Security Breaches are good for you

A presentation by Adam Shostack at Shmoocon 2007, with some notes.

I begin with John Snow, and his work on Cholera.

Snow’s work on cholera is interesting because it predates Pasteur’s work on germ transmission of disease, and in fact led to public health as a field. Snow did his work with Henry Whitehead, a priest. Both risked death to gather data on mortality while a plague infested the area around Broad Street.

Snow wasn’t sure precisely what data to gather, but he collected information, learned from it, and proposed that removing the handle of the Broad street pump would hasten the end of the epidemic.

(More on Snow is in Steven Johnson’s “The Ghost Map,” which I highly recommend.)

In contrast, getting good data about information security is much harder. There’s lots of walled gardens of data, where the data is sanitized, and it’s hard to use or learn from.

So, why can’t we share? There are four reasons usually given: liability, embarrassment, customers would flee, and we might lose our jobs.

I quote Dan Geer as saying “No CSO on Wall Street has the authority to share even firewall logs because no General Counsel can see the point.”

I believe that breach disclosure changes everything.
A sincere thank you to ChoicePoint for helping to bring this about, even if that wasn’t their plan.

Choicepoint was one of the first companies to be required to report to the public that they had lost control of personal data. In their case, it was a Nigerian con man, who accessed data on 36,000 Californians and 127,000 other people to commit fraud by impersonation. For a variety of reasons, the story made a perfect storm around the new laws, and helped to publicize them.

Unfortunately for my thesis, the fact is Choicepoint was fined, I mock them extensively on my blog at http://www.emergentchaos.com/archives/cat_choicepoint.html, they lost customers, and their CSO now works at PriceWaterhouse Coopers. Not very good news when I claimed that the issues of liability, embarrassment, loss of customers and jobs were chimeras.

Choicepoint is an outlier, and has suffered unusually. We can learn this by looking at the Dataloss database maintained at http://attrition.org/dataloss/dldoss.html. In early March, it contained 560 records, and most of them have not resulted in customers fleeing or people losing their jobs.

I can make the first claim because of work by Acquisiti, Friedman, and Telang in “Is there a Cost to Privacy Breaches? An Event Study.” I quote from their abstract, and summarize it as “2 days, a few %, and then companies (stock prices) recover.” The Ponemon Institute offers a different analysis: that it’s expensive to notify, and that customers flee.

What’s important is that we can actually propose a hypothesis, experiment, and see what’s happening with real world data. We can also analyze methodologies, and comment on the data.

We can do this because we have data.
We can also look at the question of if customers flee. The market doesn’t seem to think they do, because when I looked at SEC filings to try to find companies warning their investors that customers would flee, I couldn’t find any. My approach was to choose several companies with unusual names, and search EDGAR for their filings. I tried to find one that was telling investors that they expected to see lower revenues.

In the age of Sarbanes-Oxley, I believe that no mention of the issues is telling.

Next I look at the issue of embarrassment. There are over 500 reports in the media, and most don’t seem to be really embarrassing. More interesting is a trend towards reporters talking in tones of moral outrage over failures to notify. Watch for that in stories.

There are also reports from places where the law doesn’t require notice, and where the law is unclear. I believe these are evidence that there’s a perceived moral and ethical requirement to disclose, and disclose quickly.

If people lose their jobs, we should be able to discover that via survey. I think the numbers are really low based on informal observation.

Some notes about the laws: California’s 1386 started it all, there are now 34 other laws. See [http://www.perkinsoie.com/statebreachchart/chart.pdf](http://www.perkinsoie.com/statebreachchart/chart.pdf). Also note that the Australian and some Canadian Privacy Commissioners are interpreting their extant laws as requiring notification.

So breach disclosure is good for you. It allows us to overcome fears. It allows us to discuss some of our problems in a forthright manner. We can use the data to start investigating what happens and why. The data isn’t great, but I expect it will get better.

Most importantly, we’re talking about failures, and the sky is not falling.
The Ontario/British Columbia breach notification form, which companies must fill out, asks what happened, and what you’ll do to make sure it doesn’t happen again. We could thus think about studying the things companies say they’ll do, and see if they show up again.

I hope the data is subject to Freedom of Information Act requests.

We can use data to answer questions, like what fraction of incidents are caused by insiders? This has long been contentious, but if we can agree on what an incident is, what an insider is, and what cause is, we can learn something.

The details aren’t important, what’s important is that we can stop going around and around on matters of opinion, and replace them with data.

The final slide refutes the Shmoocon slogan of “Less Moose than Ever” with the consistent zero moose sightings at Shmoocon, and asks if we could have negative moose.

You shall know the truth, and the truth shall set you free.