

Are You Using a Reactive Security Model? It's Time to Get Proactive.

By **B. Scott Harroff**, Chief Information Security Architect, Diebold Global Security

Give me a pen drive and access to your network. There's a very good chance I'll be downloading sensitive data in minutes.

Surprised? Most retailers are. And while I'm merely playing around, professional attackers are playing for keeps—eager to compromise your data, your customers' data, even your network's overall performance. And eager to beat your system at the register...one transaction at a time.

Most Networks Are Reactive

But, what exactly is a reactive security model? And how does it make your loss prevention efforts more complicated?

Let's use your home PC as an example. Your home PC will install and run most any application you click on...even viruses, spyware, and hacker attempts. Eventually, your PC's defenses, such as anti-virus and anti-spyware software, will come to the rescue. The PC tries to react to problems as it encounters them, day by day. We find ourselves always on the lookout for the next new bad thing.

Your IT network likely behaves the same way, only on a larger scale. It, too, will willingly install and run most applications, some harmless and some malicious.

What if you could flip that security model upside down? Instead of running every program then deleting the bad ones, your network would run just the good applications and block those undesirable ones? This would let you lock down your infrastructure and enhance your loss prevention efforts.

Simple Solutions Let Retailers Be Proactive

These solutions exist. They're inexpensive, simple to install and operate, and proactively keep a retailer's terminals and network more secure.

The loss prevention or IT person can implement the solution themselves, or have a security firm do it. Once that solution is in place, the IT person can determine which programs will be allowed to run on which computers...and when. Any application not on "the list" will be prevented from loading into memory.

Prevents Data Loss

- Secures a store's "digital doorways" by preventing all unapproved applications from running.
- Enables systems and networks to run faster and smoother with fewer freezes, crashes, and reformats.
- Monitors and logs all software running on all terminals.



- Allows the retailer to modify software privileges by the hour, day, week, month, and many other parameters.
- Catches data security breaches by flagging a higher-than-normal amount of credit card queries, or queries originating from a PC other than the one normally used.
- Enables retailers to more effectively comply with software licensing agreements.
- Uses a small percentage of the CPU, which is more than offset by blocked programs that are no longer running.

Prevents Transaction Loss

How many times have you caught a store employee going into your system, lowering the price of an item...say from \$100 to \$50...selling the item to an acquaintance for the lower amount, then raising the price back to \$100? Or how about the employee who raises an item's price...by \$25, for example...sells the item at that higher price, then brings the price back down and pockets the \$25? Today's solutions watch for these and other security breaches.

Proven in Other Industries

These solutions are used in major banks and government agencies. And they could perform just as well in the retail industry. Even though every industry is different, the IT infrastructures used in most industries are quite similar, consisting of PCs, servers, and networks.

Demonstrations are available. To schedule one or simply obtain more information, please contact B. Scott Harroff at security@diebold.com or 1-800-Diebold. ■