

# Baseline

## TECH TRACK

BY MICHAEL VIZARD

# DATA PROTECTION STARTS FROM WITHIN

FERRARI'S LESSON IN SECURITY LEAKS PROVES THE POWER OF PREVENTIVE SECURITY.

WHEN IT COMES TO DATA SECURITY, everybody knows an ounce of prevention will always be worth more than a pound of cure, yet every day we still hear stories about how people inexplicably fail to put the right security measures in place.

One example of an ounce of prevention turning out to be worth hundreds of millions of dollars is a recent case involving the alleged theft of intellectual property belonging to the Ferrari racing team. A former Ferrari employee who'd defected to archival racing team McLaren Group

took with him Ferrari designs for special gases used in the tires of the company's Formula One racing cars as well as designs for the cars' hydraulic systems. As it turns out, however, Ferrari had deployed security software from Verdasys that lets it track every individual who accesses certain files.

When the police searched the former employee's home, they found documents the Verdasys software determined had been produced by this individual on printers at Ferrari. McLaren was stripped of its racing points for the year by the Formula One racing authority, essentially giving this year's racing honors, worth hundred of millions of dollars in marketing rights, to Ferrari.

While this scenario illustrates how prevention is always the best policy, sometimes IT organizations have to learn the harder way. Case in point: IBM's recent misadventures in data security.

A third-party contractor transporting backup tapes reported that tapes containing information about former IBM employees had gone bouncing down a highway after inexplicably exiting a truck traveling Interstate 287 in Westchester County, NY. IBM security executives personally searched the four-lane highway for the tapes to no avail. IBM subsequently instituted a new overarching approach to data security after testing no fewer than 42 products.

Like Ferrari, IBM is relying on Verdasys software to track how data is being accessed by individuals using specific machines after performing a cost analysis that, according to IBM vice president for security and privacy Julie Donahue, estimates that each individual security breach costs the company about \$185 to remediate.

**While everyone seems focused on the unknown external threats to security, the hard truth of the matter is that the real threat to data security most often comes from within.**

Of course, in true IBM fashion, the company is now preparing to launch a managed data-loss-prevention service around the Verdasys software as a way to profit from its past mistakes.

In terms of risk to the business, the IBM situation pales in comparison with the experience of Broadcom and its CIO Ken Venner. Broadcom implemented the Verdasys software after an employee reported that fellow engineers had left Broadcom to start up another company with about \$250 million worth of intel-

lectual capital. That case not only resulted in several people going to jail but also in the prevention of a second theft, which was discovered by the Verdasys software, Venner says.

The Verdasys Digital Guardian 5 software is an agent-based framework that not only encrypts data but also tracks data as it leaves any number of exit points, including USB drives, public e-mail systems such as Google's Gmail, FTP servers, instant messaging applications, printers and tape drives.

While everyone seems focused on the unknown external threats to security, the hard truth of the matter is that the real threat to data security most often comes from within. As Verdasys chief scientist Dan Geer says, one of the primary benefits of securing your IT organization from internal threats is that most external threats come in the form of people pretending to be internal IT assets. So by definition, securing the internal IT architecture pretty much eliminates most of the external threats as well.

Alas, Geer notes, there is no such thing as absolute security when it comes to IT; many of the same constructs that apply in the real world apply in IT. For example, if somebody really wants to steal your car, you're probably out of luck, unless you can make it more appealing to steal somebody else's car by making yours more difficult to steal.

As life would have it, the same concept also applies to IT systems and business data. ◀

MICHAEL VIZARD IS EDITORIAL DIRECTOR AT ZIFF DAVIS ENTERPRISE. PLEASE SEND QUESTIONS AND COMMENTS ON THIS ARTICLE TO HIM AT MICHAEL.VIZARD@ZIFFDAVISENTERPRISE.COM.

Reprinted from Baseline, December 2007 with permission from Ziff Davis Media Inc.  
©2007 Ziff Davis Publishing Holdings Inc. All rights reserved.

# VERDASYS

GLOBAL DATA SECURITY SOLUTIONS