

Data Breaches

Where are the Biggest Risks?
(A Work-In-Progress Report)

Suzanne Widup
Digital Forensics Association

Overview



Laws



Statistics



Trends

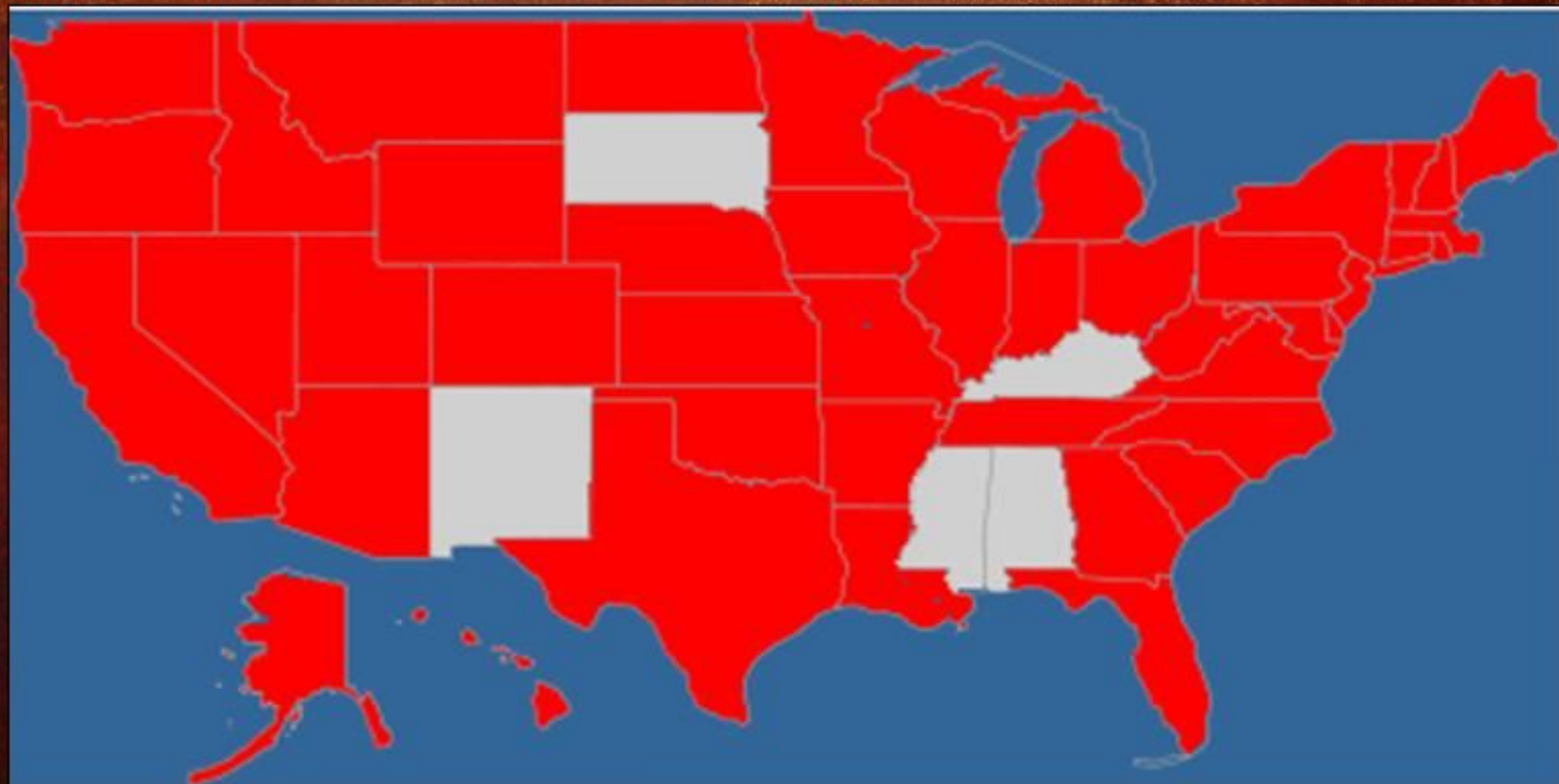
zanne Widup 2009. All Rights Reserved.

Then and Now

- 2003 California SB1386 was the first—many other states patterned theirs after this law.
- New laws augmenting existing
- No single Federal law

States with Breach Laws

45 states, plus Puerto Rico and the District of Columbia have breach notification laws now.



About the Study

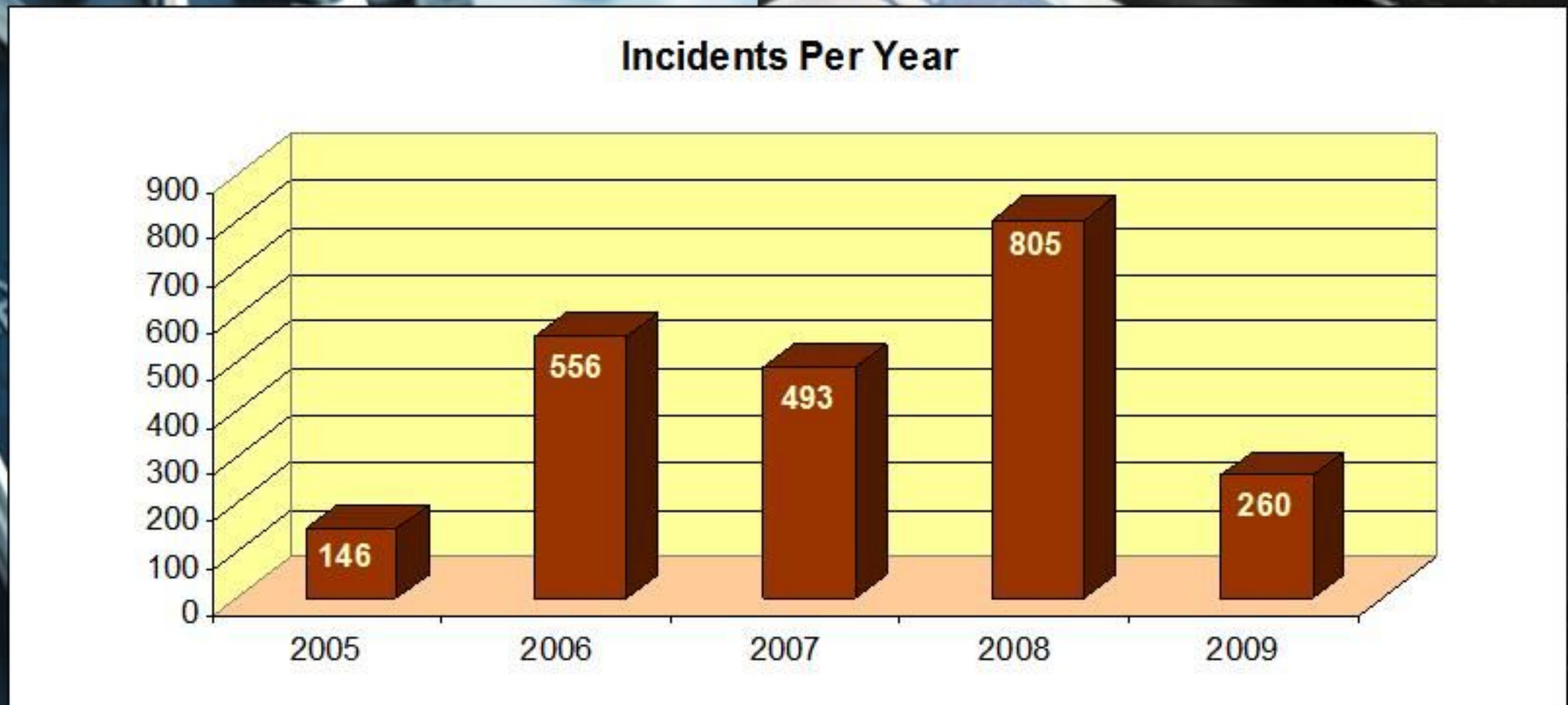
- Why conduct it?
- Where is the data from?
- How many records are there?
- How long a time period does it cover?

Data Sources

- DataLossDB (Open Security Foundation)
- Privacy Rights Clearinghouse
- Government sites
- Private tracking organizations

Data Breach Incidents

Number of Incidents (January 2005 – June 2009)

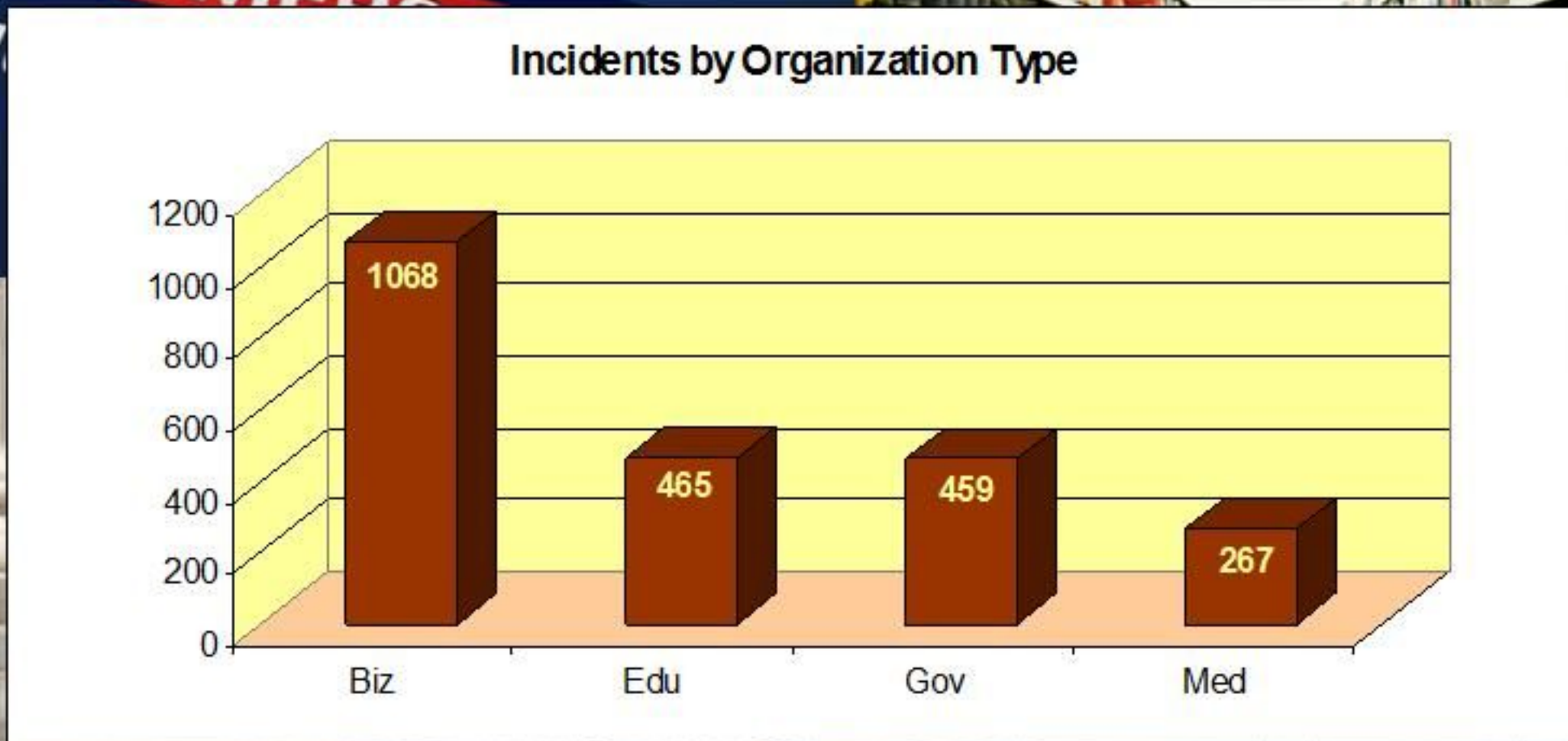


Top 5 Organizations for Number of Incidents

Organization	# Incidents
University of California (various)	17
LPL Financial	11
Experian	9
University of Iowa	9
California State University	8

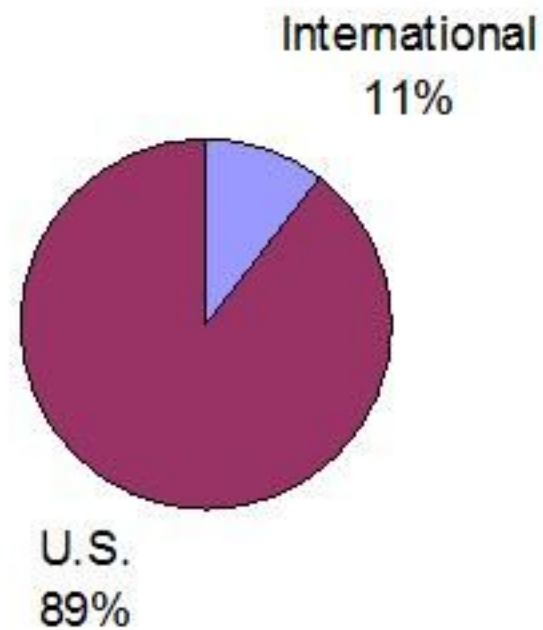


Incidents by Organization Type



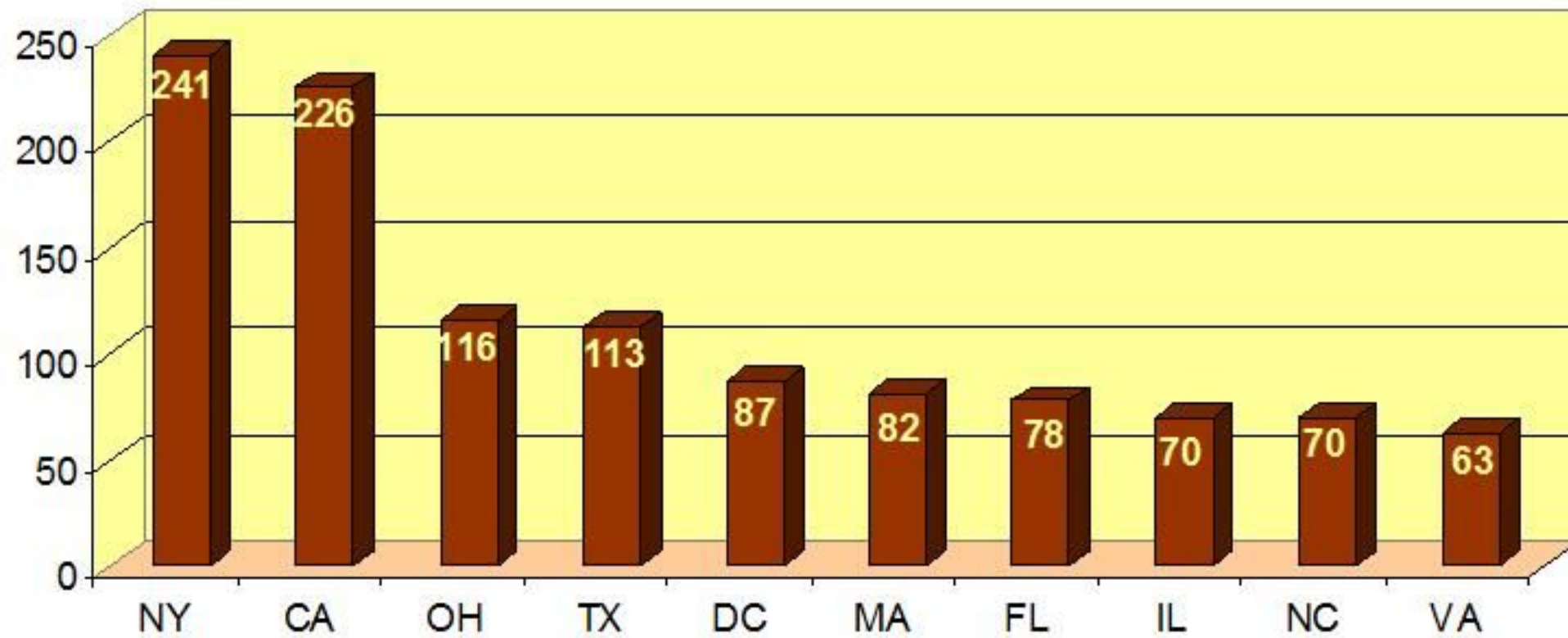
U.S. vs. International

U.S. vs. International Incidents



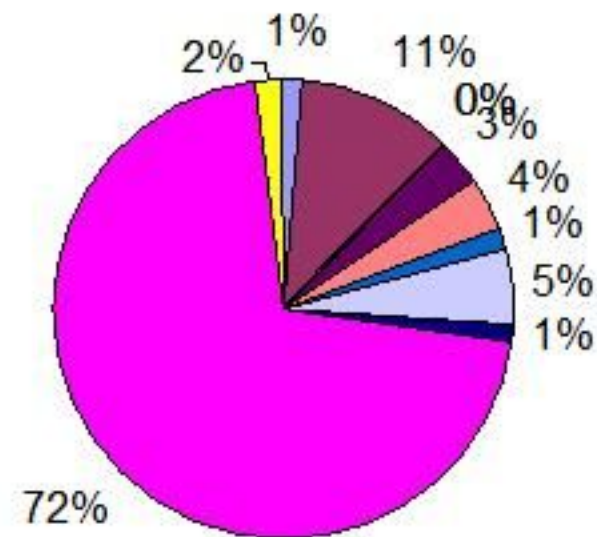
Incidents by State

Top Ten States for Incidents



Incidents by Data Type

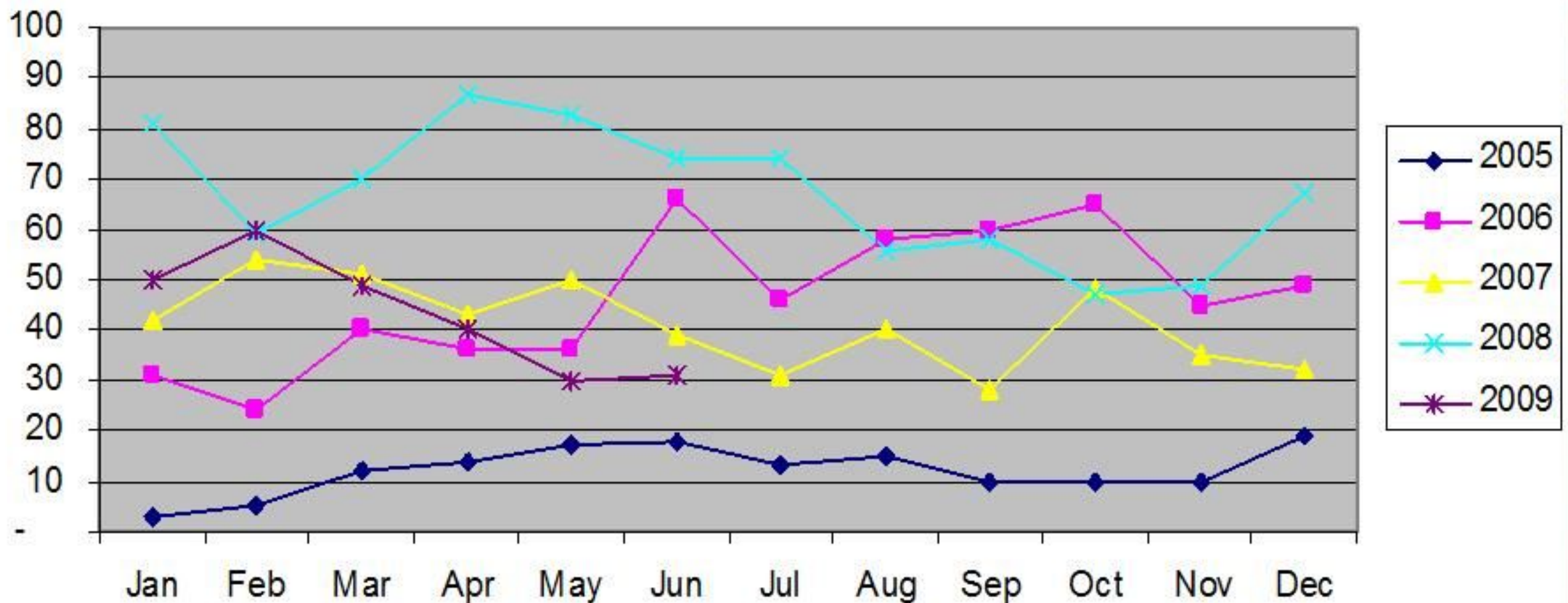
Incidents by Data Type



- ACC
- CCN
- DOB
- EMA
- FIN
- MED
- MISC
- NAA
- PPN
- SSN
- UNK

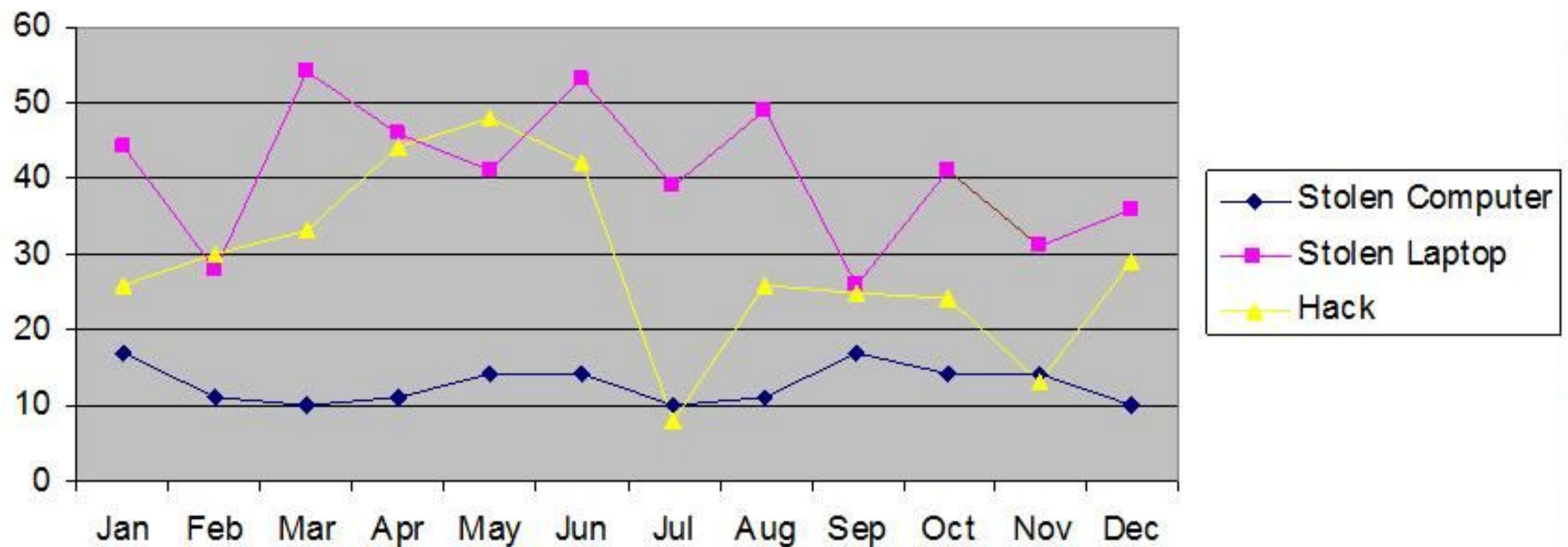
A Temporal View

Breach Incidents by Month/Year



Top Vectors by Month

Incidents by Month



Records Disclosed

Top 5 Largest Incidents

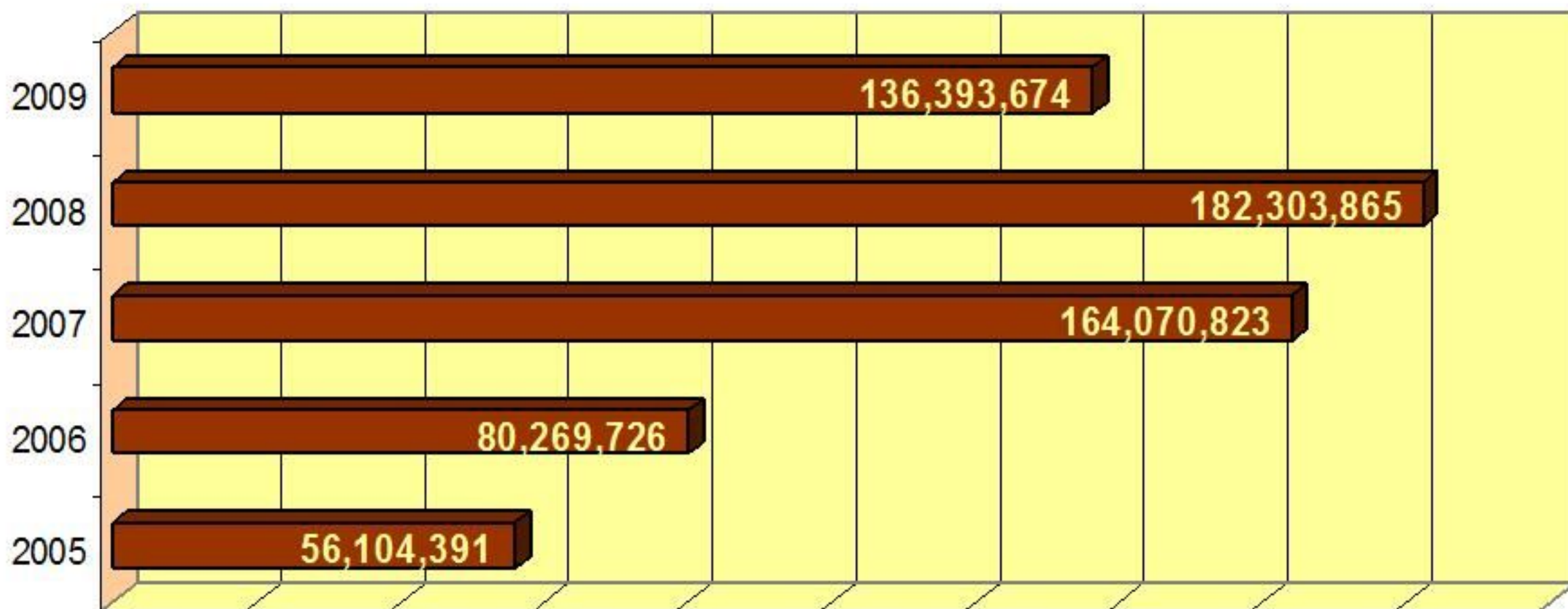
The known number of records disclosed is over 619 million.

Records	Year	Organization	Vector
130,000,000	2009	Heartland Payment Systems	Hack
94,000,000	2007	TJX Companies Inc.	Hack
90,000,000	1984	TRW, Sears Roebuck	Hack
40,000,000	2005	CardSystems	Hack
30,000,000	2004	America Online	Fraud-SE



Number of Records (January 2005 – June 2009)

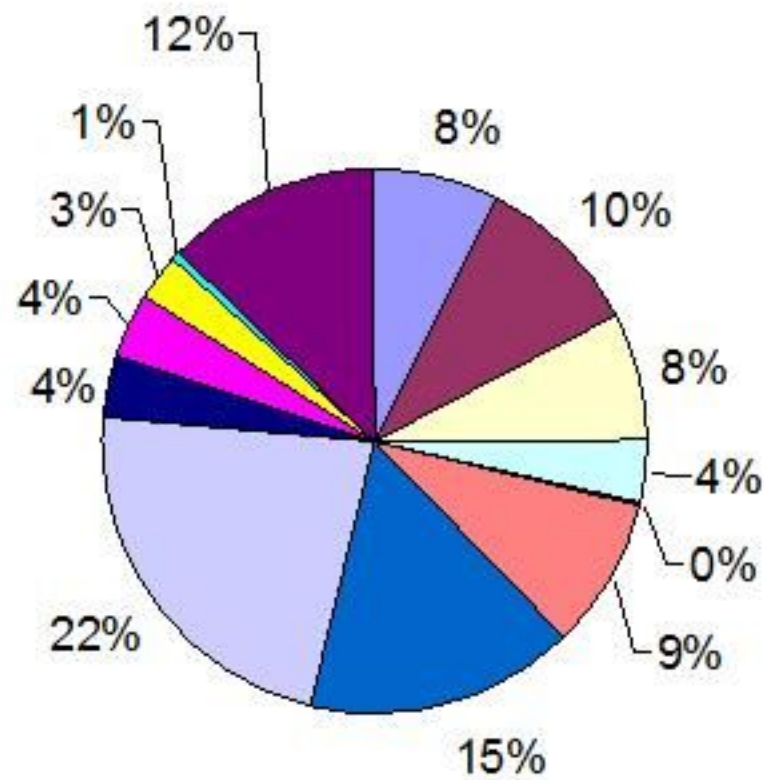
Records Disclosed Per Year



Breach Vectors

Breach Vectors

Incidents by Breach Vectors



- Computer
- Documents
- Drive/Media
- Email
- Fax
- Fraud - SE
- Hack
- Laptop
- Snail Mail
- Tape
- Unknown
- Virus
- Web

Breach Vectors: Laptop

- Incident leader at 22% of breaches (512 incidents).
- Highly under-reported vector

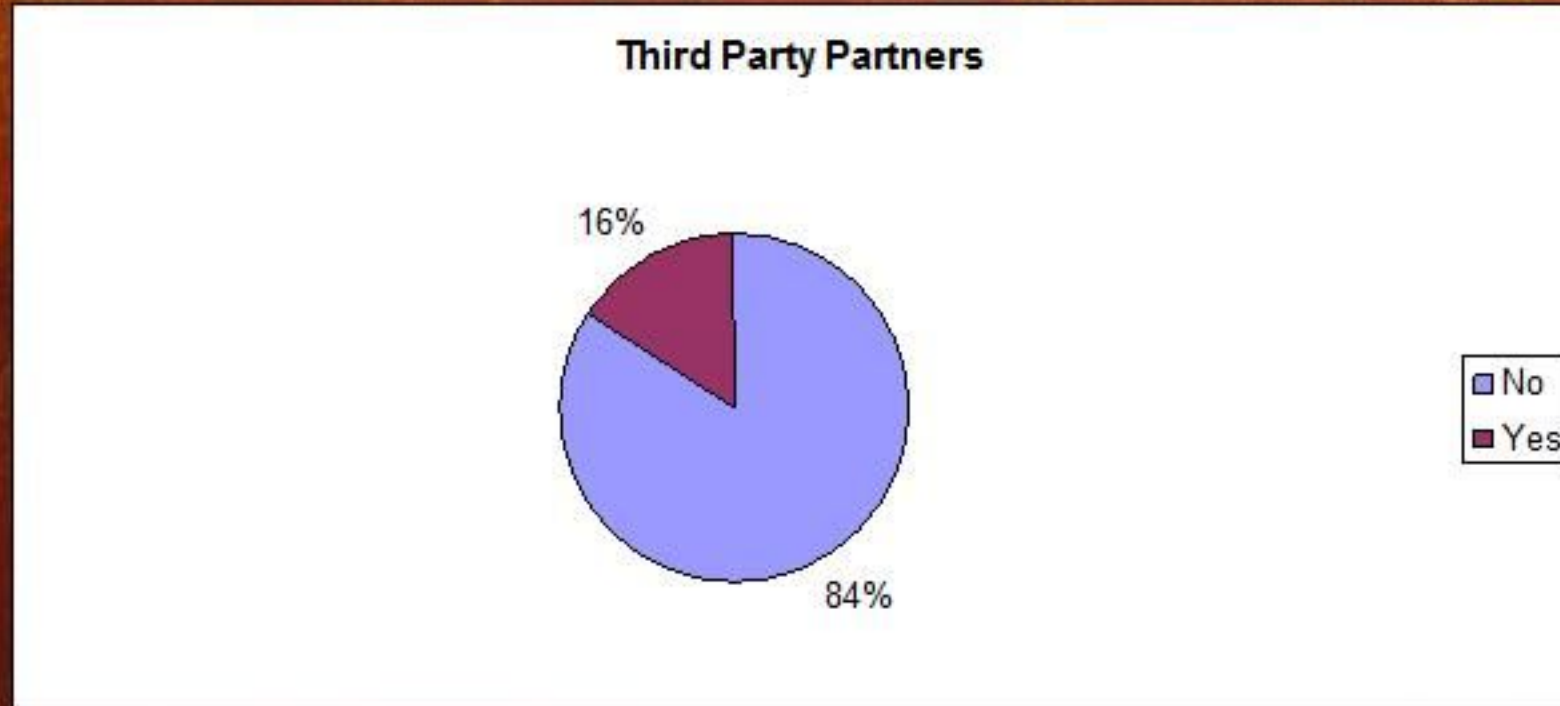


Breach Vectors: Hacking

- Record loss leader at 51% of records disclosed
- Accounts for only 15% of the incidents



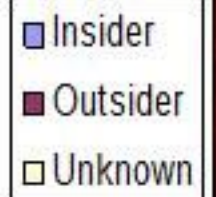
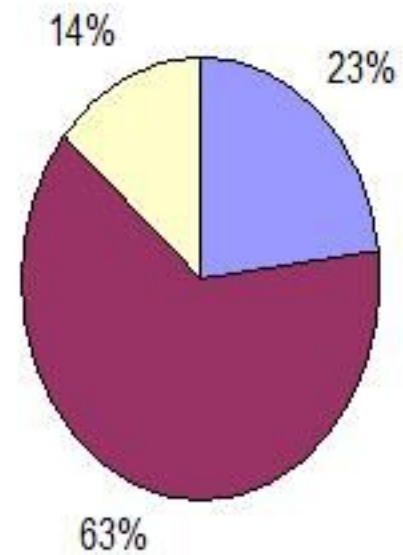
Third Party Facilitated Breaches



Insiders vs. Outsiders



Incidents by Insider/Outsider



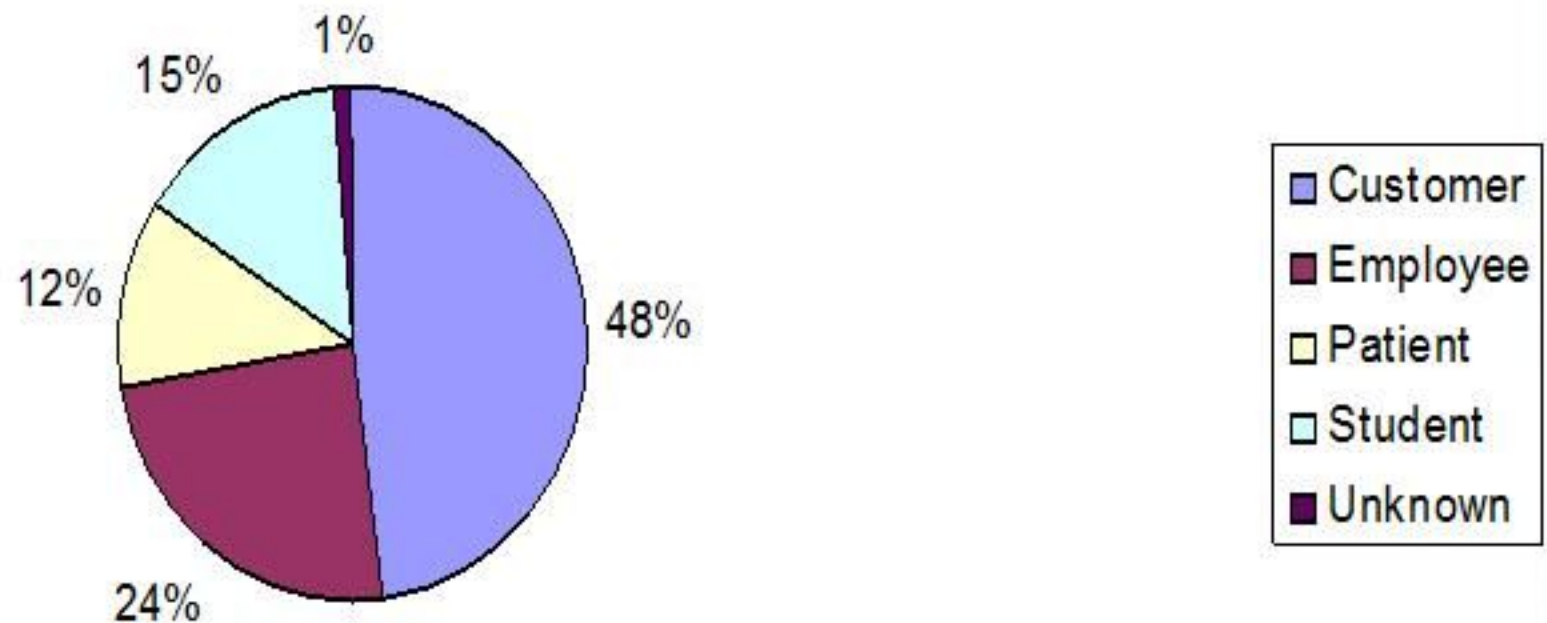
Relationships

Data Subjects and Victim Organizations

- The data subject is the person the data describes. You are the data subject in any record maintained by an organization containing data describing you.
- The relationships tracked are:
 - Customer
 - Employee
 - Patient
 - Student
 - Unknown

What Have We Found?

Incident Relationships



Credit Monitoring

Credit Monitoring Offered by Data Subject Relationship

	Relationship					Total
	Customer	Employee	Patient	Student	Unknown	
No	179	86	34	28	6	333
Unknown	637	294	217	281	17	1446
Yes	265	169	24	19	4	481
Total	1081	549	275	328	27	2260

Trends

Trends

- Victims who are reimbursed for their expenses cannot sue.
- Insider snooping reports are increasing.
- Organized crime has become increasingly involved.
- Calls to overhaul existing privacy law, and to develop a federal data breach law.

Questions?

Slide show will be made available at suzannewidup.com
under publications.