Data on Data Breaches: Past, Present and Future

Adam Shostack and Chris Walsh
Emergent Chaos

This presentation represents the official position of the Emergent Chaos blog, not our employers

Welcome to Sevilla

Navigational charts were kept secret during the age of exploration

- Henry the Navigator encouraged exploration
- Wanted the results for competitive advantage
- Columbus ended up in the Caribbean
- Lots of sailors died at sea
- Maps are still secret in some places
  - They don’t like http://maps.google.com

We face navigation hazards, too

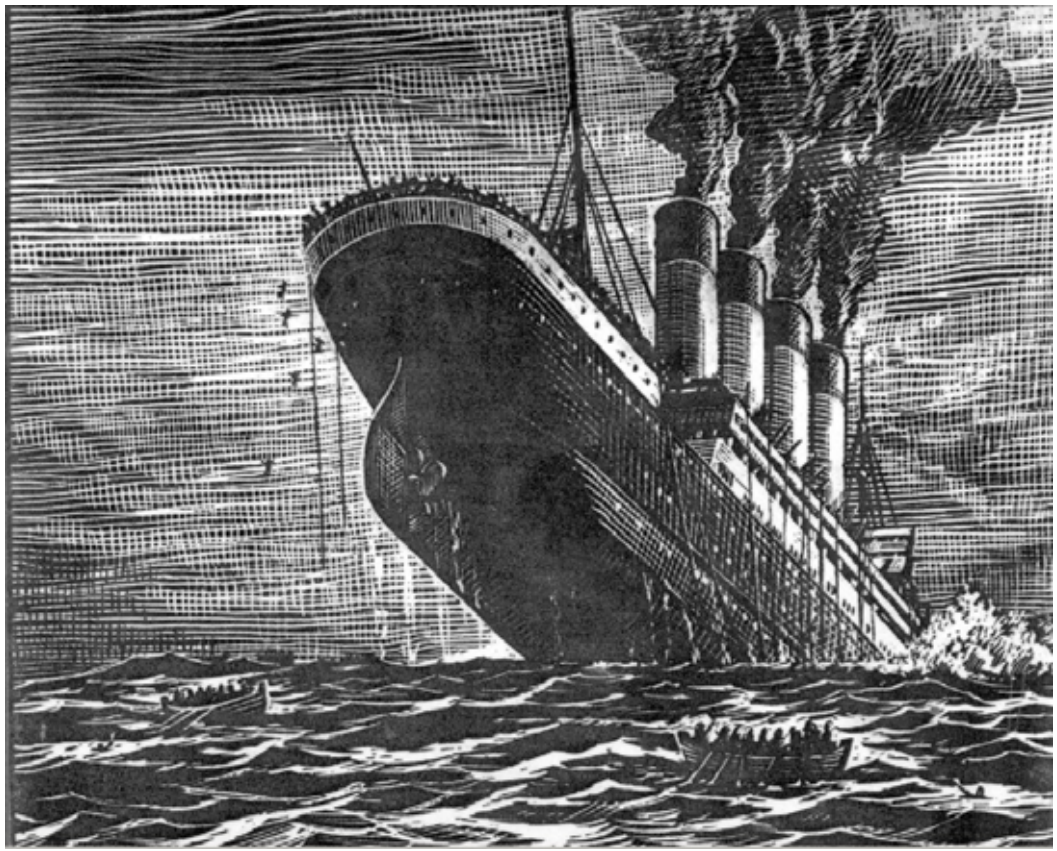


Image:http://www.materials.unsw.edu.au/news/brittlefracture/titanic%20sinking.jpg

We need to:

Know they exist :^)

Know how damaging they can be

Know our weak points if we run into them.

Know how to avoid them.

Case in Point: Security breaches involving personal information

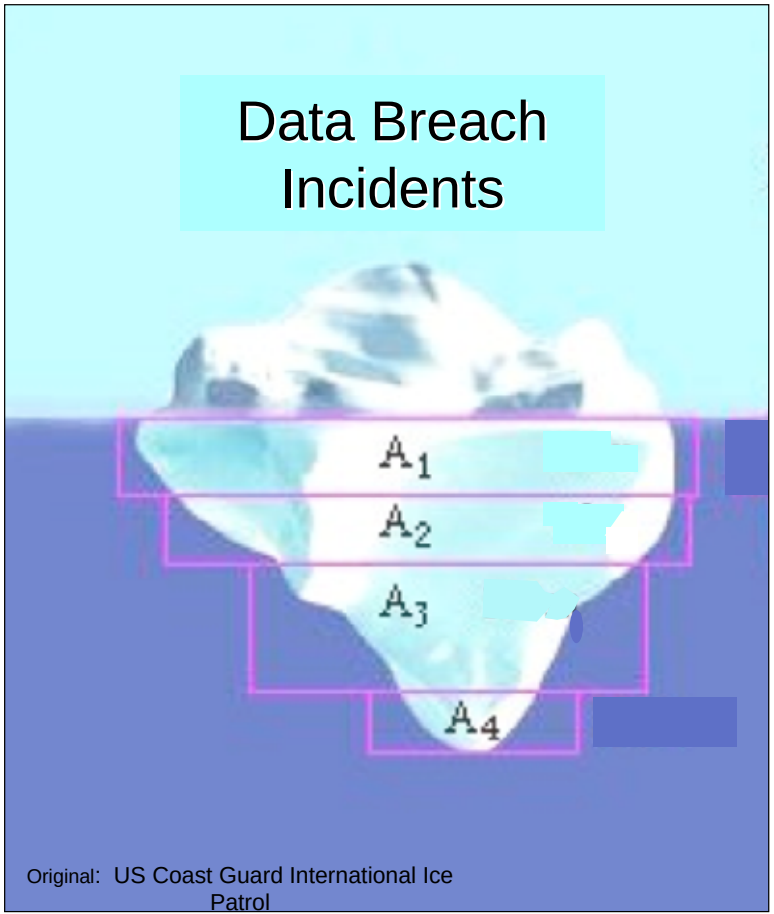
Definitely exist
But how numerous?
How do we know?
Are some more at risk than others?

Can be damaging
But how much so, and to whom?
How do we know?

Weak points driven by economics, not physics

Avoidance techniques must be strategic

Security Breaches: How numerous?



Below the waterline:

1. Undetected incidents
2. Unreported incidents
3. Reported, but unanalyzed
4. Reported, but privileged

Focus here is on 2, 3, and a little bit of 4.

How Do We Know?

Individual reports: News stories, press releases

Collections of same

-For general use - Emergent Chaos breaches category, Attrition.org's DLDOS, etc.

-Google Alerts are the researcher's friend

-For specific purposes - data behind a journal article

-Often use commercial news archives such as LexisNexis

Reports are much more numerous now that states have notification laws

Attrition's DLDOS

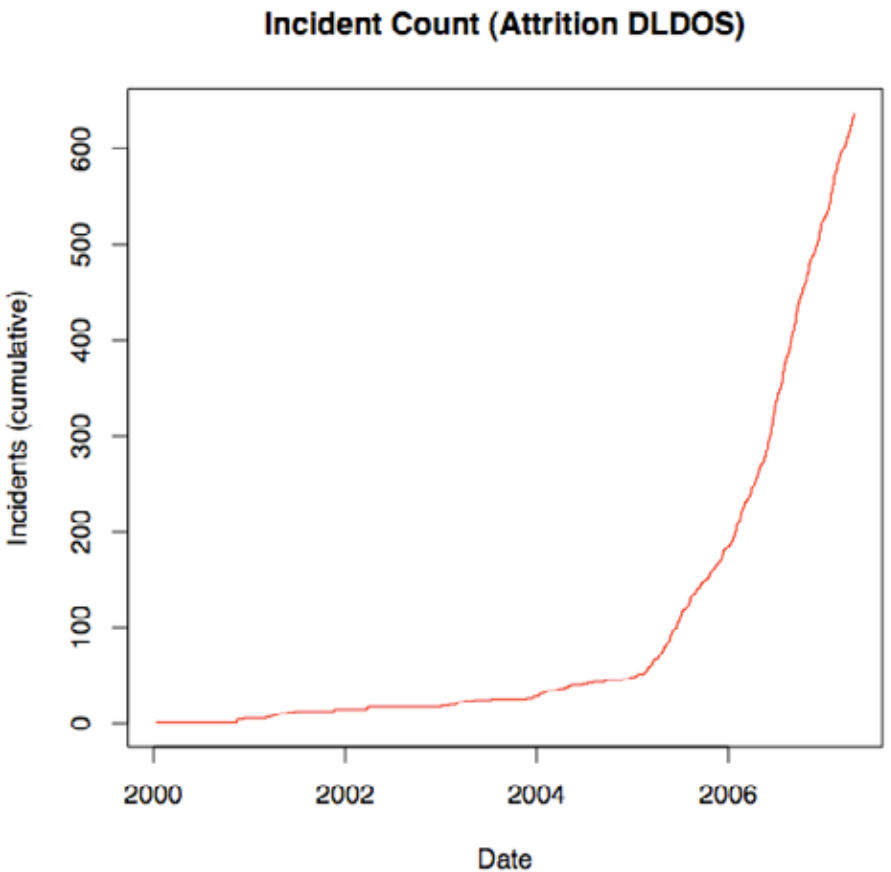
http://attrition.org/dataloss/dldos.html

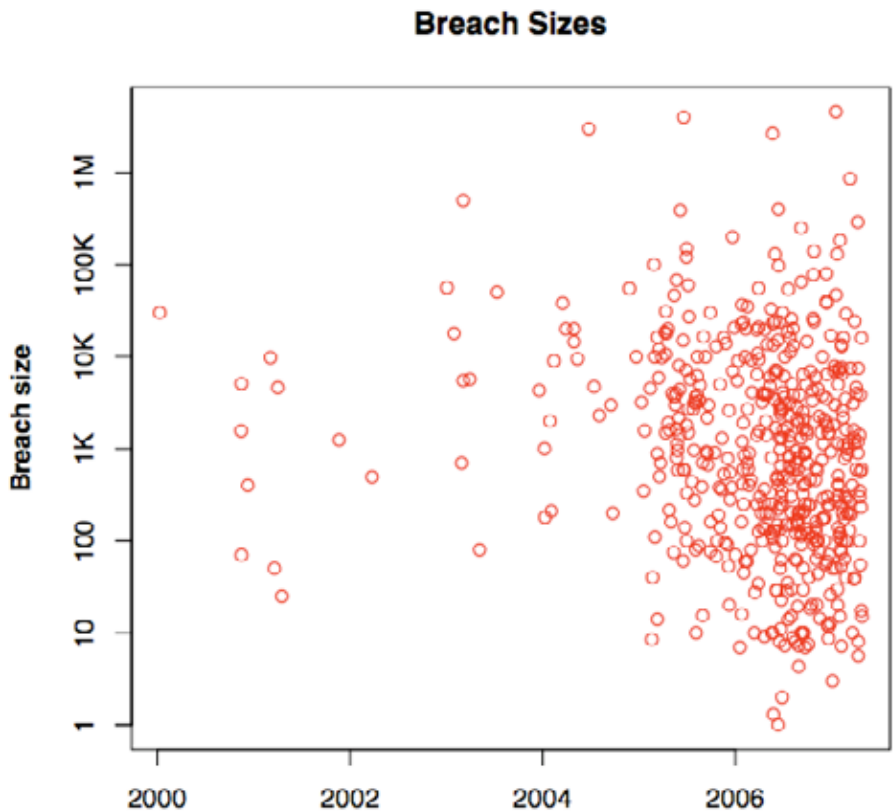
- Provides "date, the company that reported the breach, the type of data impacted, the number of records impacted, third party companies involved, and a few other sortable items"

- 700 records as of June 13, 2007.

- A main data supplier to other well-known sources, academic works, etc.

Attrition.org Incident Archive





Etiolated.org

etiolated consumer\citizen

Shedding light on who's doing what with your private information. Searchable Attrition.org DLDOS index.

Search: Go

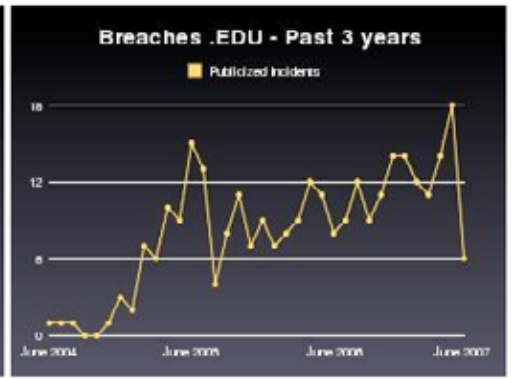
Main Statistics Research »Maps« Contact Login Signup Contribute!

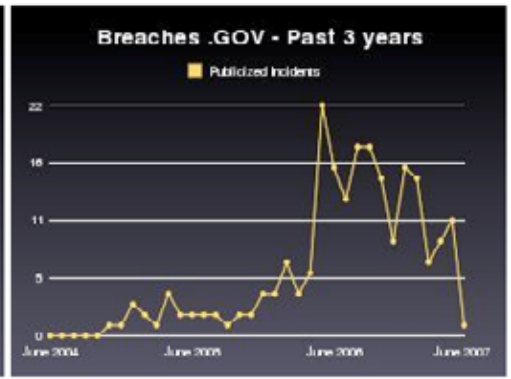
Largest Incidents Since 2000

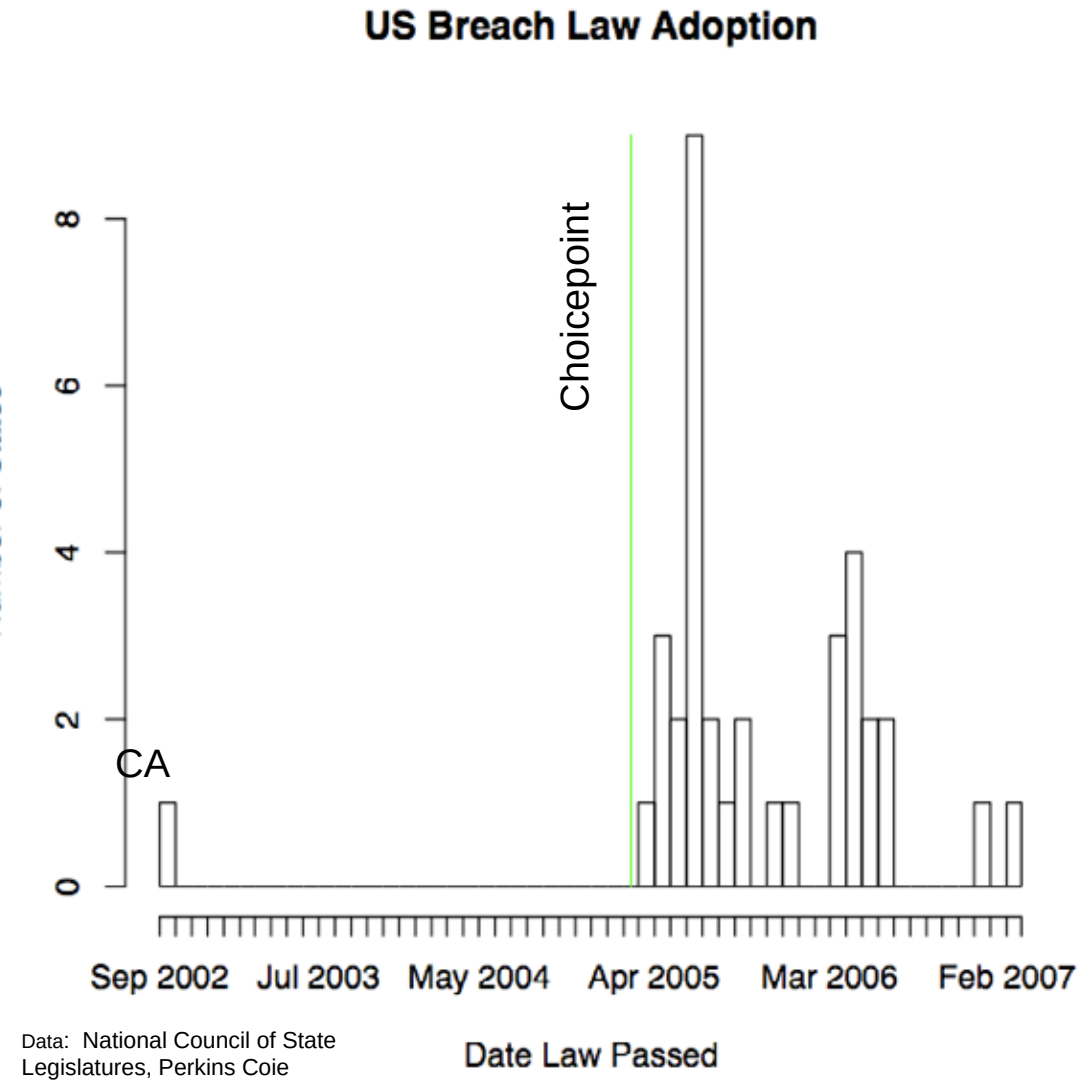
Number Affected	Date	Companies
45,700,000	2007-01-17	TJX Companies Inc.
40,000,000	2005-06-19	Visa, CardSystems, Mastercard, American Express
30,000,000	2004-06-24	America Online
26,500,000	2006-05-22	U.S. Department of Veterans Affairs
8,637,405	2007-03-12	Dai Nippon Printing Company
5,000,000	2003-03-06	Data Processors International
4,000,000	2006-06-13	KDDI
3,900,000	2005-06-06	Citigroup, UPS
2,900,000	2007-04-10	Georgia Department of Community Health, Affiliated Computer Services
2,500,000	2006-09-07	Chase Card Services

Most Recent Incidents

Number Affected	Date	Companies
3,000	2007-06-11	Grand Valley State University
17,000	2007-06-11	Pfizer
10,847	2007-06-11	Verus Inc., Stevens Hospital, Kennewick General Hospital, Concord Hospital
3,000	2007-06-09	Concordia Hospital
1,100	2007-06-08	University of Iowa
5,735	2007-06-08	University of Virginia
Zero or Unknown	2007-06-07	Deerfield Medical Building
Zero or Unknown	2007-06-06	Cedarburg High School
400	2007-06-03	Gadsden State Community College
4,000	2007-06-01	Northwestern University



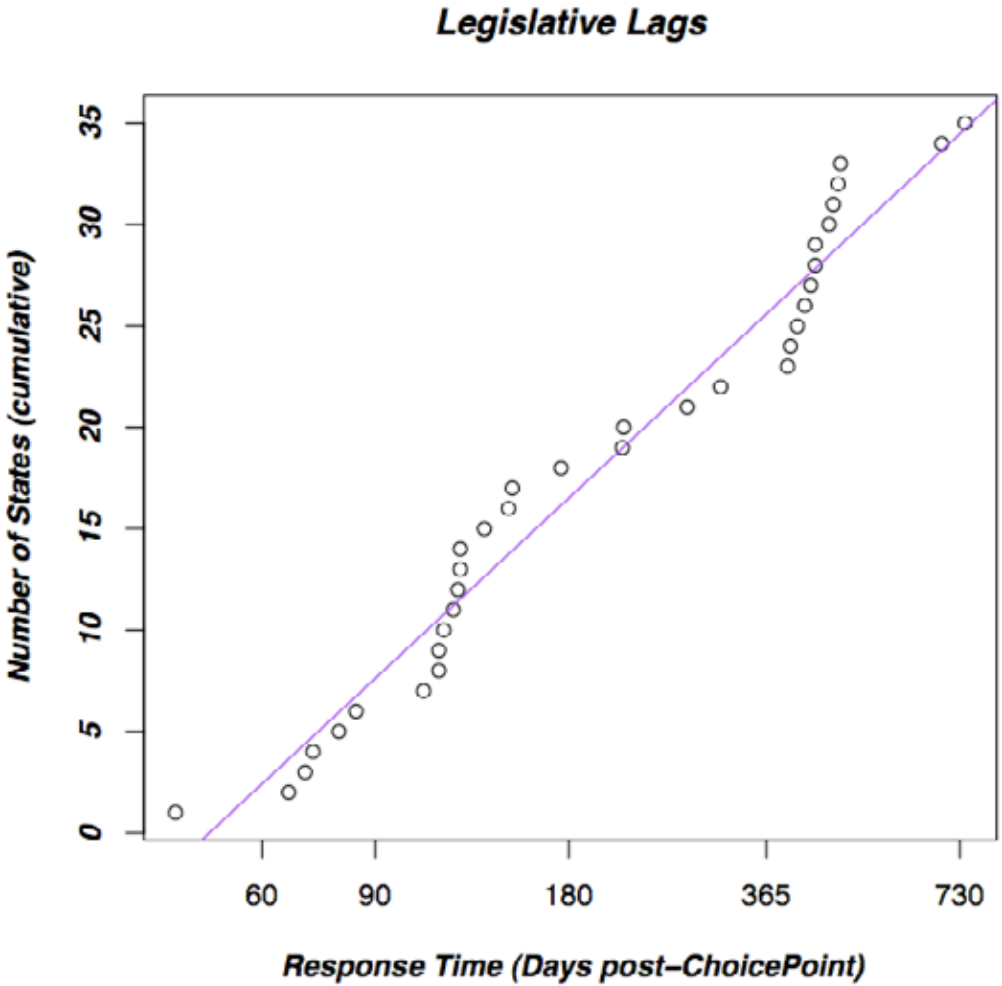




Data: National Council of State Legislatures, Perkins Coie

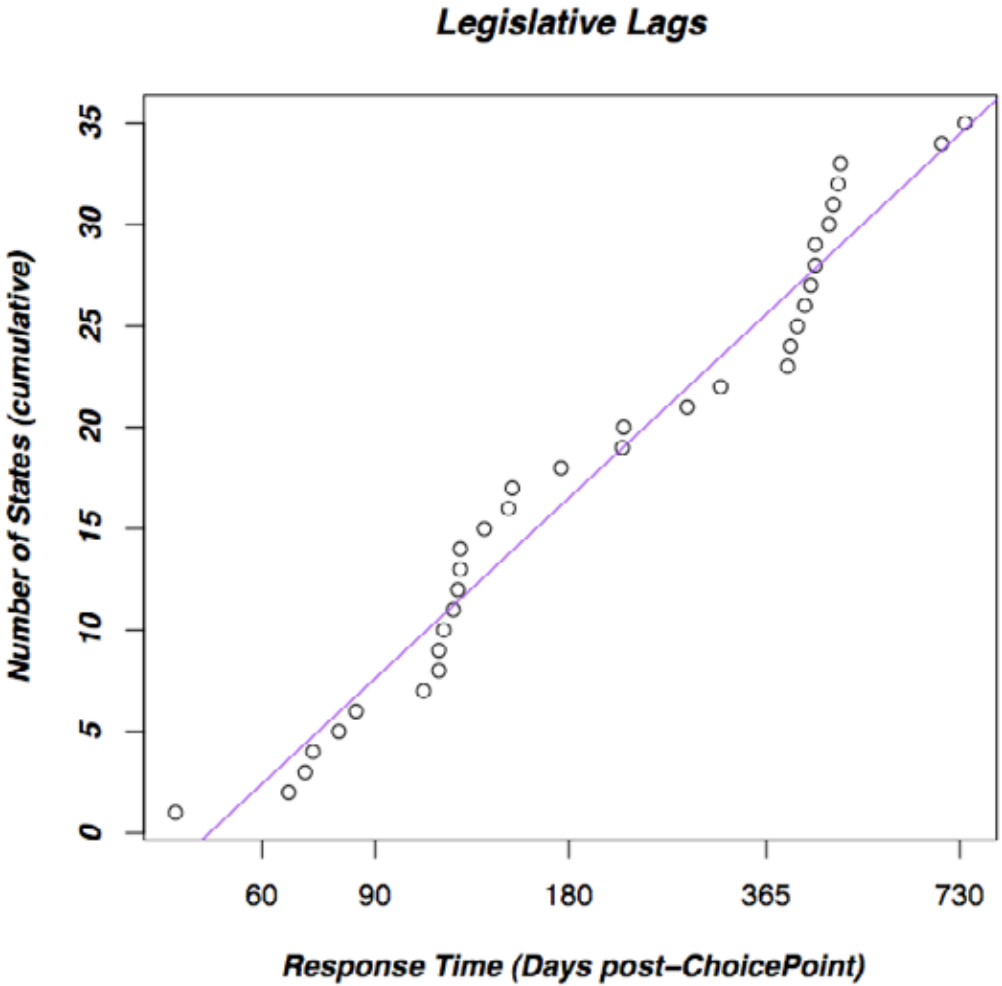
The Choicepoint incident certainly spurred legislative action.

U.S. State Breach Notification Laws



It is hard to measure the information security impact of these laws, in part because we only have two years' worth of data

Law passage times grow exponentially

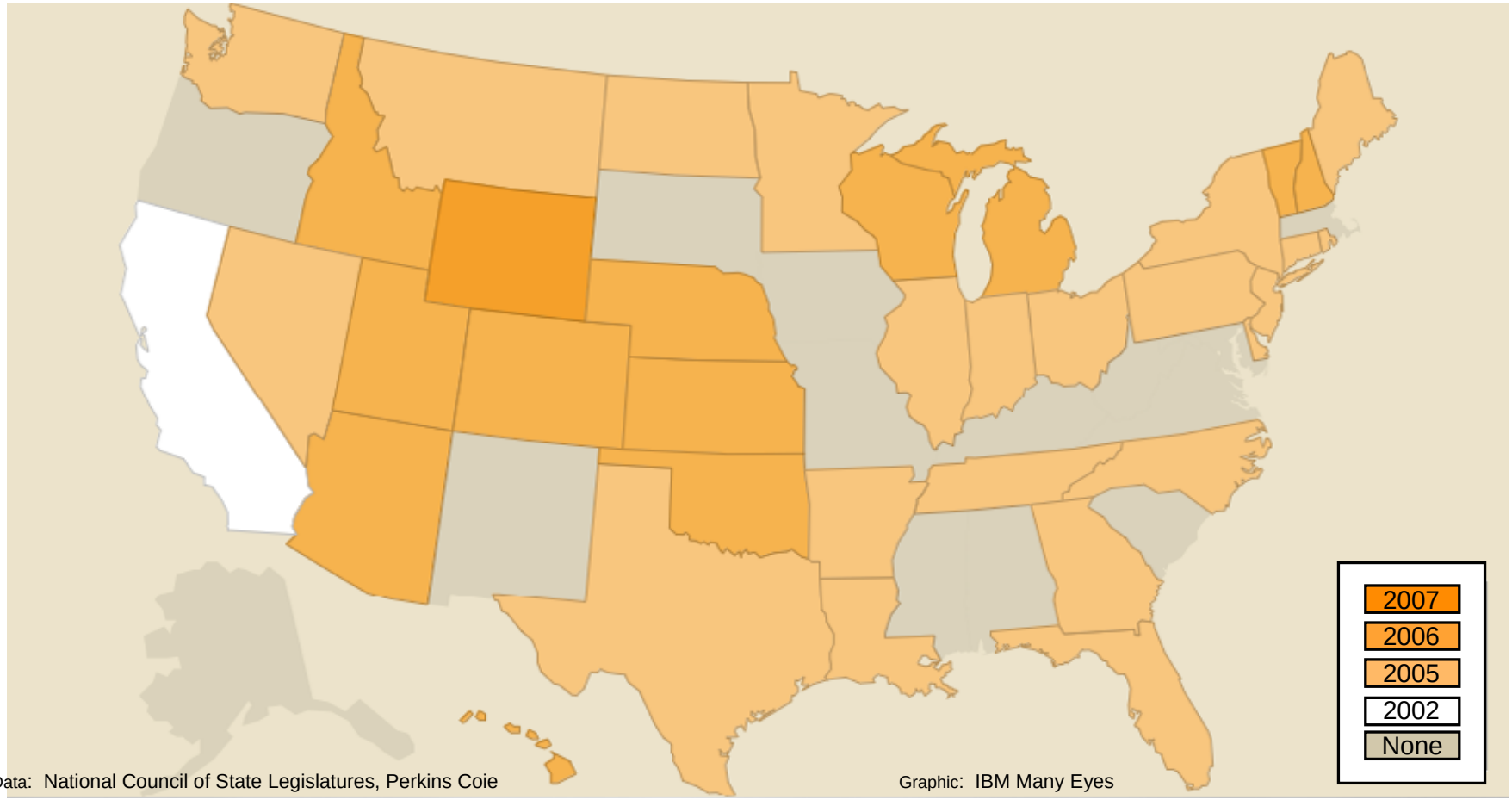


This extremely simple model suggests reporting will not be universally required for several years.

December 17, 2010

Take that with a grain of salt, but perhaps we should look closely at what these laws offer us and learn from it.

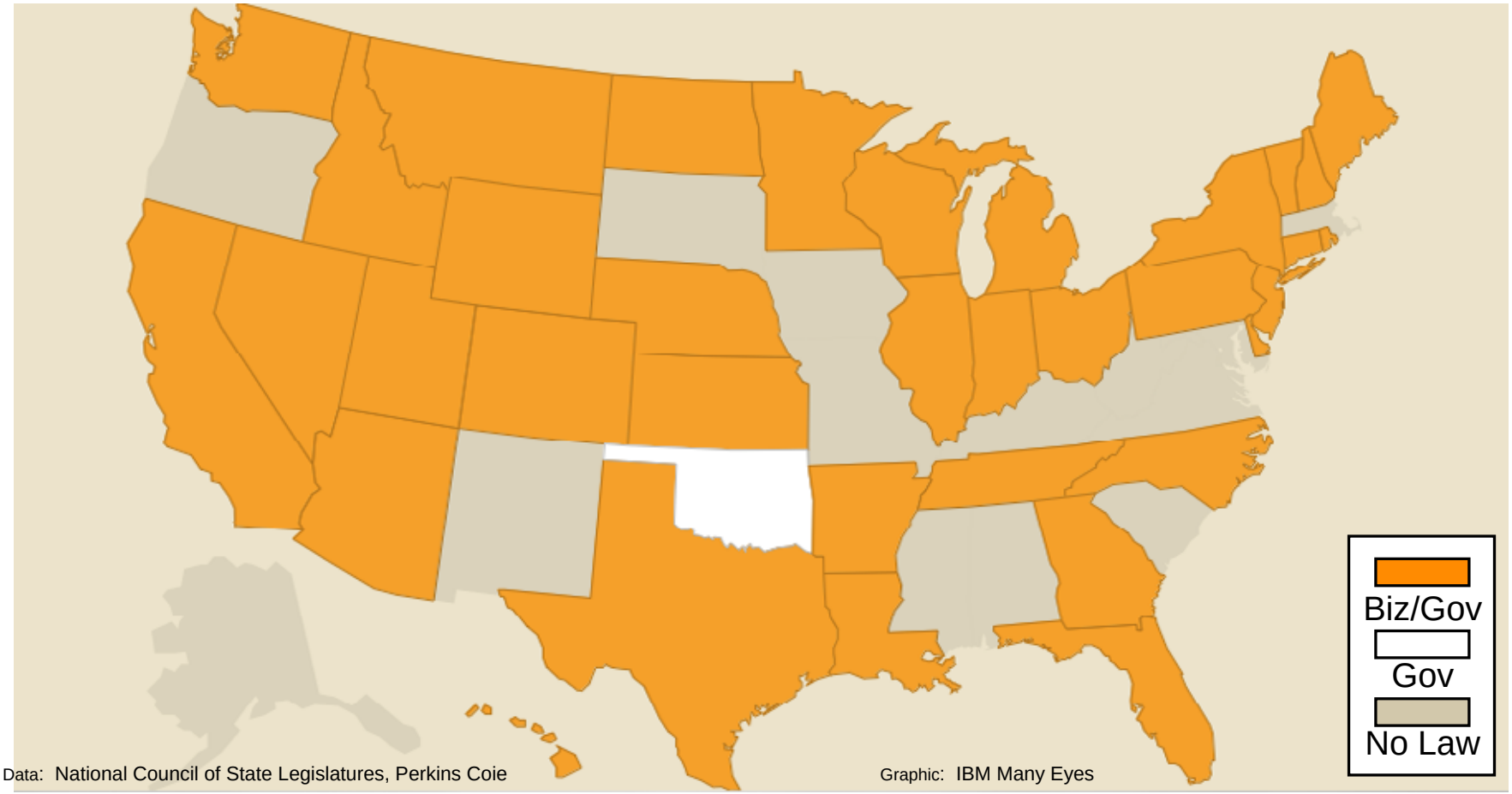
US Data Breach Laws: Date Passed



Data: National Council of State Legislatures, Perkins Coie

Graphic: IBM Many Eyes

US Data Breach Laws: Entities Covered



How Do We Know?

Reports required by national regulators

-Oversight committee reports

-FOIA

Reports required by states

-FOIA still needed (except in N.H.) but there are way fewer states than agencies

-Some primary sources available on-line

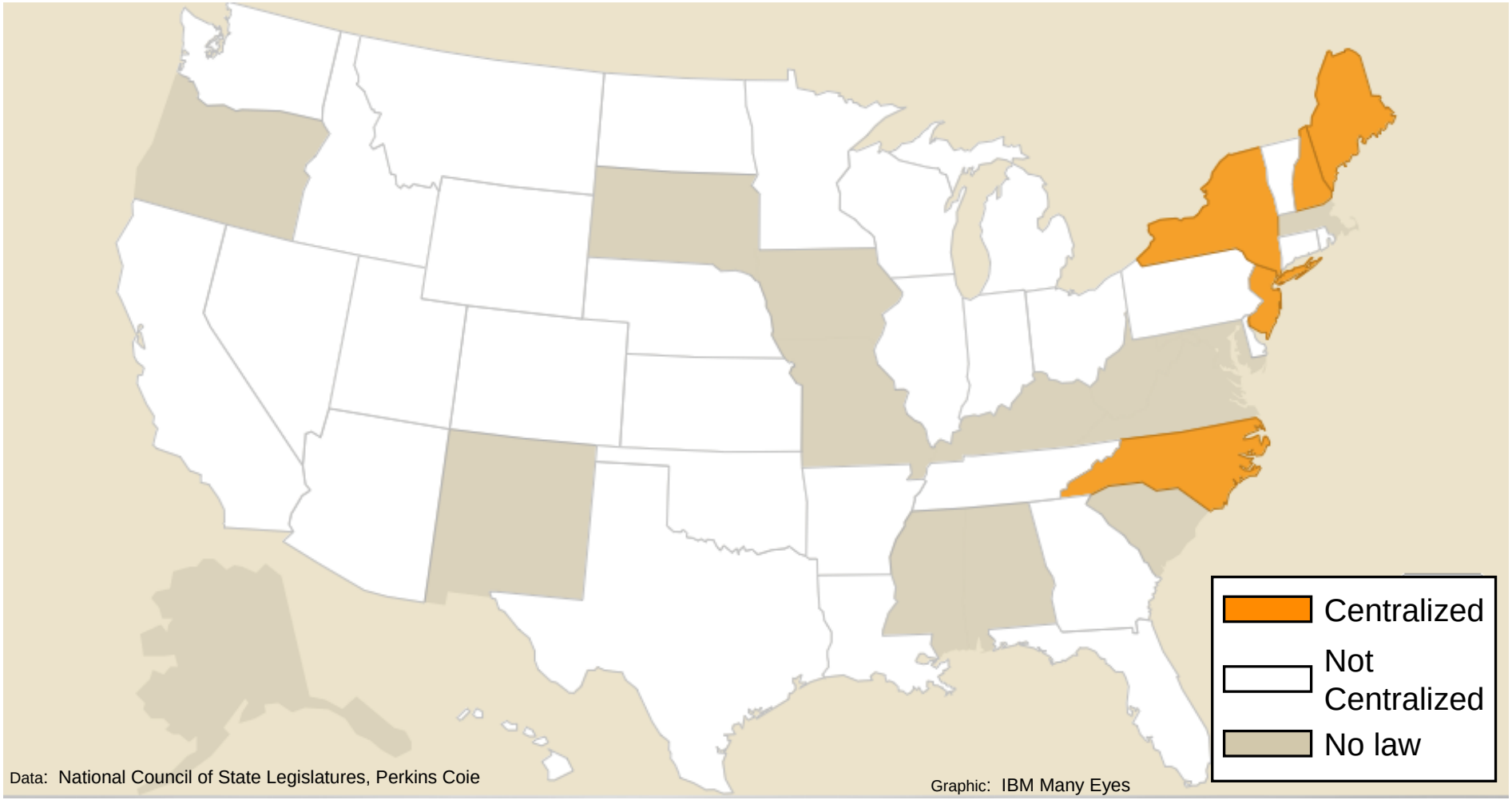
http://doj.nh.gov/consumer/breaches.html

http://www.cwalsh.org/cgi-bin/docview.pl

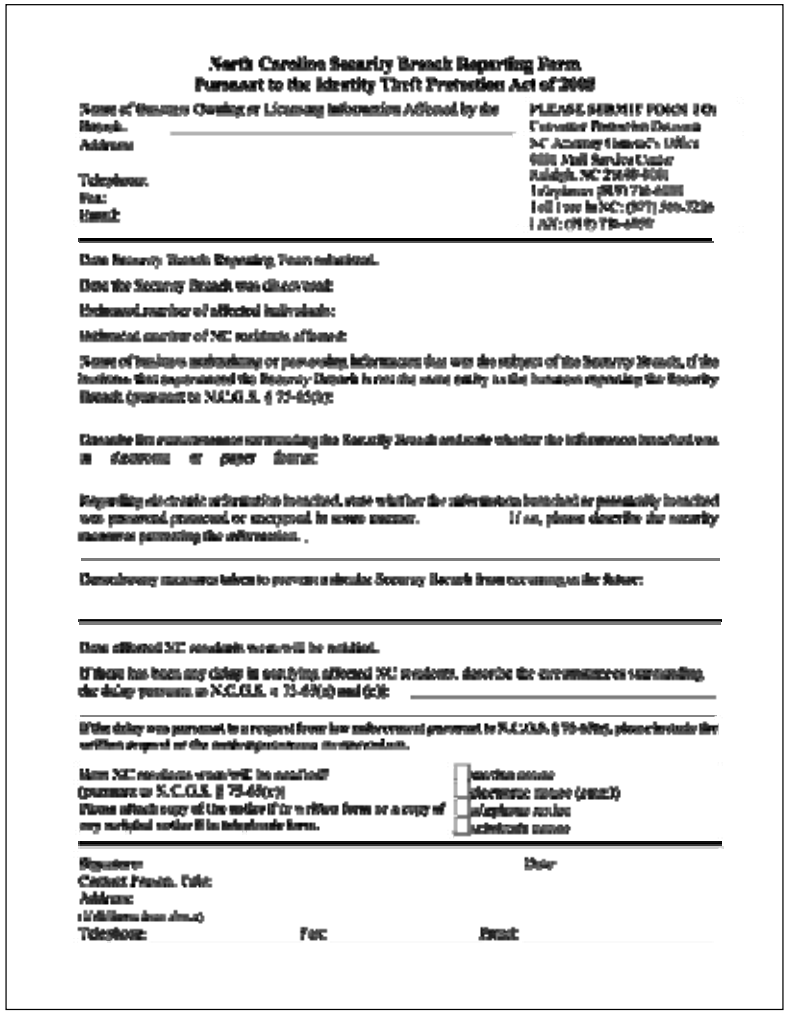
Question is: Do they add information, or just “more of the same”?

Test: Look at reports obtained by states, and reports obtained through “traditional means”. What, if anything, is added?

Central reporting is uncommon



What is collected by states?



North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach:
Address:

Telephone:
Fax:
Email:

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted:

Date the Security Breach was discovered:

Estimated number of affected individuals:

Estimated number of NC residents affected:

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)):

Describe the circumstances surrounding the Security Breach and note whether the information breached was in electronic or paper format:

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted, in some manner. If so, please describe the security measures protecting the information.

Describe any measures taken to prevent a similar Security Breach from occurring in the future:

Date affected NC residents were/will be notified:

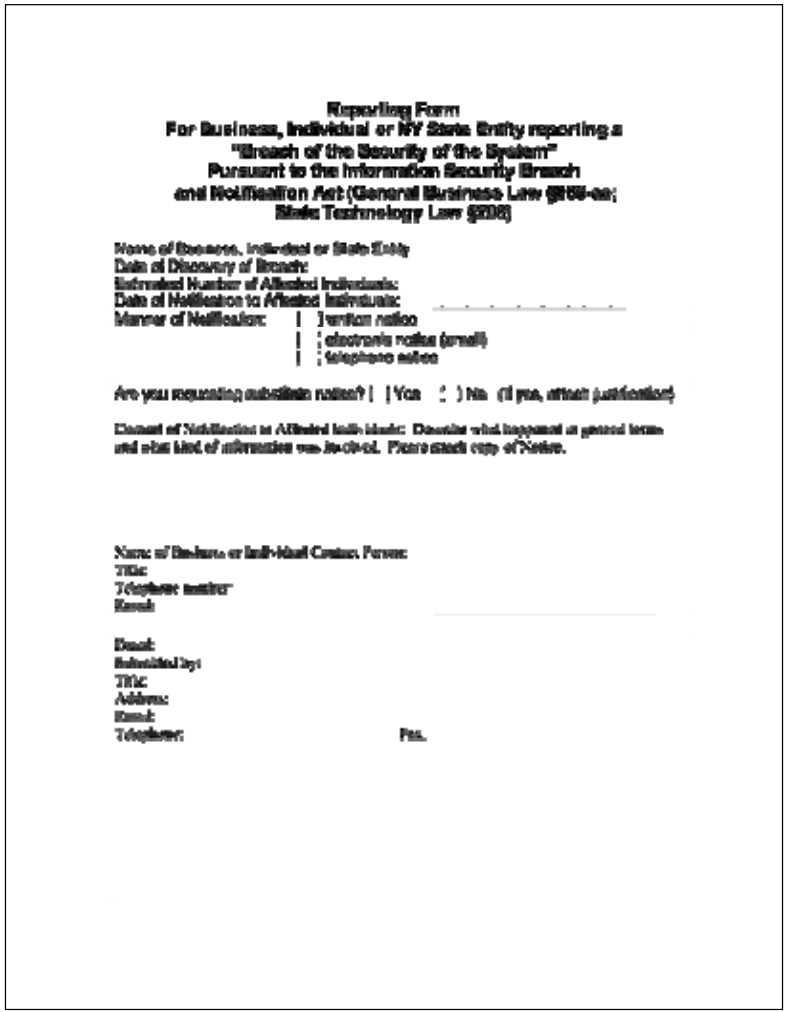
If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c):

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the memorandum documenting the request.

How NC residents were/will be notified (pursuant to N.C.G.S. § 75-65(e)):
Please attach copy of the notice if in written form or a copy of any script if in telephone form.

- ☐ Written notice
- ☐ Electronic notice (email)
- ☐ Telephone notice
- ☐ Substitute notice

Signature:
Contact Person, Title:
Address:
(if different from above)
Telephone:
Fax:
Email:
Date:



Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
and Notification Act (General Business Law §899-aa;
State Technology Law §208)

Name of Business, Individual or State Entity
Date of Discovery of Breach:
Estimated Number of Affected Individuals:
Date of Notification to Affected Individuals:
Manner of Notification: | | Written notice
| | Electronic notice (email)
| | Telephone notice

Are you requesting substitute notice? | | Yes | | No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

Name of Business or Individual Contact Person:
Title:
Telephone number:
Email:

Email:
Submitted by:
Title:
Address:
Email:
Telephone:
Fax:

A Quick Test

Look at incidents involving entities based in New York

Should all be reported to the state, since New Yorkers undoubtedly involved

Should appear in “traditional” reports

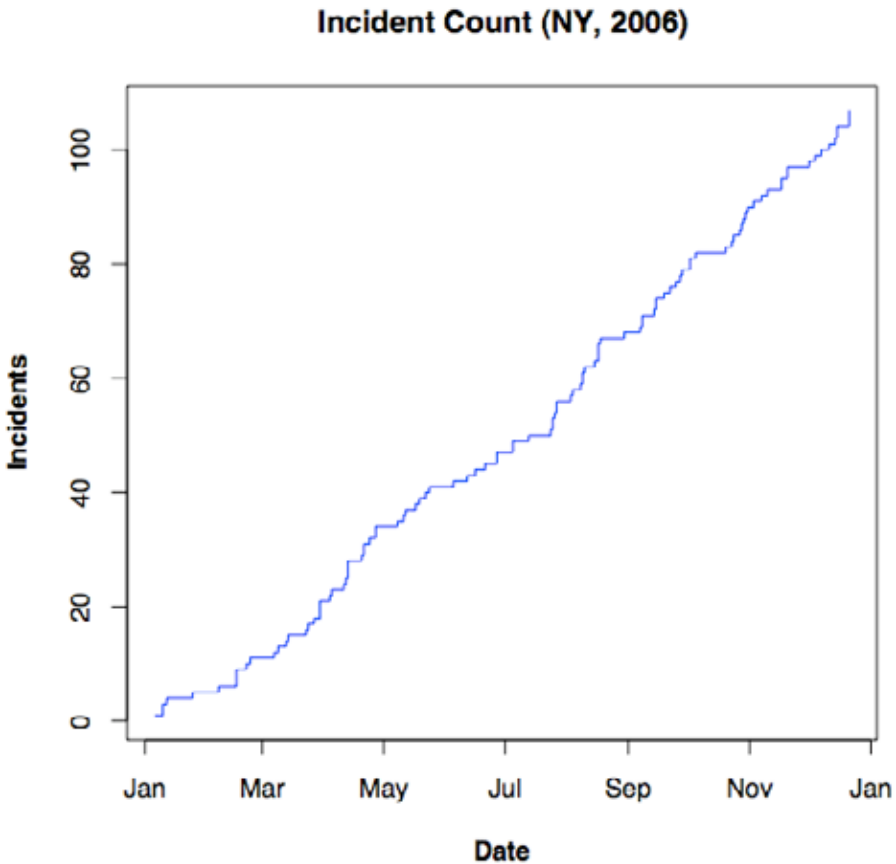
“Traditional” data set

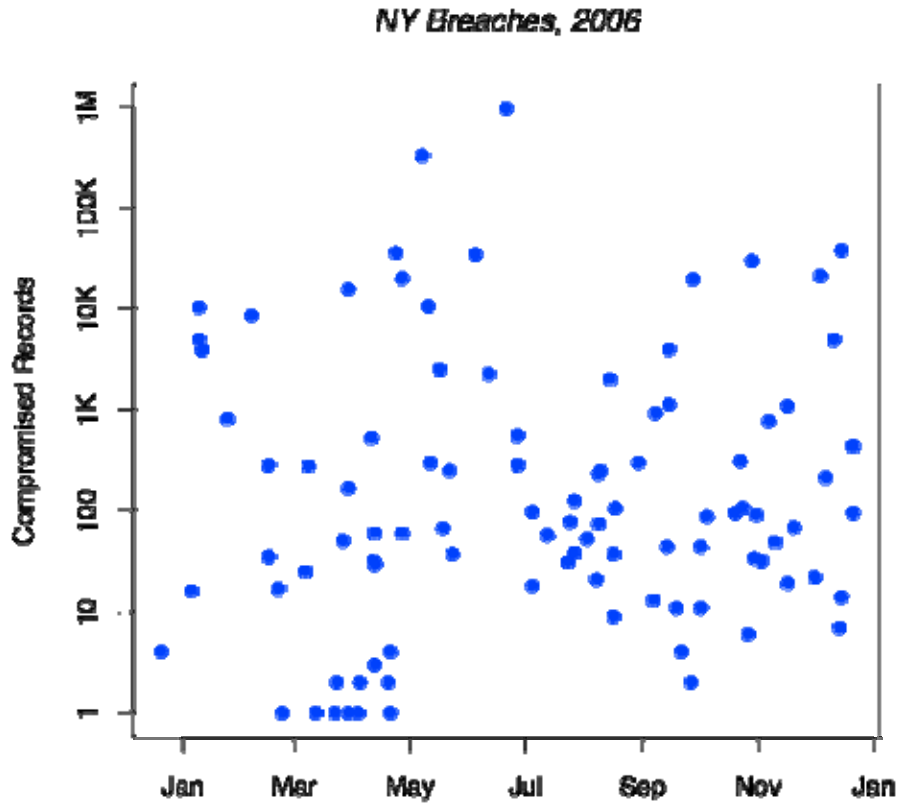
University of Washington (based on Attrition, Privacyrights.org, news reports)

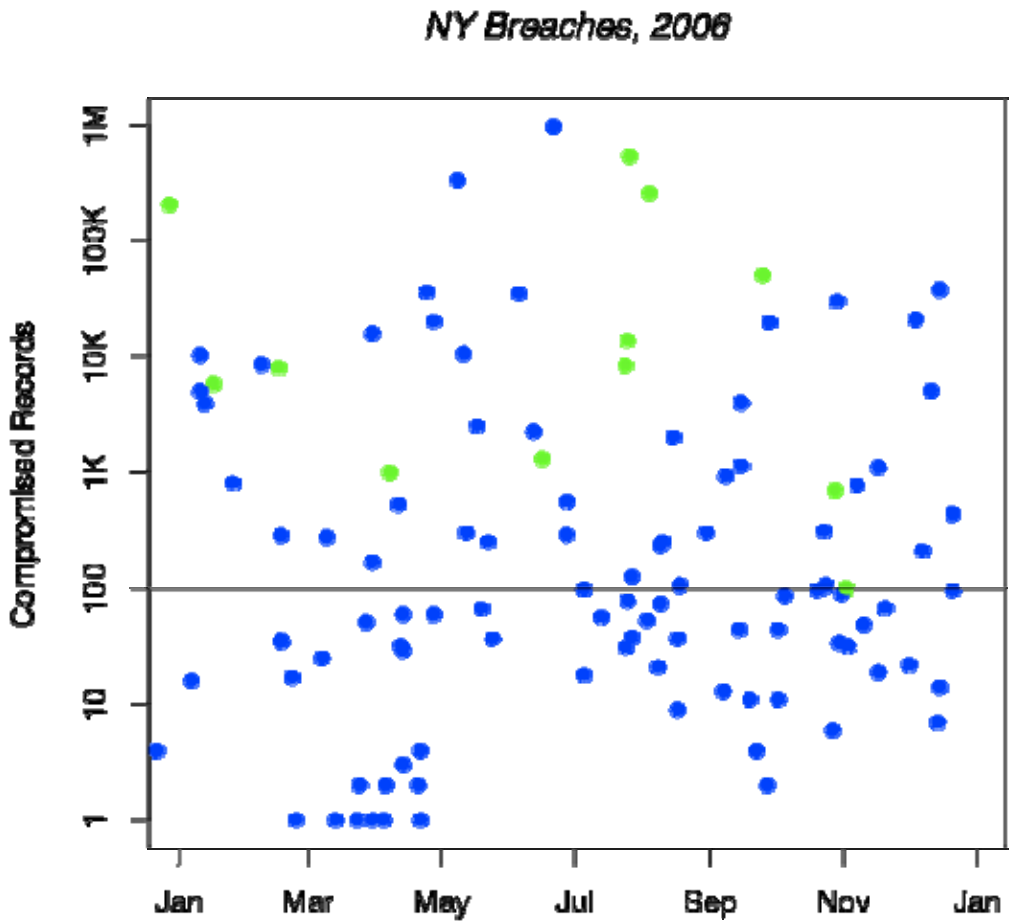
NY reports

Obtained via FOIA requests

f the picture is markedly different, state reports add value.


Incident Count (NY, 2006)
Incidents
0
20
40
60
80
100
Jan
Mar
May
Jul
Sep
Nov
Jan
Date

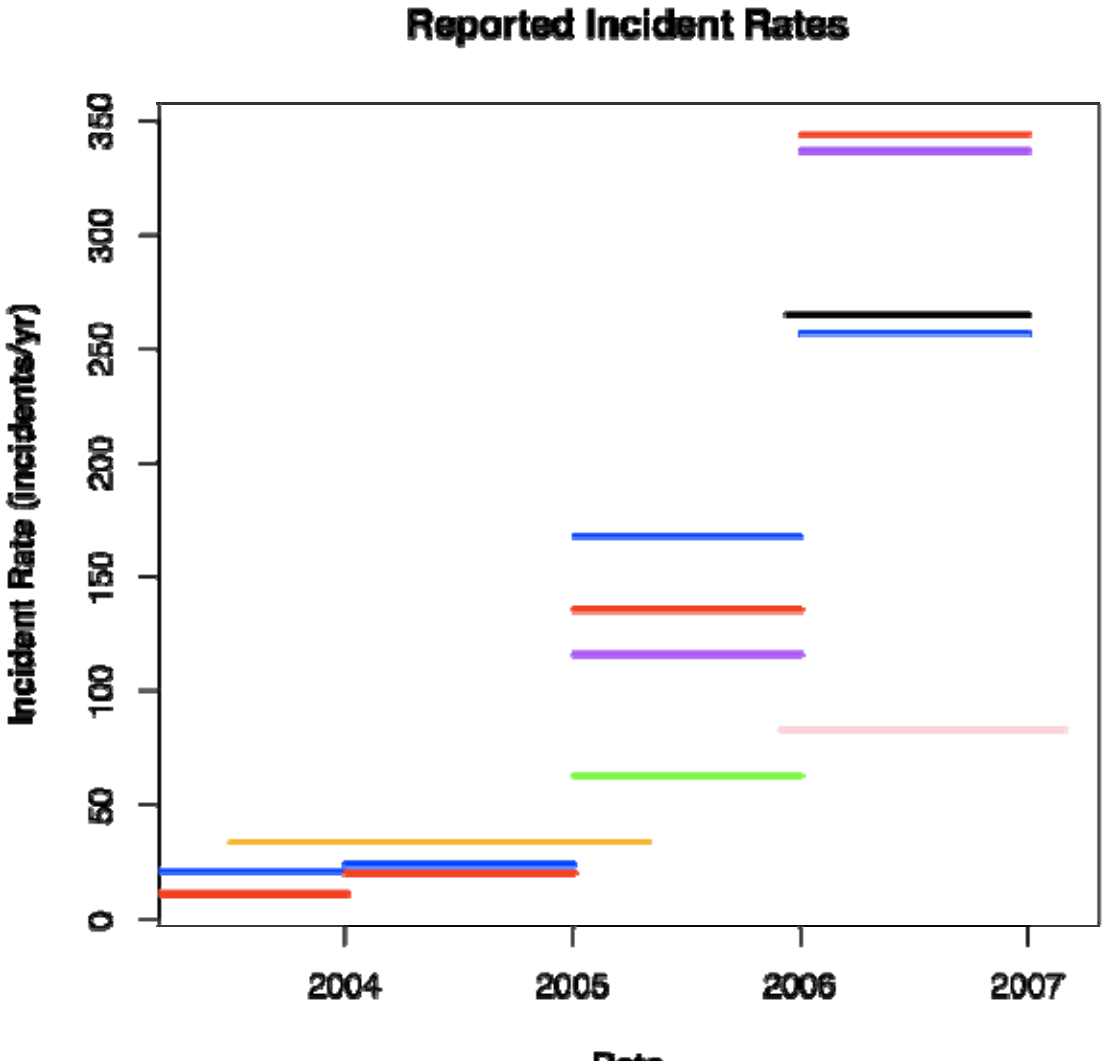

NY Breaches, 2006
Compromised Records
1
10
100
1K
10K
100K
1M
Jan
Mar
May
Jul
Sep
Nov
Jan



Green: University of Washington

Blue: New York reports

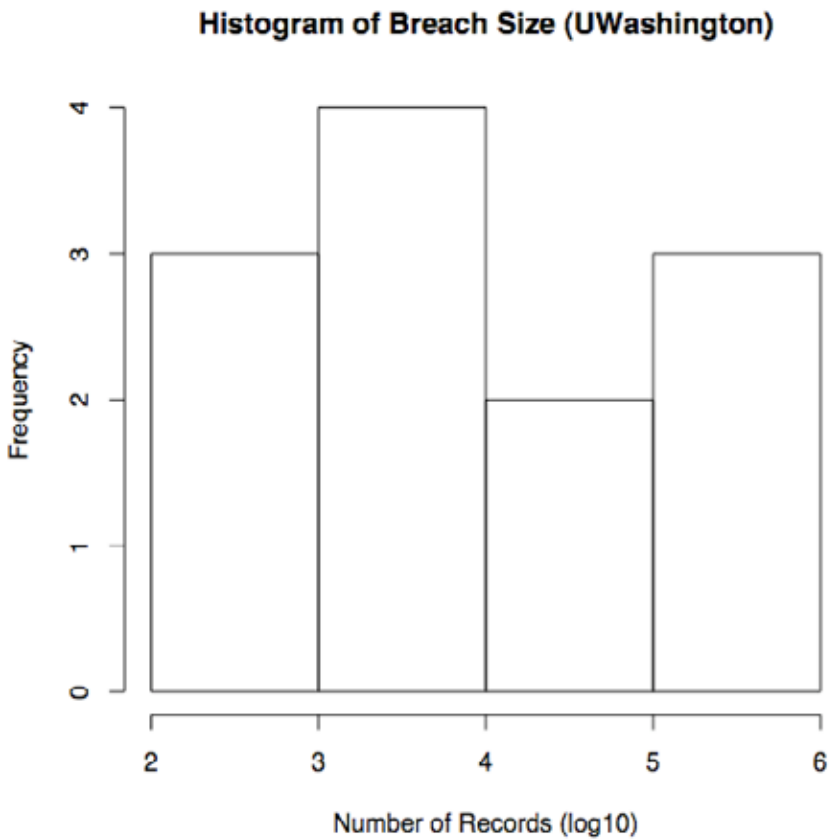
This is new information!

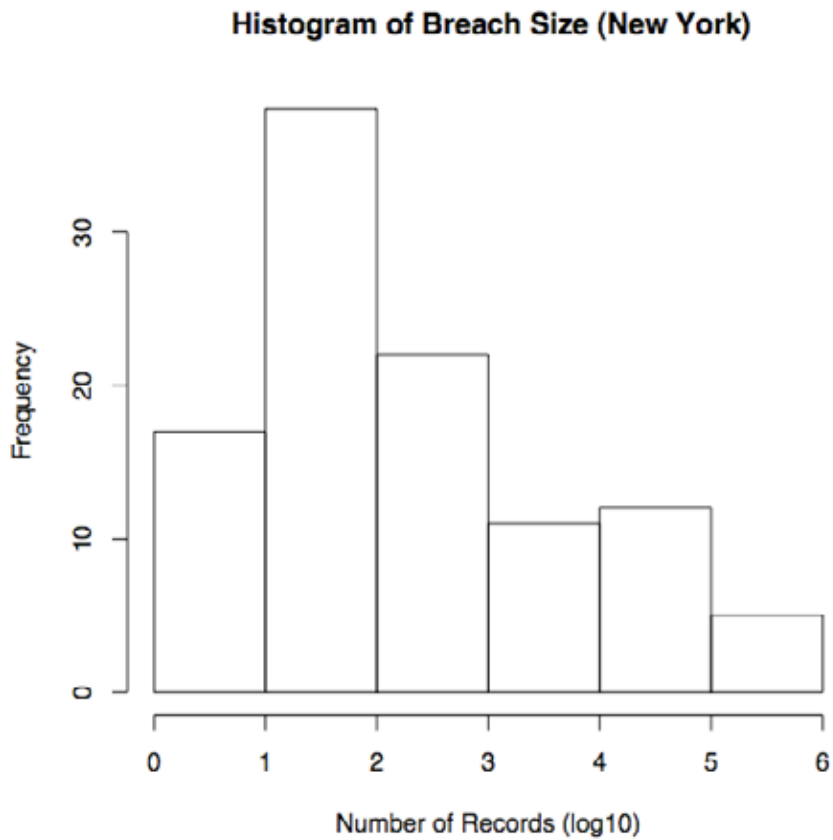


Line segments show incident observation rates for multiple sources, over time.

Attrition	
PrivacyRights	
UWashington	
UIUC	
NY	
NC	
CA	

The Bigger Stuff makes the news?





What are the weak points?

	Exposed Online	External Intrusion	Insider Abuse or Theft	Missing or Stolen Hardware	Mishandled	Other	Unspecified
UWash	3		1	8			
New York	17	7	3	65	2	4	3
New York > 99	5	3	1	37	2	0	2

Results for NY, and for NY cases with more than 99 individuals affected, are statistically indistinguishable

Lesson: Keep track of your stuff, and know how to configure your web server

	Exposed Online	Insider Abuse or Theft	Missing or Stolen Hardware
UWash	1.6%	0.5%	97.9%
New York	1.0%	0%	98.7%

Or, maybe ... Just keep track of your stuff!

	New York	UWash
Utilities	2	0
Manufacturing	2	2
Retail Trade	1	0
Transportation and Warehousing	2	2
Information	2	2
Finance and Insurance	34	2
Educational Services	28	0
Health and Social Assistance	16	2
Arts, Entertainment, Recreation	1	0
Accommodation and Food Service	1	1
Public Administration	14	3
Other Services	1	0

washingtonpost.com June 1, 2005:

The California Department of Consumer Affairs reported May 27 that since the state's notification law went into effect in July 2003, it has been aware of 61 significant breach notifications involving an average of 163,500 individuals each. About one-fourth of the breaches occurred at financial institutions and another one-fourth at universities, with 15 percent reported by medical institutions, 8 percent by government and 7 percent by retailers, according to the figures.

washingtonpost.com June 1, 2005:

The California Department of Consumer Affairs reported May 27 that since the state's notification law went into effect in July 2003, it has been aware of 61 significant breach notifications involving an average of 163,500 individuals each. About one-fourth of the breaches occurred at financial institutions and another one-fourth at universities, with 15 percent reported by medical institutions, 8 percent by government and 7 percent by retailers, according to the figures.

So what now?

Should we only care about lost/stolen media and hardware?

What about low-frequency, huge impact events?
Massive retailer breaches?
Card processor breaches?

Small breaches may also be signs of poor practices.

Additional reporting, and clarification of notification requirements would help us get the information we need to make risk decisions.

More states' information would help

- Would let us get a better handle on (seemingly) rare events
- Would expose biases (if any) in current, "traditional" reporting
- Would help us to assess whether breaches tend to be local, regional, or national
- Would better inform national and international policy makers
- Would better reveal the role of third parties as "impact magnifiers"

How to obtain this additional information?

- Revise existing laws to add central reporting
- Adopt breach notification requirements beyond U.S.
- Pass US Federal legislation
- Increase voluntary notification

Revise existing laws

- Require reporting to state Attorney General or consumer protection agency
- Standardize reporting to enhance comparability of states' data
- Close loopholes so that breached entity must report, whether it owns data or not.

Adopt breach notification requirements beyond U.S.

While privacy protections afforded to data subjects are significantly greater in many non-US nations, the extent to which these translate into different rates of data exposure is not known.

Pass US Federal Legislation

Legislation on a national level would eliminate a blind spot: federal agencies not bound by state law

Central reporting is critical: eliminates need to individually request data from scores of agencies

Increase Voluntary Reporting

- Higher notification trigger, but mandatory reporting to central entity?
- As means of limiting possible subsequent legal liability
- If you tell people, they can take steps, and thereby limit *your* risk
- Normative pressure: Customers expect it, law or no law
- Honesty never killed anybody: TJX sales rise after they tell of very large breach!
- Reflexive secrecy could be punished by regulators: why risk it?
- It's an assurance game: Sharing helps all if sufficient numbers share. We just need to get there.

Things We Might Care About

Breach consequences

Impact on stock price

Impact on customer loyalty/”churn”

Direct notification costs

Impact on identity theft

Repeat offenders? Do they learn?

Aspects of the notifications themselves

Do they show acceptance of responsibility?

Is there a clear “CYA” tone?

What level of detail do they provide?

Do standard forms increase the amount of information provided?

Thanks