

Cybercrime Toll Mounts for Businesses

By Ellen Messmer

September 22, 2008

<http://www.networkworld.com/news/2008/092208-cybercrime.html>

Cybercrime is more than a buzzword, it's a critical business concern, say 1,387 IT professionals surveyed by security firm Finjan.

Ninety-one percent of respondents call cybercrime a "major business risk," and 73% say they are more concerned about data theft than about downtime and loss of productivity from malware. In addition, 25% of respondents admit to data breaches in their organizations, according to the survey that Finjan conducted in July and released today.

Cybercrime's impact is no surprise to those on the front lines.

"Fraud today is highly sophisticated, and the people doing it get smarter and smarter, so we have to, also," says Gilbert Fiorentino, CEO at [TigerDirect](#). The computer and electronics equipment retailer is a subsidiary of Systemax, which also owns CompUSA.

When credit cards are stolen in volume in big heists like the one perpetrated against [TJX](#), those [stolen cards](#) are put to use by fraudsters who try to rip off stores like TigerDirect, Fiorentino says.

TigerDirect has 30 retail stores as well as an online Web sales operation for businesses and consumers. According to Fiorentino, the majority of the unrelenting attempts to hoodwink TigerDirect with stolen credit- and debit-cards will occur online in consumer sales.

A retailer like TigerDirect is an attractive target for those trying to use a stolen card because computer and electronics merchandise is easy to sell on the black market, Fiorentino points out.

One common ploy these days is for a fraudster to watch the home of a person whose credit-card information has been stolen, to determine if the person is out of the house most of the day, says Fiorentino. Fraudsters know retailers are more suspicious if a credit-card order requests delivery to a different address than the billing address of the credit card. So a fraudster might place orders to have equipment sent to the victim's home, and then intercept it, pretending to live there.

TigerDirect's home-grown antifraud system, developed over many years, seeks to raise a red flag on any manner of suspicious sales.

Red flags would be raised, for instance, for payment card data submitted from any IP address in Eastern Europe, or card numbers that have traversed through so-called anonymizer sites that hide the originating IP address. But there's plenty of U.S. domestic online fraud attempts to worry about, too, Fiorentino adds.

TigerDirect handles 20,000 to 40,000 orders for its goods each day, depending on the time of year, and most are shipped the same day the order is received. But online fraud attempts slow things down and place a burden on productivity.

"In our automated system, 83% of our orders require no manual review," says Fiorentino. But the remaining 17% of orders get a red flag that requires human intervention. Possible actions might include calling a customer, a bank or other steps to ensure credit-card fraud won't occur.

In spite of caution and preemptive actions, TigerDirect will still get hit by costly card-related fraud each year through a small percentage of bad sales -- which the retailer absorbs, not the victim of the stolen card. "It costs us millions and it costs the industry billions," Fiorentino says.

One step the company has recently taken is to use a service from fraud-management service provider [Ethoca](#) that provides a secure way for businesses accepting payment cards to share information about fraudulent card use instantly with each other. This is done in an anonymous way, so merchants can check to see if specific card fraud is occurring with another merchant.

The idea is that retailers collaborating together to discretely share fraud data will result in a better defense than each one of them on their own, Fiorentino says.