Identity Theft and Financial Fraud: Some Strangeness in the Proportions

Hal Berghel, *University of Nevada, Las Vegas*

If we can't trust banks, healthcare providers, colleges, and government entities to protect our privacy, who can we trust?

Identity theft and financial fraud vulnerabilities are being exposed at ever-increasing rates these days. No news there. What I find remarkable is the type and variety of these vulnerabilities.

A recent news story concerned the leak of personal information by the Metro Atlanta YMCA. According to the facility's disclosure letter to its members,

> [We] learned on November 9, 2011 of the theft of several computers from the office of our software testing and development vendor. … One of the stolen computers, that was password protected, included information on facility members who were active in 2008 and who had transactions that required bank draft, debit or credit card charges. The data included first name, last name, address, phone number, email, birthdates, and encrypted bank account, debit or credit card numbers. …We deeply regret any concern or inconvenience the theft of these computers may cause you.

The letter recommended that the members

- closely monitor their financial accounts,
- review all transactions,
- be alert for any unauthorized account activity,
- register a fraud alert with the three main credit bureaus, and
- obtain a free credit report from annualcreditreport.com.

This is an interesting story from a number of perspectives, not the least of which is the apparent failure of the Y to accept any responsibility for the security breach that may have resulted in the loss of its members' personal information. Second, the lost information qualifies as core components of private personal identifiers (PPIs) as defined by the payment card industry (PCI) and the banking industry, and as required by federal and state regulations.

Note that this isn't the stricter, extended definition used by the US Office of Management and Budget, the National Institute of Standards and Technology, and other organizations that wish to extend the definition to include anything that can uniquely identify, contact, or locate people or enable the same. Rather, this is the softer, limited, vanilla version expected of every organization that handles credit and debit cards.

In addition, the tenor of the member letter is that it was the third-party vendor that slipped up—as if that absolves the Y of responsibility. Finally, note that as far as the Y is concerned, it's entirely up to the victims to seek further remediation, regardless of the fact that they're going to feel the costs of this mishap for quite some time to come—even if the personal data isn't ultimately used for criminal activities.

To be sure, there are many legal questions as well, but What I'm interested in is how we got ourselves into the position in which this sort of thing is possible. The focus here is on the type and variety of these reported breaches when viewed as a whole.

THE MAGNITUDE OF THE PROBLEM

In addition to the YMCA incident, other recent events of interest include a hospital website breach that resulted in the public release of 10,000 patients' credit card num-

 Published by the IEEE Computer Society 0018-9162/12/$31.00 © 2012 IEEE

r1out.indd 86 12/20/11 11:25 AM

bers, the compromise of 2,000 dental patients' records by a password theft, a lost backup tape that may have exposed 1.6 million people to ID theft, and the largest ID theft bust in US history (www.itffroc.org/rr.html).

The actual number of identity theft and financial fraud victims can only be estimated. It's understood that many, if not most, cases remain either unreported or undetected. Some industries, such as banking and gaming, go to great lengths to avoid any media coverage suggesting that their security has been compromised. Not only is this bad for business, but there's also the ever-present risk that the tag-and-baggers will arrive with a warrant and seize the companies' hard drives.

To my knowledge, there has never been definitive research on the extent of underreporting. Of one thing we can be sure: if modern business and industry aren't specifically required by law—under some fairly parochial legal interpretation, of course—to report breaches of customer/client confidentiality, the breaches won't get reported.

However, we do have some ballpark estimates of the extent of losses. Private consultancies such as Gartner and Javelin Strategy & Research conduct surveys to gather this data. Consumer groups such as the Better Business Bureau and some US government agencies, including the Federal Trade Commission, collect information on reported complaints from both internal and external sources. Other government agencies such as the US Department of Justice, the FBI, and the Secret Service conduct investigations to collect information.

In all of these cases, estimated losses are necessarily extrapolations. Although no one really has an accurate handle on the dollar amount, there's a general consensus that the "three orders of magnitude" rule of thumb comes pretty close to most estimates: each year, 1 to 10 million people lose on the order of $1 to $10,000, resulting in a loss of $1 to $10 billion dollars. This is a staggering amount of white-collar crime, even by Wall Street Ponzi scheme standards.

OUT-OF-BAND LINKS

For additional detail on the Atlanta YMCA data-theft incident, see www.ajc.com/news/dekalb/ymca-says-someone-stole-1236919.html. A copy of the letter sent to the members is available at http://media.cmgdigital.com/shared/news/documents/2011/11/21/YMCAletter.pdf.

There's no shortage of studies on the size of the identity theft and financial fraud problem. Unfortunately, accessing some of the best information requires a corporate membership. Some links that might offer a useful introduction include the following:

- **The 2010 FTC Consumer Sentinel Network Data Book: www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf**
- **Privacy Rights Clearinghouse surveys: www.privacyrights.org/ar/idtheftsurveys.htm**
- **The Identity Theft Research Center: www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml**
- **The Online Trust Alliance: www.otalliance.org**
- **The Identity Theft and Financial Fraud Research and Operations Center: www.itffroc.org**

For a more thorough analysis of an earlier reporting period, see A. Grover, H. Berghel, and D. Cobb, "The State of the Art in Identity Theft," *Advances in Computers*, vol. 83, M.V. Zelkowitz, ed., Academic Press, 2011, pp. 1-50.

THE STRANGENESS IN THE PROPORTIONS

In our lab, we routinely collect and analyze media reports of identity theft and financial fraud from a high-level perspective to provide a backdrop for our technical work in developing security appliances to help investigate and protect against such crimes. Our lab doesn't try to cover all security and privacy breaches related to identity theft and financial fraud. Rather, we report on stories that get mainstream media attention and seem interesting.

We recently analyzed major data breaches reported by the media during the 15-month period from 1 January 2010 to 31 March 2011. A high-level pass through the data revealed a list of major causes of data loss. Lost or stolen devices—flash drives, laptops, tablets, PDAs, and so on—led the list, with computer or network hacking a close second. These were followed by lost/discarded documents or physical media, accidental disclosures, and insider threats.

Accidental disclosure of private information includes internal and external data leaks resulting from improper access control, flawed records-retention implementation, improper data and media sanitization or destruction prior to equipment repurposing, ineffective data loss prevention policies and enforcement, and the like.

Figure 1 shows coarse categorizations of reported data breaches by cause. Not surprisingly, hacking produces more record compromises per incident than other causes, while the converse is true for data breaches involving physical media. But as Figure 2 shows, breaking out the breaches by organizational type reveals the most interesting results.

The figures indicate that "inviolable" institutions—banks, healthcare providers, colleges, and government entities—produced the lion's share of data breaches. If we can't trust these institutions to protect our privacy, who can we trust?

Ignoring the miscellaneous "other" category, medical providers lead the

r1out.indd 87 12/20/11 11:25 AM

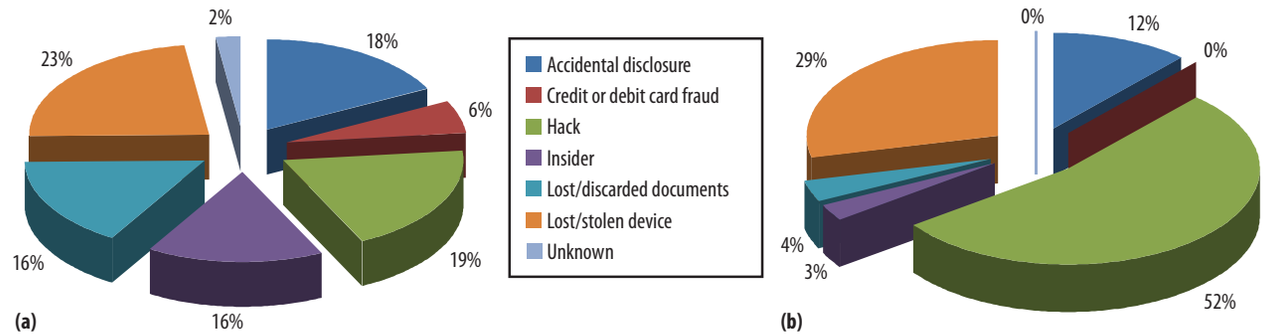

Figure 1. Categorizations of data breaches (www.itffroc.org): (a) number of breach incidents and (b) number of records compromised.

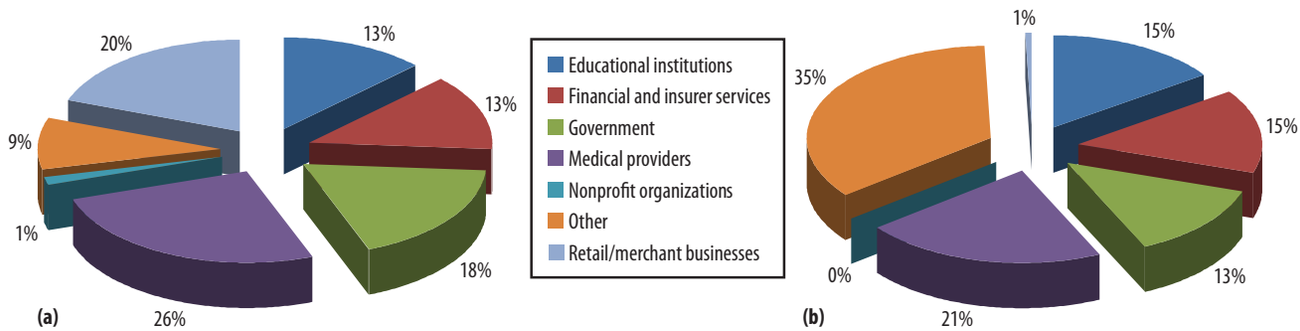

Figure 2. Data breaches by organizational type (www.itffroc.org): (a) number of breach incidents and (b) number of records compromised.

pack in terms of both the number of reported incidents and the number of records affected. Government and the financial industry vie for second and third. Just out of the running is education.

This is the strangeness in the proportions the title of this column refers to. Our trusted institutions produced a full 70 percent of the breaches and 64 percent of the compromised personal records. Weren't the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley (SOX) Act, and the Gramm-Leach-Bliley (GLB) Act supposed to fix these problems?

Think of this the next time your healthcare provider asks for your Social Security number, your university asks for your cell phone number, or your DMV puts your street address on your driver's license. Giving up such personal and private information in the absence of a compelling need to know is an invitation for abuse. Your physician should have a reasonable expectation of being paid for services, not of being able to access your Social Security retirement account.

The exceedingly bad idea of using SSNs as a primary database key dates back to 1943, when President Franklin Roosevelt extended the practice to US government databases (Executive Order 9397). It didn't take long before states and the private sector seized the opportunity to do likewise. And subsequent privacy legislation has had little to no effect in undoing the damage.

THE MADNESS BEHIND THE METHOD

The indirect cause of these privacy breaches ultimately lies in a subtle defect in the US Constitution: privacy—especially information privacy—isn't a right of citizenship. Life, liberty, and the pursuit of happiness, perhaps. Privacy, not so much. While the US Constitution offers some protection against government intrusion (at least it did until the Patriot Act era), the big threat in the Internet age comes from sources as diverse as CardSystems Solutions, Heartland Payment Systems, TJ Maxx, Sony Online Entertainment, the local DMV, the New York Yankees, the Atlanta YMCA, and Google.

Legal scholars have discussed the consequences of the neglect of privacy guarantees for many years. Future Supreme Court Justice Louis Brandeis and his law partner, Samuel Warren, suggested some remedies to this deficiency in their seminal paper "The Right to Privacy" in the Harvard Law Review in 1890 (http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html). Based on their concern about the loss of privacy that might

r1out.indd 88 12/20/11 11:25 AM

result from the handheld camera, they wrote, "Political, social, and economic changes entail the recognition of new rights." Had they anticipated the Internet, it's likely they would have added "technology" to the list of changes and made reference to information self-determination.

It's clear now that we've failed to pay heed to Warren and Brandeis' advice with the consequence that by the time that HIPAA, SOX, and GLB became law, the personal privacy toothpaste was already coming out of the common law tube. Patchwork attempts at amelioration have met with mixed success. Montana guarantees the right to privacy in its constitution. California's constitution considers privacy an inalienable right, and the state has led the way in legislating privacy protections with its breach notification and "shine the light" laws. Nevada has joined Minnesota and Washington to require PCI Data Security Standard (DSS) compliance of merchants who engage in credit card transactions.

These are all good signs, but in the end, they aren't effective enough. The patchwork approach of adding the safe harbor provisions of the law to ineffective enforcement and confusing jurisdictional issues doesn't work. The US Congress is considering federal legislation, but, based on past experience, it's unlikely that common sense will win out over special interests.

What would it take to fix the problem? Accountability and a reality check would provide a good starting place.

Accountability? How about a "hold harmful" clause: if you collect personal information on others that leads to their economic disadvantage, you have to make it right on your nickel. That would appeal to the business community like halitosis in a space helmet, but after the pro forma hue and cry, modern commerce would find a way to go on.

Reality check? We start with the recognition that computer hackers like Albert Gonzalez aren't the problem—they're a symptom of the problem. Absent this, we would have to count on institutions like our banks, healthcare providers, colleges, and governments to protect our privacy—not likely!

***Hal Berghel**, editor of the Out of Band column, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@berghel.net.*

cn Selected CS articles and columns are available for free at http://ComputingNow.computer.org.

CPS Conference Publishing Services

handles the details *so you don't have to!*

- Professional management and production of your publication
- Inclusion into the IEEE Xplore and CSDL Digital Libraries
- Access to CPS Online: Our Online Collaborative Publishing System
- Choose the product media type that works for your conference:
  Books, CDs/DVDs, USB Flash Drives, SD Cards, and Web-only delivery!

Contact CPS for a Quote Today!
www.computer.org/cps or cps@computer.org

IEEE

IEEE computer society

r1out.indd 89 12/20/11 11:25 AM