usbanker
Beyond Business as Usual

OpEd

May 2003

Identity and the Insider Threat

By David Fertell
president and CEO of Pearl Software

THE TYPICAL IDENTITY BANDIT NO LONGER PILFERS garbage cans searching for credit card receipts. Today's identity thief is a white-collar, computer savvy employee with desktop access to large financial databases chock full of customers' names, Social Security numbers and credit and bank account information. Law enforcement experts estimate half of all identity theft cases come from raiding business databanks, as it is discovered that more and more technology systems lack proper safeguards and oversight.

In 2001, the FTC received 86,000 complaints of identity theft. By 2002, the number of complaints had almost doubled to 162,000. The rising use of the Internet for business and personal communications coincides with the explosion in identity theft because computers have made it relatively easy to access and communicate sensitive information.

This point was proven last December when federal prosecutors announced they had arrested and charged three people in connection with a scheme to steal the personal financial information of 30,000 Americans by downloading computer data and then selling it to scam artists. Prosecutors alleged that over three years, the thieves had stolen millions of dollars using passwords to access personal information, including Social Security and bank account numbers.

It's not just customers that are being duped. Security experts say the fastest growing cyber crime involves the buying and selling of intellectual property—a company's new product designs, proprietary financial information, confidential memos. An increasing percentage of valuable corporate data is being electronically siphoned and sold to the competition.

The bottom line is that threats today are more likely than ever to come from inside. But what weapons does an institution have to fight fraud? How can an organization safeguard customers' privacy, secure corporate data and protect itself from legal backlash? Increasingly, financial institutions are turning to Internet monitoring software in hopes of catching employee theft before it occurs. Internet monitoring software tracks most forms of Internet communications, including Web browsing, file transfers, news group postings, chat, e-mail and instant messaging. Employers are provided with a detailed log of employees' Internet activities, including the content of transmitted messages. An Internet administrator reviewing the log can easily spot employee use that might indicate fraud or the transmission of personal or sensitive information.

There are a variety of reliable software programs available to monitor Internet use. Here are some points to consider: Involve Compliance Officers early on. Consult with Compliance Officers in the selection of data capture features that will help institutions comply with FDIC, OCC and state regulations. Make sure the software's primary focus is monitoring. Some software programs only filter content based on keywords. Other applications simply block communications based on a "block list" comprised of a list of "off limit" URLs. With identity theft, however, organizations are more concerned about leaked information, rather than communications being received so monitoring software is more appropriate. Monitoring software allows workers to send files or e-mail, for example, and then captures data from these transmissions and provides reports of Internet activity.

Make sure the software archives data for future review. Financial institutions often need documentation to comply with federal and state regulations. Choose software that records and reports on the exact data being transmitted, rather than just an activity summary. Implement a solution that validates captured data. Captured data may be corrupted during transmission or may be altered by employees wishing to hide their actions. Select software that takes a "fingerprint" of all data as it is captured so information can be validated by individuals or entities responsible for oversight or prosecution.

Implement an Internet Acceptable Use Policy (AUP). Clear guidelines are the first step toward ensuring employees' cooperation. Implementing an AUP communicates what is and is not acceptable for employees to do online. Sometimes simply having the policy and software in place acts as a deterrent to misuse.

Document everything. Internet monitoring software aids compliance with a provision of the Financial Services Modernization Act, dictating that institutions must disclose how customers' personal information is used. Because financial institutions are legally bound to keep e-mail records to protect against charges of financial misdoing and ensure proprietary information is secure, Internet monitoring software provides an audit trail that can protect against serious legal actions.