

Data Theft Replaces Downtime as Number One Worry

By Ellen Messmer

September 11, 2008

<http://www.techworld.com/security/news/index.cfm?newsid=104254&pagtype=all>

More than nine in ten of business users think cybercrime is a major problem and nearly three-quarters are more concerned about data theft than they are about network downtime.

That's according to a survey carried by security firm Finjan. The company found that 91 percent of respondents called cybercrime a "major business risk," while 73 percent said they were more concerned about data theft than about downtime and loss of productivity from malware. In addition, 25 percent of respondents admitted to data breaches in their organisations,

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 computer and electronics equipment retailer TigerDirect.

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, said Fiorentino.

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 anti-fraud 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 anonymiser sites that hide the originating IP address. But there are plenty of US domestic online fraud attempts to worry about, too, added Fiorentino.

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 percent of our orders require no manual review," says Fiorentino. But the remaining 17 percent 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.

Registration is free, and gives you access to our white paper library, case studies & analysis, downloads & speciality areas, forums, and more.

We editorially select highlights of the latest, breaking IT news, most-read articles and expert insight, and deliver them to your inbox.

Techworld's RSS feeds send the latest industry news, reviews & analysis direct to your desktop! Add to Netvibes

In spite of caution and pre-emptive 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 discreetly share fraud data will result in a better defence than each one of them on their own, said Fiorentino.