Are Large Scale Data Breaches Inevitable?

Douglas E. Salane
Center for Cybercrime Studies
John Jay College of Criminal Justice

Cyber Infrastructure Protection '09
City University of New York
City College (CCNY)
June 5, 2009

Large Scale Breaches

- What is a large scale data breach?
- Why are they important?
- Where do these breaches occur?

Information on Data Breaches

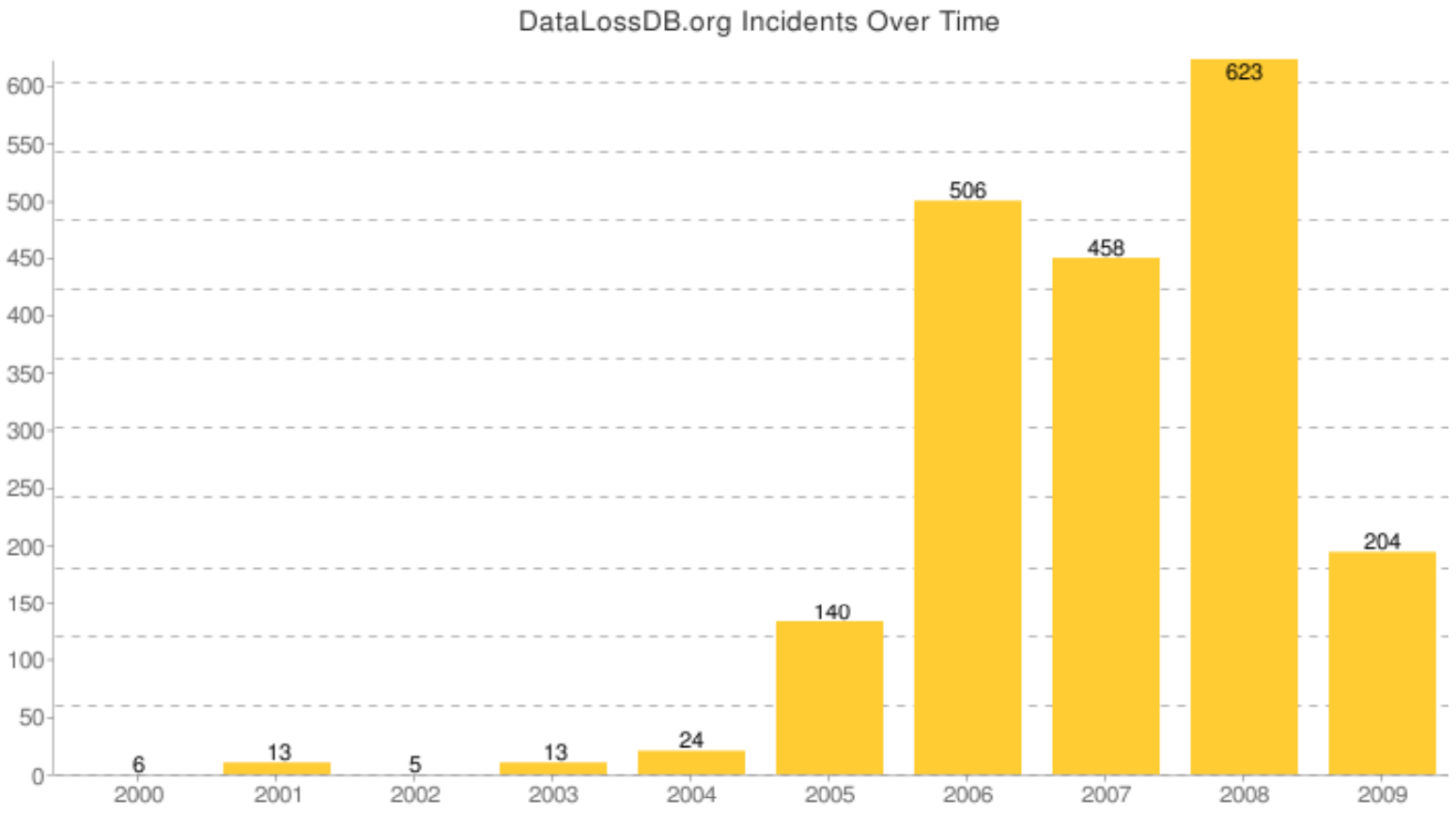
- State Breach notification Laws
- Federal Breach Notification Laws
- Role of State Attorney Generals
- Breach notification letters
- Civil and criminal prosecutions
- Company press releases and announcements
- SEC Filings

Organizations that track breaches

- Open Security Foundation: DataLoss DB project http://datalossdb.org/
- Privacy Rights Clearing House http://www.privacyrights.org/
- Federal Trade Commission http://www.ftc.gov

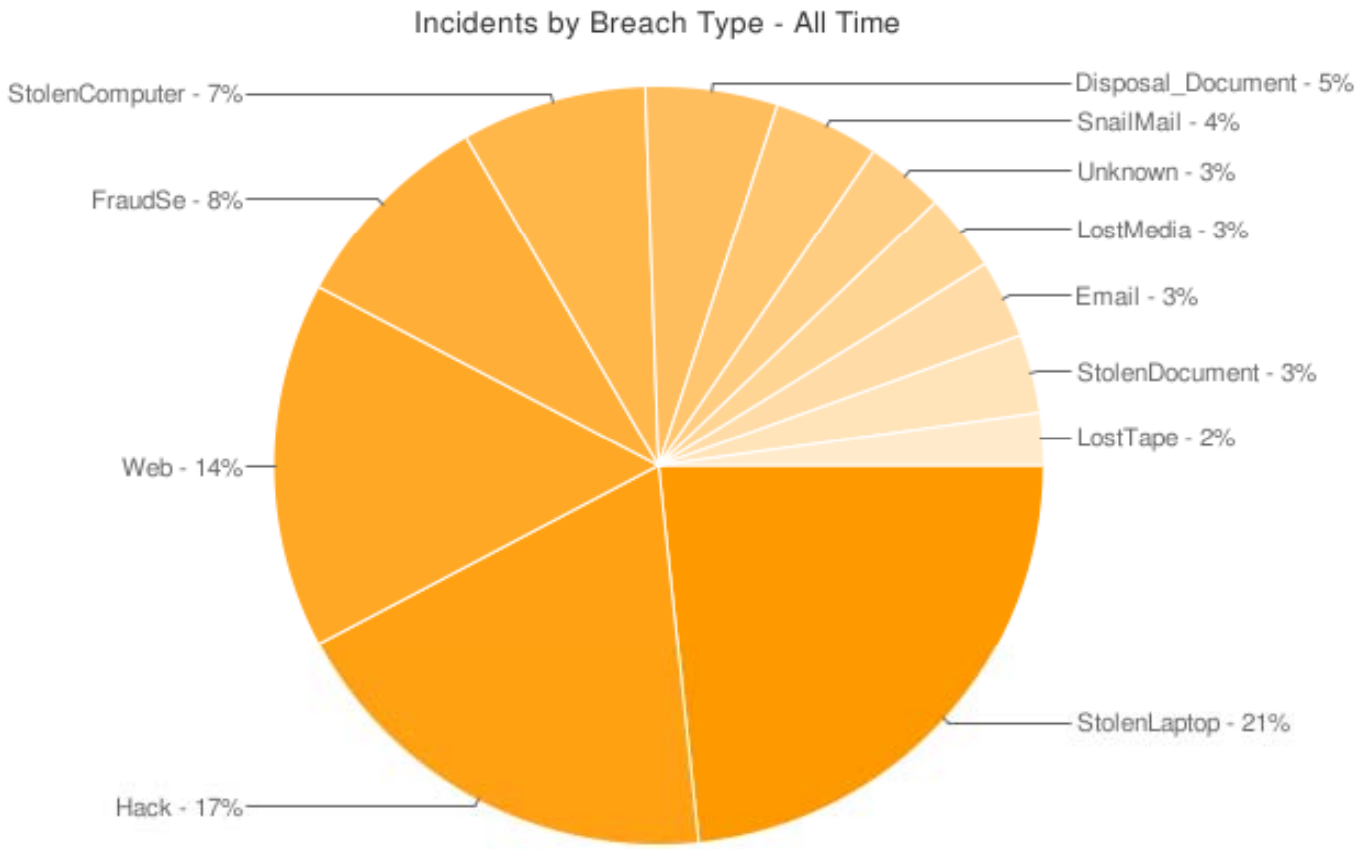
Breach Incidents 2000-2009

(source: Open Security Foundation)



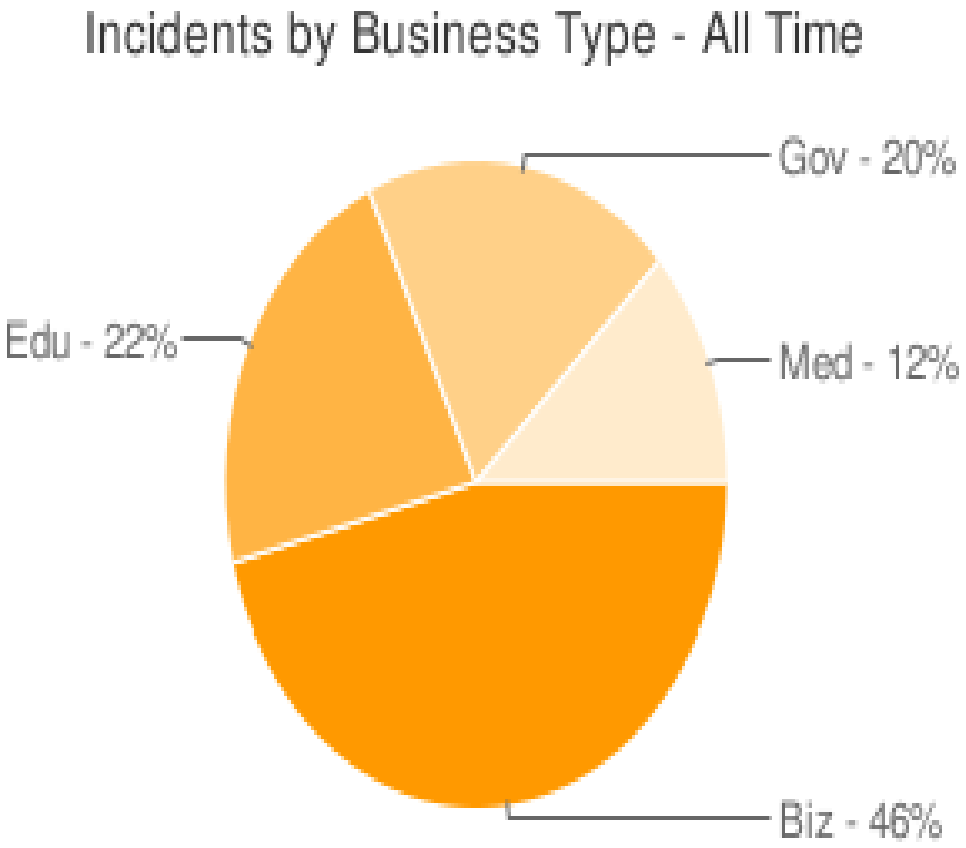
Incidents By Breach Type

(source: Open Security Foundation)

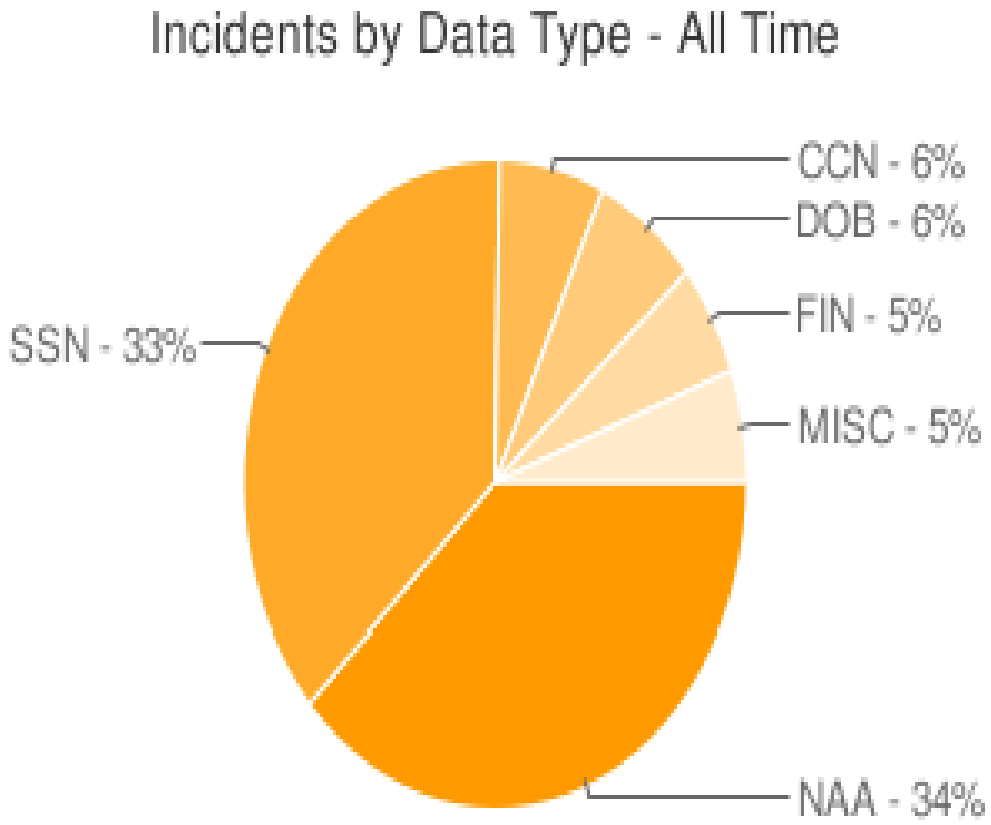


Incidents Business

(source: Open Security Foundation)



Incidents by Data Type
(source: Open Security Foundation)



Notable large scale breaches in the Data Aggregation Industry

- What is the data aggregation industry?
- Who buys information from a data aggregator?
- What types of information do these companies provide?

Breaches in the Data Aggregation: methods, costs and consequences

- Acxiom breaches 2001-2004
- Choice Point breaches 2004
- LexisNexis (Accurint) breaches 2005,2007

Breaches in the Retail and Card Payment Industry

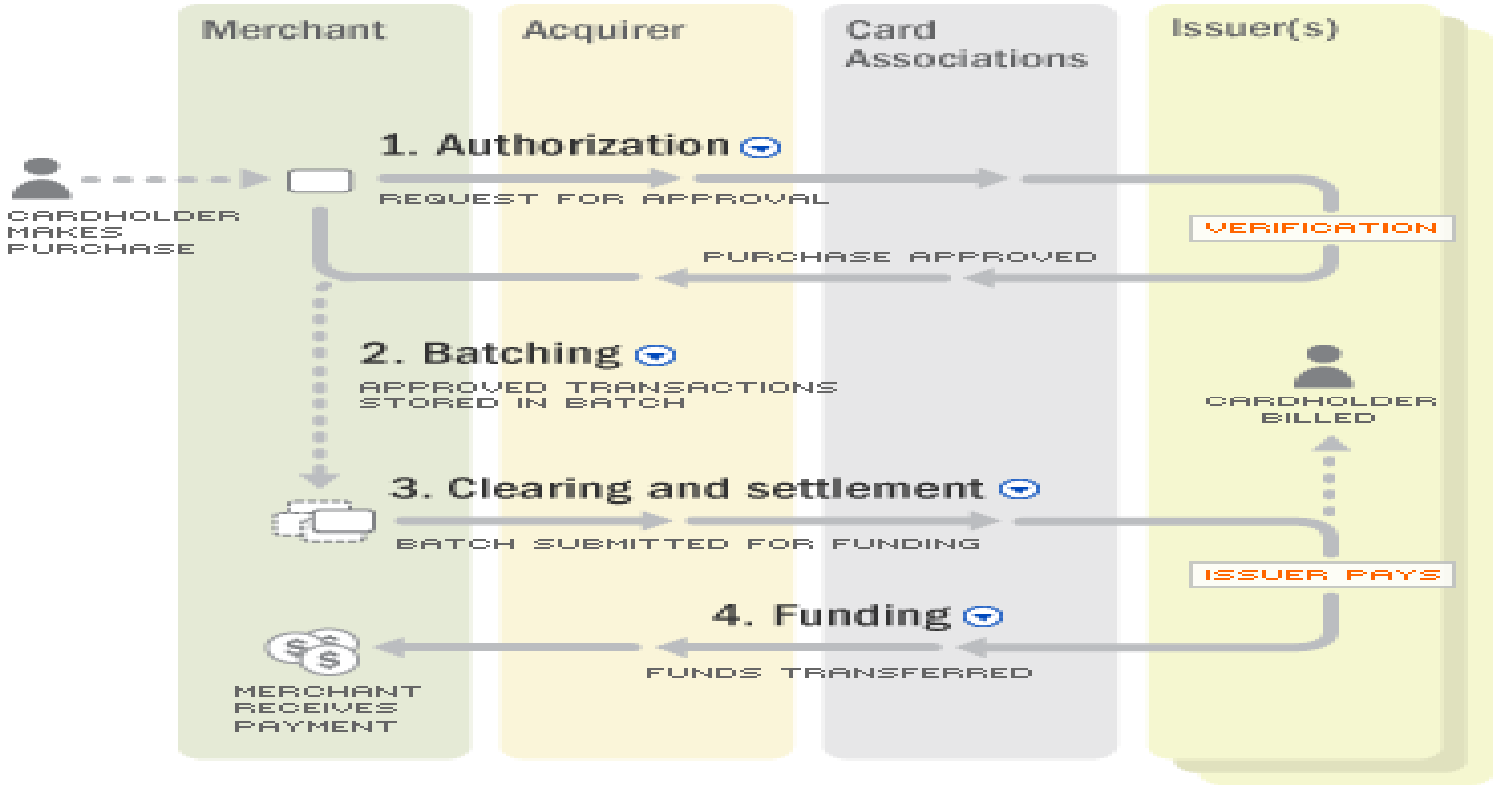
- What is the card payment processing industry?
- Why is this industry targeted and by whom?
- What do you do with 45 million credit card numbers?

Breaches in the Retail and Card Payment Processing Industries: methods, costs and consequences

- CardSystems Solutions – 45 million card numbers
- TJX Companies – 94 million cards
- RBS World Pay – 1.5 million financial records
- Heartland Payment Systems – 100 million cards

Card Payment Industry

(source: Card Processing Basics, Bank of America)



Monetizing the Crime

- Carding sites
- Cashing on a world-wide basis
- Targeted attacks, e.g., scanners and cameras

Breaches and Fraud

- Percentage of revenue lost to on-line fraud – about 1.4% for the past six years, 3.6% in 2001
- Card present fraud rate continues to decline
- ATM fraud is rising(?)
- “Identity fraud” is rising (?)
- Fraud in international card transactions is unacceptable (One in nine on-line purchases rejected)

Large scale breaches: The costs to businesses

- Breach notification costs
- Class action suites to recover costs
- Loss of confidence by business partners and clients

Remedies

- Industry wide attempts at security – PCI DSS in the payment processing industry
- Enhanced roles of the chief information security and information privacy officers
- The increasing importance of information privacy polices

Challenges

- Breach details seldom revealed, even long after the breach.
- Until recently, there were no industry wide clearing houses for breach information. (Payments processing Information Sharing Council)
- Risks of keeping breach information secret

A few IT Community Challenges

- Knowing where the data is
- Rapid system wide updating and patching
- Integration of legacy systems
- Automated fraud detection tools at each level
- Implementing end-to-end encryption
- Better systems for authorization and auditing

Law Enforcement Challenges

- Immediate notification in the event of a breach
- Improved intelligence on carding sites and cashing techniques
- Critical need for international law enforcement and governmental cooperation

Information Security Policy Challenges

- Privacy polices based on need-to-know (limit data collection and retention)
- Comingling of systems on public and private networks.
- Polices to protect large data repositories

Trends

- Breach costs will continue to grow
- National Breach Notification Legislation is coming (health care now, other sectors soon.)
- Breach notification will give FTC and HHS Dept. more authority to regulate the use of PII.

Concluding Remarks

- Breach notification laws are changing the way organizations view information security and privacy.
- Breaches of PII such as SSNs, names, addresses are especially dangerous for individuals.
- More on privacy and data breaches at the Center for Cybercrime Studies