from 77.9% and \$21.9 billion in 2009. Windows' client OS share grew 9.2% in 2010 compared to 7.5% for its server OSes. IBM grabbed the next highest market share (7.5%; \$2.3 billion revenue), followed by HP (3.7%; \$1.1 billion), Oracle (2.6%; \$780 million), and Red Hat (2%; \$610 million). Among all OSes, Gartner says, Linux server OSes and Mac OS were the fastest growing subsegments. Charged by strong desktop and laptop sales, Mac OS grew 15.8% during 2010, reaching \$520 million in revenue. "Within the Unix OS market, IBM AIX had high single-digit growth, but Unix generally experienced modest or negative growth," says Gartner managing vice president Alan Dayley.

■ Mobile Apps Are Hot . . .

The smartphone application markets are booming. IHS iSuppli reports that the combined revenues from Apple's App Store, Google's Android Market, Nokia's Ovi Store, and Research In Motion's BlackBerry App World will soar 77.7% this year to



\$3.8 billion. Combined revenues in 2009 were \$830.6 million; in 2010 they were \$2.1 billion. And with little sign of flagging momentum, iSuppli sees a bright future for the industry. The firm expects that revenues will balloon to \$5.6 billion in 2012, \$6.9 billion in 2013, and \$8.3 billion in 2014.

■ . . . With Google Android Market Rapidly Gaining Ground

Market research firm Distimo predicts in a new report that if all application stores maintain their current growth pace, in about five months, Google Android Market will be the largest store in terms of number of applications. Already, Distimo found that Google Android Market has passed Apple App Store (iPhone apps only) where free apps are concerned (134,342 vs. 121,845). Although the App Store (for iPhone) tops other stores where total apps (333,214) are concerned, it was among the slowest growing stores in terms of relative growth in March, Distimo reports. Apps for the iPad, meanwhile, grew 12% in March to reach 75,755, with about 34,000 of those being iPad-only apps. Combined, iPhone and iPad apps total 367,334. By June, however, Distimo predicts Google Android Market will have just 40,000 fewer apps than Apple's store and will close the remaining gap before the end of July. Distimo also predicts BlackBerry App World will double its apps during a six-month stretch, passing Nokia Ovi Store sometime after May. Windows Phone 7 Marketplace, meanwhile, is expected to top the Nokia and BlackBerry stores before the Windows Phone 7 Marketplace has been available for a full year.

Protect Yourself From Workers Gone Bad

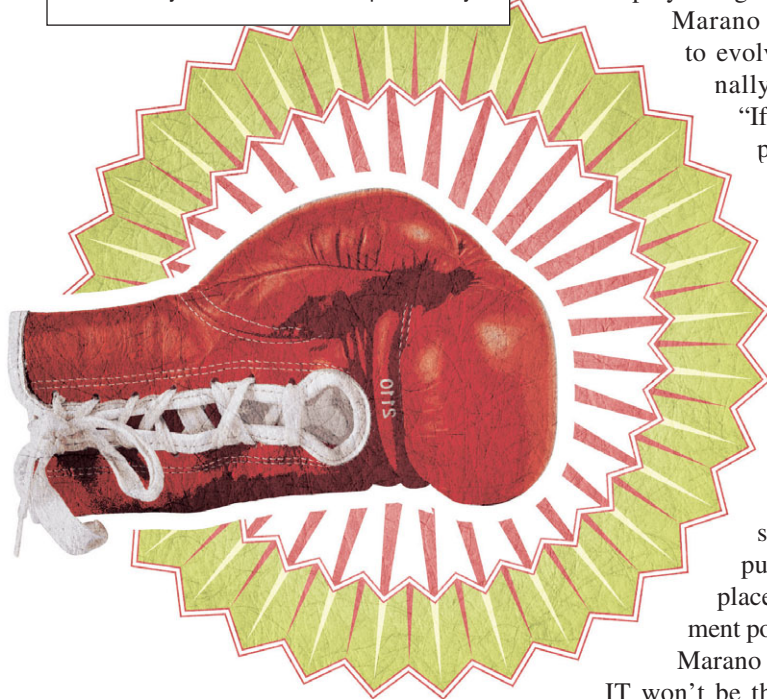
Evolved Security Processes Can Stop Rogue Employees In Their Tracks

by Carmi Levy

COMPANIES THAT DEVOTE the bulk of their IT security budgets to protecting against incursions from the outside world may find themselves needlessly vulnerable to a stealthier kind of threat from the inside: their own employees. Despite the fact that rogue employees could potentially deliver fundamental risk to the very heart of the organizations, most shops are still looking outside and not in.

Key Points

- IT security needs to evolve to proactively identify internal threats before they compromise the organization's soft underbelly.
- Rogue employees aren't always intentional; in fact, technically inept employees at the root of inadvertent exposures can cost the organization just as much as malicious ones.
- Security processes must be adapted to different roles within the organization to more effectively balance control and productivity.



"This problem is a hidden crisis," says Rob Marano, CEO of InDorse Technologies (www.indorse-tech.com). "A lot of business and IT leaders agree that it's a problem, but they don't really appreciate just how big a problem it is."

Not Always Malicious

Despite the popular perception of rogue employees as disgruntled staff surreptitiously planning a damaging exit, reality can be far less sinister. A technically inept employee with no intention of causing harm can cause just as much bottom-line pain as one who may be intent on revenge.

"People bring files home on USB flash drives or personal devices all the time," Marano says. "How many times do they, when they leave their job, somehow forget to delete these files? Do you think the company remembers?"

Marano says these quietly forgotten files can be inadvertently exposed when

peer-to-peer sharing tools are installed later on. The mobility revolution is raising the stakes still further.

"Imagine an employee who brings in his own iPad, connects it up to the corporate network, and loads some files onto it," says Robby Gulri, vice president of product marketing with Echoworx (www.echoworx.com). "The next thing you know, they've left the unencrypted device on a bus or a train. That employee, despite no intention to harm, is rogue."

Beyond Traditional Tools

Accidental or not, traditional security tools and processes focused on protecting specific pieces of the infrastructure are insufficient. And in either case, the bottom-line damage can be just as significant.

"No matter how you cut it, the majority of security solutions out there to protect against loss are tied to the siloed approach," Marano says. "The key is that I can break that model very quickly as an authorized user because there's just no way to psychologically know that your employee is going rogue."

Marano says security needs to evolve to recognize internally originating threats.

"If you watch the egress points of information, over time, you'll begin to understand employees' habits and behaviors," he says. This knowledge can heighten the organization's ability to identify changes to pattern behavior. "Understanding your usage statistics can help put policy discovery in place right at the enforcement point."

Marano says that this ensures IT won't be the last to know when an employee goes over to the dark side because the consequences will be known immediately, not weeks later following a forensic audit. "Forensics is expensive," he says, "and you'll never find out fast enough to do anything about it."

The key lies in moving past perimeter-level security that fails to recognize threats

that originate within—and never cross—the outer edge of the network, such as file-level security and solutions that actively and passively tag data files. (For more information, see the "Protect Files, Not Systems" sidebar.)

"You need something that is live and inherently built into every piece of software for every file format that you use," Marano says. "You want it to be automatic, and you don't want to have to remember to do anything. If you rely on someone to manage these monitoring processes, what do you do when that someone turns malicious?"

Look At The Parts Of The Whole

Echoworx's Gulri says organizations that have traditionally applied security to specific devices and systems need to expand their thinking. He recommends classifying people, as well.

"Don't drop all of your users into one big bucket," Gulri says. "Don't apply the same security rules universally to every worker within the company. Instead, classify them by job function and design unique security rules for each group."

Executives, information workers, field workers, and contractors use different applications in different ways and often from different locations. A one-size-fits-all security model makes it easier for employees who go bad to do so unnoticed. A more customized strategy allows IT to design effective policy frameworks for each group's specific needs, which can in turn increase IT's visibility into end-user behavior.

Gulri says the rush of smartphones and tablets through corporate front and back doors is pushing IT to adapt its security approach. Mobile-aware centralized management consoles are coming into their own, offering IT more precise control—including application whitelists and blacklists—over portable, often employee-owned devices that have traditionally been completely beyond IT's control.

"If you want or need to revoke a user's credentials, management tools mean you don't need to have the device in the office," Gulri says. "If the device gets lost or if it's in the hands of a now-rogue employee, you can turn it off immediately by removing the device's credentials or wiping it entirely. No more worrying about ongoing exposure." ■

Protect Files, Not Systems

File-level tagging means files don't just disappear when rogue employees spirit them away from corporate systems. Solutions that actively and passively tag data files can make it relatively easy for IT to track files after they've been wrongly removed from the corporate premises.

"The beauty of cloud-based Web 2.0 is that it allows you to assign unique identifiers for everyone who signs in," says Rob Marano, CEO of InDorse Technologies (www.indorse-tech.com). Active tagging lets files proactively report that they've been opened, where they were opened, and by whom—even if they're well outside the firewall. Passive tagging allows IT to scan Web sites and peer-to-peer sites to find surreptitiously removed files. It all means unprecedented long-distance IT control over files that not long ago would have been long gone along with the rogue employees who stole them.