TECHNOLOGY

Identity Theft and the Public Accounting Firm

Column: The eSecurity Advisor

Sep. 01, 2008

From the Sept. 2008 Issue

This month's column is an interview with Robert Listerman. Bob and I recently spent a lunch hour together and talked about the problem of identity theft and how technology plays a role in identity theft. It was a very informative, eye opening and interesting conversation, and based on what we discussed I thought it important to point out that practicing accountants need to understand this problem. Practitioners need to be aware of the requirements the government is imposing on all users of personal information and why these rules could potentially cause significant issues for our profession.

Generally, identity theft is not directly linked to specific technology, but technology becomes the enabler that allows identity theft to occur because the root cause could be a poorly implemented firewall, improper security patching or sloppy technical implementations. The technology is not to blame; rather, it is the way the technology is utilized or implemented. While the focus this month is on the problem of identity theft and some of the government requirements being placed on all businesses, including the accounting profession, you should also be mindful of the underlying technology issues as you read. Technology, properly implemented, can prevent identity theft in a firm. The key question

should be whether enough has been done with the technology to ensure that it is not enabling identity theft.

Before we get into the content of the interview, I would like to introduce you to Bob. Robert Listerman (Bob) is a Michigan CPA with over 25 years of experience
as a process improvement business consultant. He graduated from Michigan State University and became a CPA while employed at Touche Ross & Co., Detroit, now known as a member firm of Deloitte & Touche USA LLP. Bob added the Certified Identity Theft Risk Management Specialist (CITRMS) designation issued by The Institute of Fraud Risk Management in 2007, which recognizes his knowledge and experience in identity theft risk management.

Over 50 percent of identity theft can be traced back to unlawful or mishandling of non-public data within the work place. Recent federal and state laws have been enacted to bring both criminal and civil liability to any organization that improperly maintains data on customers, employees, vendors and even its own non-public identifying information.

Now that we have an idea of Bob's background, let's take a look
at this security problem that can affect public accounting firms just as much as it affects the business clients we serve.

John: What is identity theft?
Bob: Identity theft is the use
of personal identifying information by someone other than the rightful owner of that information for purposes of criminal activity. Generally, the criminal is using this information to benefit financially. In many cases, the person using the information is also NOT the person who originally obtained the information.
Some of the more common types of identity theft include the following:

- **Driver's license theft** – the use of a fake ID to commit or cover a crime.
- **Social Security number theft** – the use of a person's SSN to obtain income generally payable through a 1099 or W-2.
- **Character/Criminal ID theft** – the use of an ID to cover criminal activity from another state. For example, a criminal carrying an apparently valid driver's license in Virginia using someone else's identity covers up the fact that Maryland has revoked a criminal's driver's

license because of too much drunken driving activity.

- **Medical theft** – the use of someone's ID to obtain test results. For example, someone who suspects they might be HIV positive could use someone else's identity to obtain the test and results.
- **Financial Identity Theft** – The theft of information for purposes of stealing money from the victim.

John: How large is the problem?

Bob: In overall terms, the problem of identity theft is larger than the war on drugs. It is the most reported crime to the Federal Trade Commission (FTC) and is growing at a rapid pace annually. The other thing that makes this a large problem is that law enforcement has the most difficulty in pursuing the criminals committing these crimes. The problem is also multi-pronged because the Internet allows criminal gangs in Eastern Europe, China, Russia or other parts of the world to hack into computers in the United States and steal information. They then post this on the Internet for sale to others who actually use the information. Not only does this make it a large problem in terms of size, but it is also the reason it is so difficult for law enforcement to arrest and prosecute those responsible.

Many times, identity theft is a crime of opportunity, such as shoulder surfers stealing information from someone at work or the public library, or a member of the cleaning crew working after the office is empty and obtaining information left out on someone's desk.

There is an active market for stolen identities; and, depending on how much information is available on a particular person, the price for the stolen identity can be in the hundreds of dollars. In many cases, the stolen identity when used generally results in small losses that are more of a hassle for law enforcement. Since finding and prosecuting the criminals, especially if they originate overseas, is difficult; many times the only people prosecuted for the identity theft are the users of the stolen identity.

John: Why should accounting firms be concerned?

Bob:

The primary reason accounting firms should be concerned is because of the loss of reputation. Twenty percent of customers who are affected by identity theft

originating from a single source will cease doing business with that entity. Forty percent will look at other competitors with the idea of possibly changing to that provider. Five percent will sue the entity who caused their identity to be compromised. Because tax and accounting professionals and other public accounting entities are held to a higher standard in terms of confidentiality, it is likely the number of clients who would move their business would be greater than 20 percent for a public accounting firm.

In addition to the loss of faith by the customer base, the rules regulating the control of financial information promulgated by the FTC can be enforced both criminally and civilly against the entity. Several provisions of the Gramm Leach Bliley Act of 1999 can be enforced by the states in addition to the federal level. Affected individuals can have claims against the organization and, as a result, create a growing concern issue for the affected entity. If executive management is determined to have complete disregard for the provisions of the law and regulations, they can be held criminally responsible.

John: What are accounting firms required to protect under the law?

Bob: Personnel Identifying Information (PII) is what we are expected to protect. This includes the obvious such as Social Security Numbers, credit card numbers, bank account information, and birth date along with many things that we don't think of, such as an unlisted address or telephone number. The rule of thumb is that if it is not publically available in a resource established as a public source, such as a phone book, then it is PII.

Public Accounting firms are still subject to the provisions of the Gramm Leach Bliley Act even though we are no longer required to send out privacy notices. Public accountants should talk with their corporate attorney or professional liability carrier for further clarification about what and how to deal with PII.

John: What can we do to comply with the various laws applicable to public accountants?

Bob: Gramm Leach Bliley has the most teeth in terms of enforcement provisions and applicability to public accounting firms. It carries the largest fines for non-compliance. This should be the one

that most accountants become familiar with to prevent problems from developing in their firms.

From a 50,000 foot view, the things accountants can do to protect themselves is:

1. Become familiar with the applicable laws

2. Every entity should have an identified senior manager charged with protecting
PII

3. Business processes should be examined to determine if PII exists in that process and if so, does it need to be protected.

4. Establish a privacy or sensitive information policy

5. Train all employees even if they don't handle sensitive information what the policies are and what they are expected to do.

For the person in charge of maintaining the privacy information, they should establish a written policy, provide the training to the organization, and offer Identity theft protection to all employees either as a company paid benefit or as an employee paid option. The reason to provide identity theft protection is for two reasons:

1. It can serve as a red flag if a large number of claims start to occur for employees – it could mean an insider or vendor is stealing information about fellow employees.

2. It provides a resource for the employee whose identity has been stolen to help resolve the mess that is created. It reduces the time the employee spends at work trying to get the problem resolved favorably.

John: What resources are available to help me comply?
Bob: The **FTC** has a large amount of information about identity theft both from the employer and victims perspective (www.ftc.gov).

BTR-Security's website (www.btr-security.com) has a large number of resources along with other information pieces on the area of identity theft. [This site is maintained by Bob Listerman].

The **Identity Theft Resource Center** (www.idtheftcenter.org) is a non-profit that helps track breaches and provides helpful information for both victims and those responsible for preventing identity theft.

Privacy Rights Clearinghouse (www.privacyrights.org) has lots of templates and other tools for organizations trying to develop internal documents and procedures.

Summary

It is generally not the technology which causes the identity theft problem. In many cases it is human error that leads to identity theft. Hackers are proactive, but are a small part of the larger problem. Identity theft is generally a crime of opportunity when a person with a weak moral compass has the information fall into their possession without much effort. Your data whether in electronic or paper form should be thought of in terms of its monetary value on the open market to an identify thief who is attempting to sell it. To an identity theft, the data held by and maintained by a public accountant can represent a large sum of money to the thief.

We, in industry, not only need to become more alert and aware of the dangers around us from those trying to steal our data, but we also need to be aware of the new government requirements coming online which will impact our business. These rules and regulations are promulgated to ensure we are doing the right thing to protect our client's data from falling into the hands of an opportunist. Are you doing your part both technically and non-technically to secure your data?

Technology • Article