

# 'Hackers are picking on the small guys'

by [James Bickers](#) \* • 16 Sep 2008

ANNAPOLIS, Md. — New research from global payment security consultancy Trustwave analyzes the most common methods and targets of recent card breach incidents, and the results may surprise merchants.

## Methods of card data compromise — The top 10

1. SQL injection
2. Backdoor/trojan
3. Remote access issues
4. Perimeter security issues
5. Weak passwords
6. Remote exploit
7. Keystroke loggers
8. Internal attacks
9. Physical security issues
10. Wireless

The data was presented at the 2008 MICROS Users Conference, held Sept. 14-16 in Annapolis. In a joint presentation between MICROS and Trustwave, the companies announced they had partnered to offer a comprehensive suite of merchant data protection tools and services, from hardware and software to PCI auditing.

Mark Shelhart, manager of operations engineering for Trustwave, explained that his company has collected hard data from 400 recent cardholder-data compromises, and analyzed them to find the latest attack trends and techniques.

### Among the findings presented:

- The vast majority of all of the incidents — 9 out of 10 — were aimed at small merchants. Shelhart said this is a big change from just a few years ago, when big merchants were the primary target. Now that those larger entities are paying closer attention to payment security, attackers are moving on to easier targets. "Hackers are picking on the small guys," he said.
- Despite the emphasis often placed on payment security in the online channel, 69 percent of the attacks were card-present. "The attack today is in your space," Shelhart said.
- Most of the attacks (52 percent) were in foodservice, with retail a distant second (27 percent). Once again, Shelhart noted that many attackers will aim for the low-hanging fruit, and foodservice IT often "doesn't get the TLC that it needs."
- The most commonly attacked target (67 percent) is POS software, with online shopping far behind (25 percent). In a test conducted with Visa last year, Trustwave spent four hours doing a basic Internet scan, looking for ripe targets. Within four hours, the test identified the IP addresses of 1,600 POS systems — easily spotted due to improperly configured firewalls or other critical issues.
- Just who is to blame for those improperly configured systems? Sixty-three percent of the time it's a third party — a POS developer, an integrator or a local IT firm. Shelhart pointed out an alarming finding that many local IT integrators will use the same passwords for all of their clients that run a particular piece of software. "So the attacker knows, 'If I can get into one of them, I can get into all of them,'" he said. "It's a cookie-cutter approach."
- One of the requirements of the PCI data standard is that merchants must not improperly store detailed card data — "track data," the magnetically encoded information that, if placed in malicious hands, can be used to make any number of duplicate cards. Distressingly, 95 percent of brick-and-mortar merchants surveyed are running non-compliant software and are storing track data. Online merchants aren't doing much better — 60 percent of them are improperly storing CVC (card validation code) data, those extra digits on the front or back of a card that aim to provide one extra layer of security.