

Hackers Shift Attacks to Small Firms

By **GEOFFREY A. FOWLER** And **BEN WORTHEN**

• JULY 21, 2011

Recent hacking attacks on [Sony Corp.](#) and [Lockheed Martin Corp.](#) grabbed headlines. What happened at City Newsstand Inc. last year did not.

Unbeknownst to owner Joe Angelastri, cyber thieves planted a software program on the cash registers at his two Chicago-area magazine shops that sent customer credit-card numbers to Russia. [MasterCard Inc.](#) demanded an investigation, at Mr. Angelastri's expense, and the whole ordeal left him out about \$22,000.



Clayton Hauck for The Wall Street Journal

Joe Angelastri, owner of City Newsstand in the Chicago area, is out \$22,000 because cyber hackers attacked his stores' payment system.

His experience highlights a growing threat to small businesses. Hackers are expanding their sights beyond multinationals to include any business that stores data in electronic form. Small companies, which are making the leap to computerized systems and digital records, have now become hackers' main target.

"Who would want to break into us?" asked Mr. Angelastri, who says the breach cut his annual profit in half. "We're not running a bank."

With limited budgets and few or no technical experts on staff, small businesses generally have weak security. Cyber criminals have taken notice. In 2010, the U.S. Secret Service and [Verizon Communications Inc.](#)'s forensic analysis unit, which investigates attacks, responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer. [Visa Inc.](#)

estimates about 95% of the credit-card data breaches it discovers are on its smallest business customers.

How Hackers Stole Credit-Card Information from City Newsstand

The computers at the magazine shop had a program called Remote Desktop installed that made it possible to access them over the Internet. That program had a weak username and password: 'pos' in both cases.

A hacker used Remote Desktop to gain access to the computers at City Newsstand's Chicago store as early as April 15, 2009. The hacker secretly installed software that captured credit-card information. Later, the hacker installed similar software on computers in City Newsstand's Evanston location.

The credit-card reader at City Newsstand is connected to the PC. When processing a transaction, the credit-card data is sent from the reader to the PC, and then over the Internet for approval from the processor. The software the hacker installed intercepted and made a copy of the credit-card data before they were sent to the processor. The hacked credit-card data were sent to a server based in Russia and to a Yahoo email address.

The hacker's software was detected and removed on June 25, 2010, more than a year after a hacker first gained access to City Newsstand's computers.

Source: WSJ reporting
Photos: Clayton Hauck for The Wall Street Journal

Hacking at small businesses "is a prolific problem," says Dean Kinsman, a special agent in the Federal Bureau of Investigation's cyber division, which has more than 400 active investigations into these crimes. "It's going to get much worse before it gets better."



Hackers are expanding their sites beyond big companies to include any business that stores data in electronic form. For small businesses, the impact could be crippling. Geoffrey Fowler reports for the Wall Street Journal.

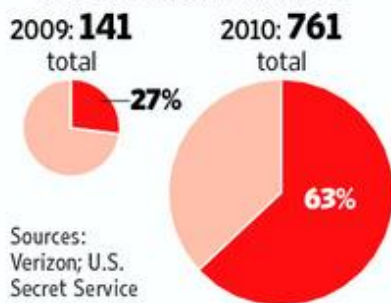
In the time it takes to break into a major company like Citigroup Inc., a hacker could steal data from dozens of small businesses and not get detected, says Bryce Case Jr., a former hacker who broke into several government and corporate websites a decade ago and now runs an online message board for hackers called Digital Gangster. Now that small companies use computers, "the juice has become worth the squeeze," he says. "Even a pizza place has addresses, names and credit-card information."

Mr. Case, now a consultant in Colorado Springs, Colo., who helps small businesses identify security problems, has a trick for showing clients just how weak their systems are. He sometimes calls employees pretending to be a tech-department worker or consultant doing work for the boss and convinces them to tell him their passwords. "All you have to do is get a hold of one not-so-competent person and you're in," he says.

Small Breaches

Security experts are investigating more cyber attacks against small companies

■ Percentage of attacks at businesses with 100 or fewer employees



The fact that there are so many types of security threats makes it difficult for small firms to protect themselves. In April, the FBI issued an alert about a style of attack in which hackers steal a business's online banking login details and use them to transfer funds out of the business's account. That's what happened to Lease Duckwall just after 1 p.m. on Nov. 2, when someone logged into his company's bank account for Green Ford Sales Inc. in Abilene, Kan. The hacker added nine new employees to the car dealership's payroll and transferred \$63,000 to them.

Mr. Duckwall learned about the transfers at 7:45 a.m. the next day. He called his bank, which froze the funds in six cases. But three payments had already been withdrawn by the recipients and the cash wired offshore.

"I don't have a clue" how or why his company was targeted, says Mr. Duckwall, who is still out about \$22,000.

The costs of a breach can put a small company out of business. In 2006 and 2007, a Bellingham, Wash., restaurant called Burger Me LLC had its computerized cash register hacked. Criminals made untold numbers of fraudulent charges on customer credit cards.

After the incident, a credit-card company shut down Burger Me's account and put a hold on thousands of dollars in incoming payments, says Rich Griffith, its former owner. By late 2008, fees and lost business from not being able to

accept credit cards put Mr. Griffith in so much debt—\$12,000 for investigation and remediation costs alone—that he closed his formerly break-even burger joint.

The cyber attack "cost me my dream," says Mr. Griffith, 47 years old. The hacker who stole the data was never identified.

Financially motivated attacks typically rely on computer code that hackers plant on victims' computers, often as attachments or links in emails sent to employees. While these malicious programs are well known to security experts, hackers tweak them frequently enough to render them undetectable to antivirus software.

Bigger companies, while not immune, generally do a better job of protecting themselves. [AT&T Inc.](#), for example, has a command center with giant screens that track all the traffic on its network. Other large companies mine data for warning signs, taking note when an employee swipes an identity badge in New York only to log onto the network from California, for instance.

Smaller companies are less likely to grasp the security threat. A 2010 survey by the National Retail Federation and First Data Corp. of small- and medium-size retailers in the U.S. found that 64% believed their businesses weren't vulnerable to card data theft and only 49% had assessed their security safeguards.

One of the most common styles of attack on small businesses targets credit-card information that a hacker can sell or use to make fraudulent purchases. To gird against this, the major credit-card companies in 2006 formed an industry group called the Payment Card Industry Security Standards Council, which establishes minimum technical protections for businesses that accept credit cards.

While credit-card companies require all businesses that accept their cards to comply with those standards, known as PCI, they have few measures to enforce them for small businesses. Bob Russo, general manager of the PCI Council, says many small businesses neglect basic security measures such as changing default passwords.

Mr. Angelastri's case shows how even a business that tries to protect itself can fall victim to hackers.

A Chicago native, Mr. Angelastri, 52, started his company in 1978 when he bought out the small street corner newsstand he started working at after high school. Over the years, he grew his business to two 1,500-square-foot locations in Chicago and Evanston, Ill., carrying more than 5,000 different magazines.

City Newsstand didn't have a computer technician on staff. But Mr. Angelastri had decades of experience with

computers after converting to a computer-based cash register in 1990. That first computerized register, known as a point-of-sale, or POS, system, wasn't hooked into the Internet. Every time it needed to process a credit card, it would use a telephone modem to log into the bank.

Four years ago, he upgraded to a now-standard [Microsoft Corp. Windows PC](#) that connected directly to the Internet. Mr. Angelastri didn't ignore security. He regularly updated the payment software on his computer to keep up with the latest standards. About two years ago, he got a local technology contractor to install a payment processing system called PC Charge, made by [VeriFone Systems Inc.](#)

On April 14, 2010, he received an email from Accelerated Payment Technologies Inc.'s X-Charge, a sales agent for his credit-card processor, saying MasterCard had identified "some sort of breach or compromise" within his system. It didn't specify what, and asked him to fill out a questionnaire and return it within two weeks.

Mr. Angelastri checked his systems and called in an outside technology consultant. That investigator found one problem on his computer—a piece of hacking software known as malware—which the investigator removed. Still, X-Charge kept forwarding him emails between MasterCard and a payment processor called [Global Payments Inc.](#) that suspected fraud.

After a sixth email warning in June 2010, Mr. Angelastri says MasterCard demanded he hire a forensic investigator to do a thorough review of his system, essentially a digital version of the investigations that police often conduct at crime scenes. Mr. Angelastri hired Chicago-based Trustwave Inc.

A Trustwave investigator worked at Mr. Angelastri's newsstand until 2 a.m. one morning looking for cyber clues as to how his system might be leaking credit cards to hackers.

The investigator discovered a program called Kameo was capturing everything that came into Mr. Angelastri's system before it even reached the PC Charge payment software. Kameo was exporting that information over the Internet, giving hackers credit-card numbers, customer names and other details.

It turned out the hackers had been lurking in his system since April 15, 2009. They had gained access to Mr. Angelastri's computer through a program he used to periodically access his technology system from outside the shop. The program could be used by anyone who knew the password, and he had picked an especially weak one: "pos," a common nickname for the cash-register software that was also the system's user name.

Bob Cortopassi, Accelerated Payment Technologies' compliance security officer, said the breach happened because of a "lack of basic security requirements" and isn't the fault of its payment system. MasterCard declined comment on Mr. Angelastri's case, and Global Payments declined to comment.

Security experts say hackers routinely scan the Internet for computers configured this way. Such searches are fast and easy, and often the computers they find have weak passwords.

The hack on Mr. Angelastri's newsstand highlights another murky area of cyber attacks. The people whose information is stolen often are never informed, despite varying state laws that require breached organizations to notify them.

Small businesses like City Newsstand don't typically record the names and contact information of their customers and payment-card companies discourage businesses from keeping credit-card data. Mr. Angelastri never learned exactly which of his customers were affected, or how many.

Many small businesses complain they get little support from law enforcement or the credit-card industry once they are hit. After the investigation, Mr. Angelastri sent the report back to his credit-card processing company. It demanded he improve his technology, including installing a new higher-grade firewall. He also cut off access to the open Internet for the computers with the cash register software. Now all they can do is pass information to the credit-card processor.

Mr. Angelastri says he is still paying off the \$22,000 he spent on the investigations and security improvements. City Newsstand has thin margins, he says, on about \$1 million in annual sales.

He reported the incident to the Chicago and Evanston police, but he never followed up. A spokesman for the Evanston Police Department said the department only has jurisdiction to look into crimes committed in the city, which it defines based on where the hacker is located. The Chicago Police Department didn't respond to a request for comment.

Mr. Angelastri also spoke a few times with the Secret Service, the federal entity charged with investigating hacking attacks, but he says that investigation didn't go anywhere. The Secret Service declined to comment.

Mr. Angelastri still doesn't know who attacked his system, but the hackers left some clues. Trustwave's investigation found that a Yahoo email address was receiving the data being collected by the hacker's malware. A message sent to that address by The Wall Street Journal wasn't returned. Yahoo said it doesn't comment on individual account holders.

The data also was being sent to an Internet server in Russia hosted by a Russian hosting company called FirstVDS, according to the investigation.

Aleksandr Belykh, the head of the abuse department of FirstVDS, said the user of the virtual server identified in the City Newsstand investigation is Russian, and his firm hadn't received any complaints about it. The company shut the account down in June after its owner failed to pay the bill. Mr. Belykh wouldn't disclose other details.

Mr. Angelastri still marvels that his business was attacked at all. "We thought there would be very little chance that somebody would come into a business of our size to pull off something like this," he says.

—Nonna Fomenko contributed to this article.