THE WALL STREET JOURNAL.
WSJ.com

USING TECHNOLOGY | Updated July 5, 2012, 6:17 p.m. ET

Cybercriminals Sniff Out Vulnerable Firms

By SARAH E. NEEDLEMAN

Sarah E. Needleman/The Wall Street Journal

Lloyd Keilson, pictured, chief executive of Lifestyle Forms Displays, had $1.2 million stolen from his company's bank account in a matter of hours.

With cybercriminals a greater threat to small businesses than ever before, more entrepreneurs like Lloyd Keilson are left asking themselves who is to blame for hacking attacks that drain their business accounts.

In May, Lifestyle Forms & Displays Inc., a mannequin maker and importer led by the 65-year-old Mr. Keilson, had $1.2 million wiped out of its bank accounts in just hours through online transactions. The theft from the Brooklyn, N.Y., company, which has about 100 employees, wasn't an isolated incident.

Many smaller businesses find themselves vulnerable to cyberthieves, mainly because they have limited budgets for Web security and few or no technology experts on staff.

"Small businesses feel like they're immune from cybercrime, and they're wrong. They are absolutely on the list of potential targets of cybercriminals," said Larry Ponemon, chairman of the Ponemon Institute, a privacy think tank in Traverse City, Mich. The average U.S. data breach cost companies $194 per compromised record last year, he added.

About 72% of the 855 data breaches world-wide analyzed last year by Verizon Communications Inc.'s forensic analysis unit were at companies with 100 or fewer employees. That's up from

The founder of a mannequin factory in Brooklyn, N.Y., with 100 employees, woke up one day in May to discover that $1.2 million was stolen from his business accounts, a victim of cybercrime.. Sarah Needleman reports.

How Hackers Attack

Here's a closer look at the problems suffered by one small-business owner whose business bank account was drained by cyberhackers.

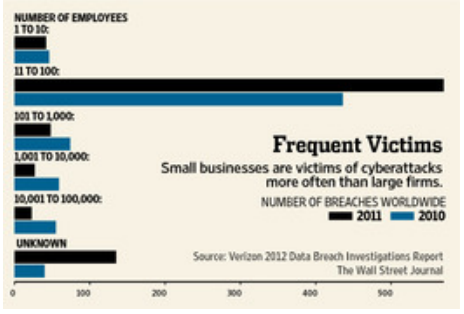
63% of the 761 data breaches it analyzed in 2010. The figures included investigations conducted by Verizon's team, as well as data-breach investigations by various law-enforcement groups around the globe, including the U.S. Secret Service and the Australian Federal Police.

A survey last year of executives at 500 U.S. companies of varying sizes found that 76% had had a cybersecurity incident within the past 12 months resulting in the loss of money, data, intellectual property or the ability to conduct day-to-day business, according to the Computing Technology Industry Association, an information-technology industry trade group. About half of those cases were described by the businesses as "serious," it said.

Mr. Keilson's troubles began on a Monday afternoon when his company's head of finance wasn't able to make a routine online payment to a foreign vendor. The executive got error messages during repeated attempts to log in to the company's banking website with a password from a secure-ID token.

Bank officials denied any problems on their end, so Mr. Keilson's three-person IT team surmised that the company had been hit by a virus, despite having up-to-date antivirus software, he said.

The company was able to clean up its computers the following morning, but by then the damage had already been done. Cyberthieves had made off with $1.2 million, wiring the money through nine transactions of about $150,000 each to three major U.S. banks and one Chinese bank.



Mr. Keilson, an ordained rabbi and attorney who co-founded Lifestyle Forms & Displays in 1985, said the business normally makes just one or two wire transfers a day totaling no more than $300,000.

He immediately set out to try to get the stolen money back by notifying his company's bank of the problem. Officials there said they would issue retrieval notices right away to the banks that had received the stolen funds: Bank of America Corp., Wells Fargo & Co., J.P. Morgan Chase & Co. and Agricultural Bank of China Ltd., Mr. Keilson said.

Within five days, the company's bank, New York-based Signature Bank, succeeded in recovering nearly $800,000 from two of the recipients—Wells Fargo and J.P. Morgan Chase.

Spokespeople for Wells Fargo, Bank of America and J.P. Morgan Chase declined to comment. Attempts to reach Agricultural Bank of China were unsuccessful.

Mark Sigona, Signature's chief operating officer, confirmed Mr. Keilson's account of the bank's role in the matter, adding that its own security hadn't been compromised. Normally the bank doesn't comment publicly on its client relationships, but Mr. Keilson authorized it to do so in this case.

To retrieve the remaining stolen funds, Mr. Keilson said he asked people in his network of friends and associates for help in putting pressure on the two other recipient banks.

Through one connection made while doing volunteer work for his area's Jewish community, he said, he managed to get on the phone with the secretary to the CEO of one of the U.S. banks that had received some of the stolen money and ask for restitution. "I wanted to make a nuisance of myself, so that they would do everything possible to satisfy me," he said.

He also called the Federal Bureau of Investigation and New York Police Department.

Within two weeks, officials from both organizations came to his company's 100,000-square-foot headquarters in Brooklyn's East New York neighborhood to investigate, but he knows of no further attempt by either agency to follow up. He said an FBI agent told him that his company was the victim of a new virus and an unknown perpetrator.

The FBI, citing its policy, declined to comment. The New York Police Department also declined to comment.

Mr. Keilson's efforts paid off only partly. Within 15 days of the robbery, he had regained about $1.04 million of the stolen money. The restof the money remains unaccounted for. He said he now is trying to determine whether his company's bank is legally responsible for making up the balance.

Signature's Mr. Sigona declined to comment.

Courts often find banks aren't liable in cybercrime cases in which a business client's computer systems were breached, according to George Tubin, senior security strategist for Trusteer Inc., a provider of cybercrime prevention technology in Boston. He said many cases brought by small-business owners after their business accounts have been hacked are being settled out of court.

"It comes down to what type of security a bank has in place to detect fraud and what the small business did for the hackers to be able to access its accounts," Mr. Tubin said. "As long as the bank provides commercially reasonable security, then the bank's not liable."

Cybersecurity experts say small-business owners need to do more to protect their firms from high-tech thieves than rely on standard security products.

Since the attack, Mr. Keilson has taken more steps to protect his business. All outbound bank transactions now require verbal clearance from an authorized company executive. And he said he bought a $1 million insurance policy at a cost of $13,000 a year to cover any losses from computer fraud.

Businesses in North America set aside on average about 5% of their IT budgets for security last year, or about $591 per employee, according to technology research firm Gartner Inc., which is based in Stamford, Conn. Overall, they are on track to spend a record $9.2 billion on new security software this year, it estimates.

"Smaller firms rely more on standard protections like firewalls and antivirus software," as opposed to the kind of sophisticated, cutting-edge controls that many large companies use, said Lawrence Pingree, an analyst at Gartner. "When you're smaller, you're more focused on executing the business as opposed to IT efficiencies."

Protecting Yourself

To cut the risk of cyberattacks on business bank accounts:

Pay for protection. Rather than rely on free security products, Invest in reliable controls for at least one computer in your office and use it to make all major all financial transactions.

Use human backup. Require your bank to get verbal authorization from an authorized employee for over a certain daily volume of transactions.

Insure your assets. Hackers are always refining their skills. Security measures that are reliable today may not work tomorrow.I

Know whom to call. Make a list of those to contact immediately should a breach occur, such as your bank's security team and law-enforcement officials.

A version of this article appeared July 5, 2012, on page B7 in the U.S. edition of The Wall Street Journal, with the headline: Cybercriminals Sniff Out Vulnerable Firms.