Have you got yours yet?

Glee Cady
Have you got yours yet?

Rights
Terms of use for work posted in CommonKnowledge.

This article is available at CommonKnowledge: http://commons.pacificu.edu/inter05/40
Have you got yours yet?

Posted on October 1, 2005 by Editor

By Glee Cady <gleecady@gmail.com>

“We write to inform you that your financial information may have been compromised…”

It’s only a matter of time, really, until you find yourself a recipient of an information breach notice. According to the reckoning kept by the excellent Privacy Rights Clearinghouse (http://www.privacyrights.org/ar/ChronDataBreaches.htm) more than 50,000,000 (yes, 50 Million) electronic records that contain sensitive information about people have gotten potentially into the wrong hands. The count grows higher every month. The tally is only as accurate as the reports, of course. By that I mean that in many systems it is impossible to accurately identify what records have been accessed. The size estimates of the breaches stem most likely from calculations of the total number of records in the affected data stores. To be responsible to their customers, record-keepers usually report the worst-case scenarios if they can’t determine exactly which records were exposed.

Thus, Houston, we record-keepers have several problems here.

Some of the data protection problems stem from our own naiveté, I think. It’s not that business is intending to expose information. After all, most businesses do not want their customer or employee information available to competitors or fraudsters, whether or not there is a law or regulation forbidding it. Exposing information helps neither the business nor the customer. Nor does releasing medical information or student information help the patient, the student, the medical facility or the school. Few record-keepers want their records exposed.

Hacking.

Breaches termed “hacking” really mean intrusions into systems that were not adequately protected: an insecure server, an unclosed or unlocked back-door.

Institutions of any size at all have lots of records. Not all the records are necessarily where the custodians think they are. We don’t necessarily know who made copies; we don’t know who viewed which records; and if we’re really unlucky, the copies we don’t know about aren’t
In many systems, it is very easy indeed for an authorized user to export some records out of a database: names and addresses, accounts with certain characteristics, or just a whole set of records unintentionally. Usually systems have features to do this built in. (On a personal level, look at the relative ease with which you could move your contact files from one email client to another.) The smaller database copy may be used for a mailing list, research or system testing, or providing an additional report that isn’t easy to tease out of the larger database. It’s easier to keep those records rather than to erase the files when our task is complete. After all, we might “need” the records again. Once several people have generated these private reports, we have “private data stores” scattered around an institution. Even if the institution has good data security practices, it’s pretty easy to set up a computer, put it on the local network, and if the person setting it up doesn’t really understand security processes, the system will be insecure from the get-go. Many new computers ship with “open” systems: default settings for administrator passwords, settings that make it easier for the manufacturer’s technical staff to diagnose problems from a remote location, for example.

Many systems supporting record-keeping; financial, medical, and school transcript information databases were designed and built in a time where disk space was very expensive and processing transactions as fast as possible was critical. This meant that logging at the data element, or even record level, was out of the question. It wouldn’t even have occurred to most system designers to think of logging as something to trade-off against some other design requirement. Simply put, the money wasn’t available to provide that level of diagnostic ability. “Journaling” or keeping a record of change transactions (usually in order to reconstruct a database in the even of a system failure) can be used sometimes in diagnostic traces. But that wouldn’t help us with simple viewing of records. That print screen key is both a help and an information leakage device.

Another system design trade-off that implementers have hesitated to make is encrypting the information, especially at the individual record level. With encryption, one trades processing speed for security. When each transaction has a cost and businesses have an obligation to their shareholders to keep costs down (see any Wall Street analyst report discussing viability and future prospects of a listed corporation), it’s hard for the security team to “sell” the concept until there is an incident. In the not too distant past, software encryption techniques could double or triple the processing time needed. This meant that only one-half to one-third of the number of transactions would fit through the “pipe”. Even worse, users got long delays waiting for their data result to appear. If users were on dial-up connections and located far from the main system, their sessions could easily “time out” in the middle of an inquiry. Screaming users on the help line can also affect programming design decisions.

Fortunately, encryption technology is improving (even as the bad guys are getting better) and installations of encryption devices are becoming not only feasible but common.
Intrusion detection systems have been in much the same place. These systems, as you would expect from their name, report when an intrusion is detected. “Tuning” the systems, so that they report actual problems rather than false alarms, requires very skilled and knowledgeable security engineers. Putting additional barriers in front of a database slows down the access. Slowing down access makes for unhappy customers, whether internal or external. And intrusion detection systems are frequently targeted in “other guy’s fault” finger-pointing during problem diagnosis sessions. The complexity of today’s system configurations makes fault diagnostics a real challenge.

**Stolen/mislaid Backup Tapes.**

Encryption can help record-keepers here. For many systems, the backup tapes, even if not encrypted, will be difficult (but not impossible, you understand) to read. The records would be in proprietary formats. And then you’d need the right kind of tape drive. Of course, if you have access to the right kind of data center and you have knowledge of the format, it’d be relatively simple. Offsite backup tapes are most often stored in reputable, bonded locations, but for some businesses, the computer center manager’s garage doubles as an offsite warehouse. Not because of incompetence, of course, but habit.

**Dishonest or disgruntled insider.**

This one scares us all. We can run background checks, We can monitor employees. We can try to make sure our customers are who they say they are. But we can’t always catch this one before something bad happens. And despite the growing concern about this problem, it still remains one of the biggest challenge for security managers.

**Stolen computer.**

One of the earliest reported financial information breaches came from research copies: a researcher was reviewing loan transaction records, investigating borrower behavior. The database was on a laptop, locked in an office. The office was burglarized and the laptop was missing. The financial records were vulnerable and no one (except the thief) knows if they were accessed. There have now been many instances of stolen computers. Law enforcement representatives believe that many of the stolen laptops are taken to gain the equipment rather than the information. In general, information thieves will steal servers rather than laptops: more bang for the buck. Owners of laptops with business or financial information are learning to be much more wary. Computers are locked away, even if in offices. They are not left in automobiles over night and not left unattended at all.

**Notifications.**

With the rising count of people affected, legislators and regulators have been working to provide additional regulatory safeguards. Much attention has been paid to the recent spate of legislation requiring record-keepers to notify the person owning the data if sensitive information has been lost, stolen, or possibly strayed. The laws are generally based on a California state law usually termed SB 1386. (The full code as enacted can be found here: http://www.privacyprotection.ca.gov/leg2002.htm.) This law helped by defining the
characteristics of “sensitive” data: combinations of information that may result in identity theft or other financial harm. Essentially, we are talking about the conjunction of enough information that a thief could gain a new credit account using your information, or charge something to an account you already have. Other states and the federal legislature have passed or are debating similar laws. The current status of these state efforts can be found here: http://www.pirg.org/consumer/credit/statelaws.htm#breach or here: http://www.ncsl.org/programs/lis/CIP/priv/breach.htm. EPIC tracks federal legislation here: http://www.epic.org/privacy/bill_track.html.

Notification laws won’t make information thieves go away. Nor will they magically protect your information. Notification letters won’t make you feel better. They will give you information and instructions. They’ll tell you what information may have been disclosed. They’ll tell you how to watch your credit accounts and how to contact the credit reporting institutions. If you receive one, at the very least, read it. Follow the instructions. Don’t ignore it. It’s the least you can do to protect yourself and others you care about. It’s a start.

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3173].