



HOLDING BANK ACCOUNTS HOSTAGE

COMPROMISED COMPUTER SYSTEMS LEAD TO TREMENDOUS FINANCIAL LOSSES FOR COMPANIES

By **RICHARD P. FINKEL**

The alarm has sounded; online crime was up by 600 percent in 2009.

A large portion of that increase was in the area of electronic funds transfers placed through the Automated Clearing House (ACH). Late last year, the Electronic Payment Association and the Internet Crime Complaint Center issued warnings about what has come to be known as corporate account takeover.

In a corporate account takeover, a business finds that, virtually overnight, funds have been stripped from its bank accounts by cyber thieves. These cyber thieves are gaining access to, and control of, business bank accounts by stealing valid online credentials and initiating ACH transfers, usually in amounts less than \$10,000 to avoid detection.

Through October 2009, reports of attempted corporate account takeovers totaled approximately \$85 million, with actual losses of approximately \$40 million. In one published case in which a Midwest non-profit organization was targeted, cyber thieves executed an ACH batch file of 16 separate debit transfers, each less than \$9,000, for a total of more than \$142,000.

In another published case, a small California company was hit with 17 ACH transfers totaling almost \$100,000, resulting in a loss of \$48,000.

Malware Intrusions

In most cases of corporate account takeover, the subject company's computers are

infected with malicious software known as malware. Malware is often transferred through an e-mail which contains links to web sites or has documents attached.

Clicking on these links or opening these documents downloads the malware to the subject computer, providing the cyber thieves with a portal through which they can capture and observe the company's online activity.

Malware can also come from visiting legitimate web sites, especially social networking sites, by viewing pictures, videos or documents. Once installed, the malware harvests information by logging keystrokes and capturing IDs and passwords when users log in to their bank's web site. From there, the cyber thieves can create additional user accounts from the stolen credentials or initiate the transfers of funds.

In an effort to hide these activities, the cyber thieves set up what is known as a money mule network. Money mules are people recruited to assist the cyber thieves in transferring money out of the country. They are recruited through work-at-home advertisements or through popular online employment sites.

In one particular mule network, the cyber thieves hired individuals with the job title of regional clerk. The job description was to assist a Switzerland-based insurance company in distributing reimbursements to policy holders via wire transfers. Although these new employees were supplied with elaborate employee handbooks, the Swiss company did not exist.

Once hired, the mules are instructed to

open a bank account to receive money transfers. Soon thereafter, money is deposited via ACH, and the mule is instructed to forward the money, typically to accounts in Eastern Europe and Asia via wire transfers services, including Western Union and Moneygram.

The transfers are usually initiated in amounts less than \$10,000, and the mule is allowed to retain 5 percent as a commission.

The Federal Bureau of Investigation reports that the most likely targets are small-to medium-size companies, schools, non-profit organizations and government agencies. The targets are often identified from web sites that list contact information and organizational charts. From these web sites, the thieves can identify the individuals in the organization who may be handling financial transactions and then direct the malware attack to those individuals.

Combating Thievery

Although consumers have 60 days to notify their banks of unauthorized electronic transfers, businesses must be more vigilant to catch these transactions before the funds disappear. Reporting the fraudulent activity by midnight of the next day may allow for the transaction to be reversed before the cyber thieves cash in.

Simple strategies include daily reconciliation of cash accounts, initiating transfers from work stations restricted for financial trans-



Richard P. Finkel

Richard P. Finkel is a partner with BlumShapiro, one of the largest regional accounting, tax and business consulting firms in New England. He is based in West Hartford.

forensic accounting

& valuation — litigation —

action use only, and the use of positive pay, which involves providing an authorized list of disbursements to one's bank in advance.

The best way to deal with fraud is to prevent it.

Organizations should engage experienced professionals to undertake a fraud risk assessment to proactively identify both internal and external fraud risks and to develop cost-effective fraud prevention and detection policies and procedures. These policies should clearly define roles and set a tone that impacts an

organization from the top down.

It is also advisable to periodically re-assess risk potential. Setting a policy and putting a system in place is where it starts, but maintenance and occasional check-ups are just as helpful.

These periodic assessments involve identifying potential areas of risk, considering potential override controls and occasionally testing existing anti-fraud procedures. These "fire drills" can provide any organization with much-needed assurance that these

policies and procedures are working, and can also help to indicate what needs to be updated or changed.

The truth of the matter is that the 600 percent jump in online crime witnessed in 2009 should be a warning to all businesses and organizations that the right precautions must be taken in order to avoid corporate account takeovers.

Hyper-vigilance is never a bad thing and can wind up saving a company tremendous amounts of money in the end. ■