Franchises on guard against data thieves

February 28 2013, by Leon Stafford

Every day Hardee's franchisee Todd Pahl is on the lookout for a predator he can't see. It's not lurking in the crevices along the baseboard or slinking just beyond the range of cameras. This danger hides behind the infinite 0's and 1's in the computers that no modern company can do without.

The franchisee industry, especially restaurants, has become one of the favorite targets of data thieves.

Tight budgets that leave little money for operators to get expert help, inadequate Internet security training from the corporate leadership of chains, and restaurateur hubris have attracted criminals to the industry. They snoop out passwords and get into systems through viruses, Trojan horses and programs that copy keyboard strokes.

The result: millions in fees paid by operators to credit card companies, billions stolen from consumers and the loss of trust among restaurant customers.

"We're always monitoring our computer security because, unlike other problems, we can't see this," said Pahl, chief financial officer of By The Rockies, which also franchises Carl's Jr. restaurants. The company has more than 20 stores in the Atlanta area.

Data thieves "are invisible," he said.

Data thieves have trained their sights on restaurateurs because of flimsy firewalls and a propensity by operators to put "back office" computers with credit and debit card information on the same servers as the desktops used to surf Facebook and get reality-TV updates.

That has become costly. About 44 percent of credit card compromises originate within the food service industry, according to Trustwave, which helps companies to secure information and meet compliance standards.

The thieves sell the financial information in huge files to third parties, who then distribute the files to individuals, who run up bills as much as they can before a cardholder or a bank notices and closes an account.

When that happens, operators pay millions in fees to credit card companies for the money they have to pay consumers whose financial information is hacked, cybersecurity experts said.

And everybody is getting hit - from independent restaurants run by mom and pop operators to franchisees of big chains such as Subway, Firehouse Subs and Five Guys Burgers and Fries.

The most recent victim, Athens, Ga.-based chicken chain Zaxby's, said in January it found malware with suspicious files on computers in more than 100 of its stores - most of them franchised.

Debbie Andrews, a spokeswoman for Zaxby's, said there is no indication that customer information has been obtained by outsiders. She declined to comment further, saying the investigation is continuing.

Of course, cybersecurity issues aren't limited to the restaurant franchise community. The New York Times, Coca-Cola Co. and former President George W. Bush have all recently been the victim of cyberattacks. A study from a U.S. security firm last week accused the Chinese military of leading Internet attacks against a host of industries, including military contractors and energy companies. Consumer products giant Apple and social media leader Facebook also have been hacked.

Coca-Cola officials declined to comment on the issue of cybersecurity, reiterating an earlier statement the beverage giant issued: "Our company's security team manages security risks in conjunction with the appropriate security and law enforcement organizations around the world."

But keeping customer information safe is quickly becoming one of the restaurant industry's biggest priorities. As Americans increasingly favor debit and credit cards over cash, companies are broadening what they see as important, adding cybersecurity to the list, alongside the quality of their food, service and staffing.

Cybersecurity experts said the problem is not at the corporate level, but among individual franchisees who generally aren't getting the tools to protect themselves. Many are owners of one or two stores that don't have the size to make cybersecurity a priority. Often, they are just doing well enough to pay wages and insurance, and make a small profit that they often have to put back into the business.

"It becomes a business decision," said David Barton, principal at Atlanta-based cybersecurity firm UHY. "In most cases, you're going to spend money where you are most comfortable."

Because of those low margins, they don't take the extra steps recommended for their safety, said Tim Thomas, director of product management at Atlanta-based ControlScan, which helps companies protect their computers.

For instance, the most common mistake made is co-mingling general-use computers with those that contain financial information.

"They really need to segment their network," said Greg Grant, head of managed security services at ControlScan. "Points of sales computers have to be segregated from all other systems. People are not aware that they have to do that."

And while $50 consumer-grade firewall and virus software from Best Buy or Amazon is good for home computers, retailers with sensitive credit information from thousands of customers need much more robust protection, Grant said. They also need to think deeply about passwords and avoid easy-to-guess clues such as the restaurant's name or that of its owner.

Operators also need to use a separate DSL or cable modem line when offering customers free wireless connections, de rigueur for operators trying to attract diners who like to surf the Internet while they eat. Wireless networks offer easy access to data thieves.

The hack can be expensive, said Charles Hoff, an industry expert, restaurant attorney and operator of Hoff Hospitality. Restaurateurs can pay fees on average of $85,000 up to the six-figure range because of a breach, including fines and penalties for credit card processing, expenses related to forensic audits and the cost of reissuing customer credit cards.

Being hacked is a sensitive issue. Restaurateurs shy away from speaking on the record about efforts to fight breaches because they fear giving away sensitive information about how they protect themselves, or are afraid they'll attract data thieves looking for a challenge.

And losing customer information can cast a shadow on a business. Because identity thieves can wreck a consumer's credit for years, diners don't want to risk eating at chains that lose sensitive financial information, Hoff said.

Thomas said protection doesn't have to be expensive, but it sometimes is necessary to get outside help because the threat is constantly changing and the risk that is resolved today can be mimicked and made even more dangerous tomorrow.

Hardee's franchisee Pahl said the secret is to untangle the wires connecting sensitive information from general-use computers and to make sure no one reconfigures firewalls. If a computer goes down, only a few people are allowed to bring it back up.

That keeps access limited to as few people as possible to avoid vulnerabilities.

"We have controls that people can't surf on back office computers," he said.

(c)2013 The Atlanta Journal-Constitution (Atlanta, Ga.)
Distributed by MCT Information Services

Citation: Franchises on guard against data thieves (2013, February 28) retrieved 11 May 2024 from https://phys.org/news/2013-02-franchises-thieves.html