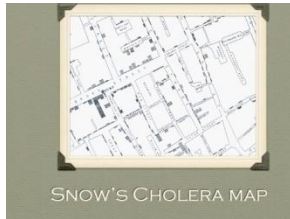


# Security Breaches are good for you

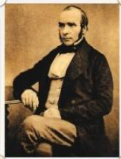
A presentation by Adam Shostack at Shmooccon 2007, with some notes.



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

### Investigation of Cholera

- No public health department
  - No bacteria theory of transmission
- John Snow, physician
- Henry Whitehead, priest
- Gathered data which they thought mattered
- Competitive analysis



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.

### Investigation of Security

- Lack of public information
- Walled gardens of data
- When was the last time you read this?



(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.

### Why Can't We Share?

- Liability
- Embarrassment
- Customers would flee
- We'd lose our jobs!

"No CSO on Wall Street has the authority to share even firewall logs because no General Counsel can see the point. (Dan Geer)"

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.

## Thank you, Choicepoint!

- One of the first companies impacted by California's 1386
- Claimed data sales to fraudster only impacted 35,000 Californians
- 38 Attorneys General were skeptical!
- Media firestorm, drew attention to issues, law



Photo: New York Times

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.

## Except!

Prediction	Reality
• Liability	• \$15m fine
• Embarrassment	• <a href="http://www.emergentchaos.com/archives/cat_choicepoint.html">http://www.emergentchaos.com/archives/cat_choicepoint.html</a>
• Customers would flee	• Choicepoint fired customers
• We'd lose our jobs!	• CSO Baich now at PWC

*So where's the good for you?*

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](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

- Attrition Dataloss database
- 560 incidents (as of early March)
- <http://attrition.org/dataloss/dldoss.html>
- Most haven't shown such results:
  - Few firings
  - Customer fleeing limited

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.

## How Do we know?

- "Is There a Cost to Privacy Breaches? An Event Study," Alessandro Acquisti, Allan Friedman, and Rahul Telang. WEIS 2006 and ICIS 2006. (<http://www.helms.cmu.edu/acquisti/research.html>)
  - "We show that there exists a negative and statistically significant impact of data breaches on a company's market value on the announcement day for the breach. The cumulative effect increases in magnitudes over the day following the breach announcement, but then decreases and loses statistical significance."
  - Translation: 2 days, a few %, and then companies recover
- Ponemon Institute tells a different story (Studies for PGP, Vontu)
  - Expensive to notify, customers flee
  - Ponemon Institute would like to help you do a better job
  - May be seeing worst case, not typical cases

I can make the first claim because of work by Acquisti, 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.

## Notice that We're Doing Science?

- Hypothesis
- Experiments
- Real world data
- Analyze methodologies

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.

### Do Customers Flee?

- The market doesn't think so
- Ponemon does
- What do SEC filings say?
  - Unable to find any
  - Eg, Concentra Preferred Systems [2006-12-12]
    - Distinctive name, should be easy search
    - No mention in SEC filings I could find.
- Does it matter enough to tell investors?

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.

### Embarrassment?

- You're 1 in 500. Get over it. Customers have.
  - TJX, VA, CPS--outliers
- Ethical obligation to report
  - Reports from countries without laws (UK, Japan, Bahamas)
  - Reports in places where law is unclear (Canada)
  - Seen in news stories-look for the belief

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.

### Do People Lose their Jobs?

- Not a lot of news reports of job loss
- Possible to study the question
  - All you need is a phone and a few weeks
  - Call the 500 orgs in Attrition's list
  - Ask to speak to someone
  - Record the results

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.

### Breach Disclosure laws

- California's SB 1386 started it all
- <http://www.perkinscoie.com/statebreachchart/chart.pdf> lists 34 other laws
- Alberta, CA and Australian Privacy Commissioners interpret existing law as containing a duty of notification
- Efforts underway to create single national standard in US

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

### Breach Disclosure Is Good for you

- Overcome fears
- Mandate discussion of some aspects of some security issues
- Enable research into what happens and why
- Ontario/British Columbia reporting form contains interesting questions

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.

### Ontario/British Columbia Breach Notice Form

- Fascinating questions
- Results may be subject to Freedom of Information requests
- We sure hope so!

Information Required	
Date of the breach:	
Description of the breach:	
A general description of what happened:	
Categories of the information:	
Describe the information (appropriately assessed, collected, used or disclosed):	
Steps taken or to be taken to reduce the harm:	
Person responsible for the breach:	

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.

### Overcome Myths with Data

- Are 80% of incidents caused by insiders?
  - ... it indicates the speaker (like countless others) fell for the "80% myth," which is a statement claiming that 80% of all security incidents are caused by insiders. (document in [1]) (the history of this myth, I challenge anyone who believes the 80% myth to trace it back to some definable source. If you do you will find it leads nowhere reputable. (Richard Dieflich))
  - <http://www.mitre.org/projects/000650/04-secure-insiders-causes-80percent>
  - Different authors have different numbers (typically 60-90%)
  - None have sources whose data you can read, until last week!
- See Enderson, Kios, and Philip N. Howard. "A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records, 1990-2006."
  - Studied 589 incidents
  - 60% involved "organizational mismanagement"

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.

### Overcoming Myths (2)

- Who's right?
- I don't care
  - For purposes of this talk, anyway
- Data may let us stop going around and around

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.

### One Final Bit of data: Less Moose than ever?

- Reliable reports of moose
- 1 km radius
- During Shmoocon
- Negative Moose?

Year	Warden Park	National Zoologic Park (out.)
2005	4	0
2006	4	0
2007	4	0

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.

### Questions? Arguments?

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

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