labusinessjournal.com
LOS ANGELES BUSINESS JOURNAL®
THE COMMUNITY OF BUSINESS™
Volume 35, Number 26 July 1 – 7, 2013

Banks' Commercial Customers Face Online Risks

By STAN STAHL

An L.A. accounting firm recently discovered cybercriminals had fraudulently transferred $150,000 from its bank account. An escrow company in the South Bay had $400,000 stolen by online bank thieves. In 2011, Bloomberg estimated that total online bank fraud losses were in excess of $1 billion. The situation has only grown worse in the two years since Bloomberg's analysis.

The modus operandi in all these stories – and in others like them – is basically the same. The victim – acting in all innocence – unknowingly installs a cybercriminal's malicious software (malware) on its computer. The malware captures the company's online bank credentials, sending them over the Internet back to the cybercriminal who is often halfway around the world. Armed with the victim's bank credentials, the cybercriminal now goes online to the bank, impersonates the victim and steals the money.

The cybercriminal's technology is so good that standard defenses are simply not up to the challenge. The malware easily gets past the victim's firewall and antivirus software. The cybercriminal steals not only the victim's user ID and password but also the answers to all the security questions, like his mother's maiden name or the name of his first pet. Best-in-breed cybercriminals are even able to bypass the bank's security token, the little key fobs with numbers that change every 60 seconds.

While all banks have anti-fraud systems designed to detect and prevent fraud, these systems are hard pressed to identify a money transfer request as illegitimate when it comes from the victim's own computer using the victim's legitimate credentials.

Making matters worse – rubbing salt in the wound – is when the victim discovers that it – not the bank – is responsible for the loss. This is a crucial difference in banking regulations between commercial and consumer accounts. Consumers are protected by Regulation E, which provides for bank reimbursement in the event of fraud. Commercial account holders have no such regulatory protection.

Most of the victims of online bank fraud are small businesses. Forced to absorb a fraud loss, as many as 60 percent of small businesses victimized by online bank fraud and other cybercrimes go out of business within six months.

Even though banks are not generally legally liable for online bank fraud losses, they are still extremely concerned about the problem. Part of their concern is – as one would expect – regulatory.

The deeper concern isn't regulatory, though. It's personal. Online bank fraud poisons the customer-banker relationship.

Finding fault

The customer believes the bank is clearly responsible; that its systems should have caught the fraud. The customer has had his expectations set by his experiences in the noncommercial situation, with one's credit cards and personal checking account. Nothing in the customer's imagination suggests that the bank wouldn't be responsible.

From the bank's point of view, the customer is clearly responsible. The customer's account was accessed by someone purporting to be the customer. Subsequent investigation established that the customer's computer had been hacked and online bank fraud malware installed. The bank's security procedures – at least as understood by the bank – were commercially reasonable (the bank's threshold of legal responsibility). Nothing in the bank's imagination suggests that the customer wouldn't be responsible.

Online bank fraud is lose-lose-lose no matter who is responsible. The customer loses. The bank loses. And our community loses as money is drained from our economy and jobs are lost.

Several L.A. banks have recognized that the status quo is no longer acceptable. These banks are part of our association's Financial Information Security Forum. These banks meet monthly, sharing information and collaborating on ways to better detect online bank fraud and more effectively educate customers.

Some of L.A.'s most prestigious banks are part of our working group. Our association, the Los Angeles Chapter of the International Systems Security Association, is pleased to lead the Financial Information Security Forum. The forum illustrates our association's core perspective that "It takes the village to secure the village," reflecting our mission to be the catalyst for improved cybersecurity in Los Angeles.

Securing the 300,000 businesses, non-profits, schools, religious organizations, foundations and government agencies in greater Los Angeles requires us to work together, learn together and educate others.

Our community can be proud of these forward looking financial institutions, committed to making a difference, demonstrating by their own example how we can all work together to better secure our community.

Stan Stahl is president of the Los Angeles Chapter of the Information Systems Security Association. The association is a not-for-profit, international organization of information security professionals.

ISSA-LA is the premier catalyst and information source in Los Angeles for improving the practice of information security. The Chapter provides educational programs for information security and IT professionals. The Chapter conducts outreach programs to businesses, financial institutions, nonprofits, governmental agencies, and consumers. ISSA-LA is the founding Chapter of the Information Systems Security Association, an international not-for-profit association of information security professionals and practitioners. www.ISSA-LA.org.