The Leaking Vault

Five Years of Data Breaches

Suzanne Widup

Published by:
The Digital Forensics Association

Overview

Laws

Findings

Recommendations

Laws

Then and Now

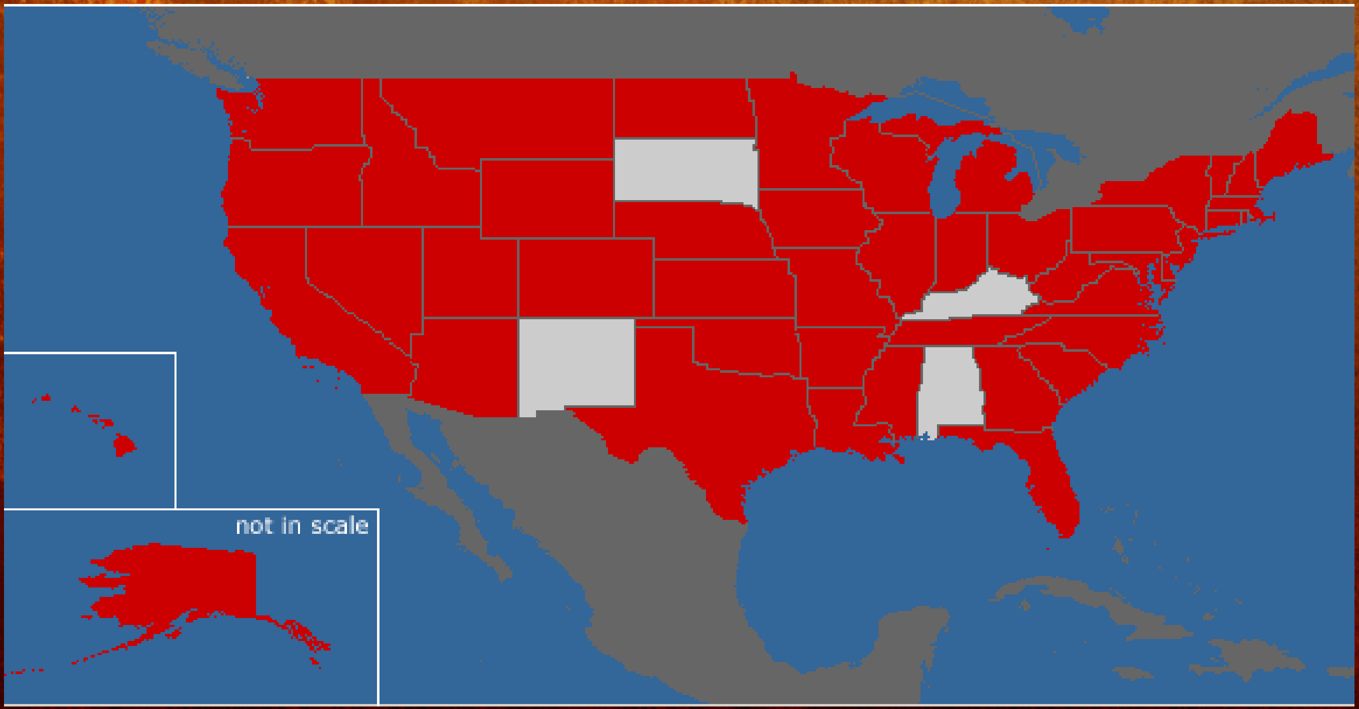
- 2003 California SB1386 took effect.
- 2007 California AB1298 added medical data to covered information.
- Massachusetts[1] and Nevada[2] laws call out encryption, destruction of records and PCI-DSS.
- No single Federal law, although one may be in the works.

[1] Mass. Gen. Laws § 93H-1 et seq.

[2] Nev. Rev. Stat. 603A.010 et seq.

States with Breach Laws

46 states, plus the District of Columbia, Puerto Rico and the Virgin Islands 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?

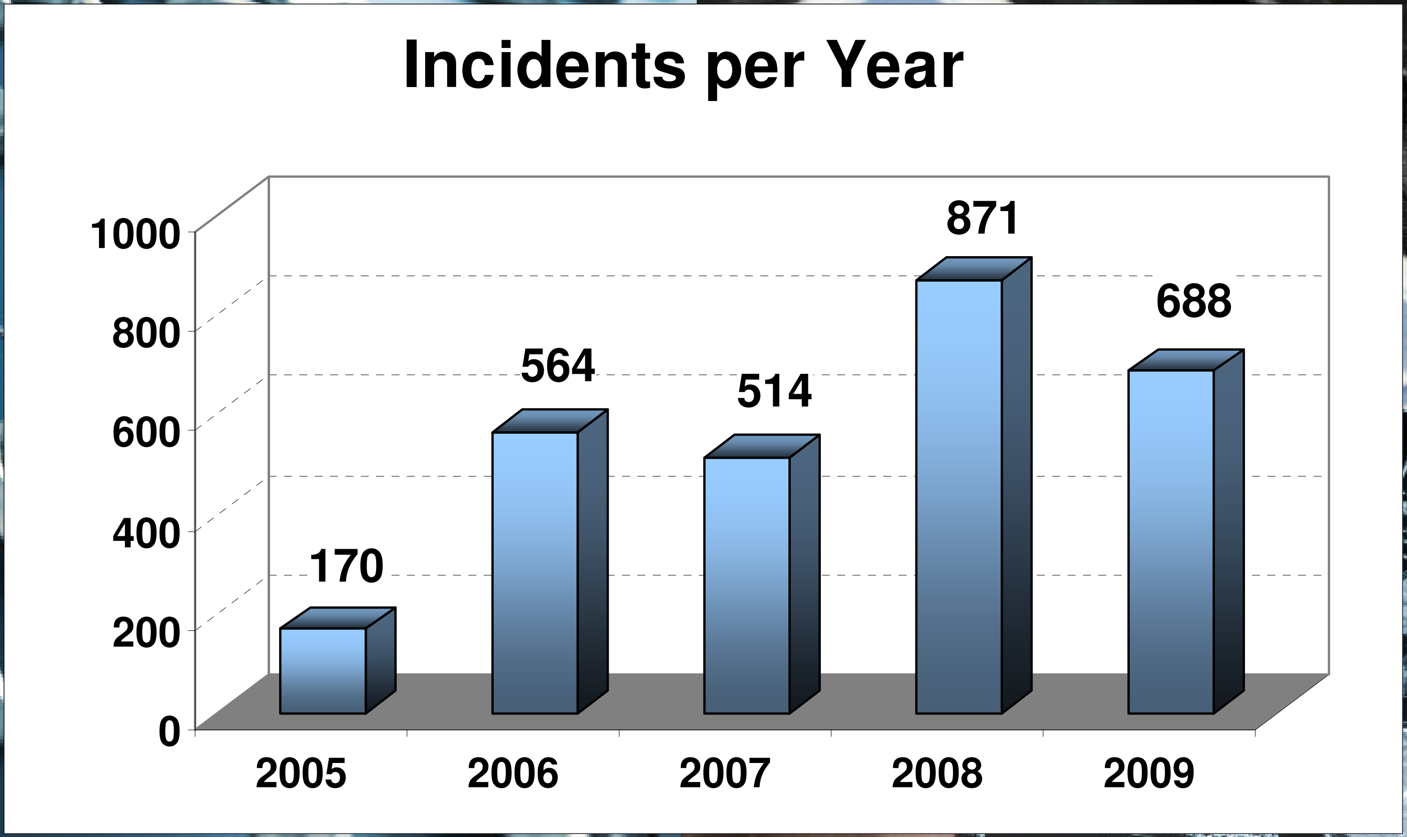
Data Sources

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

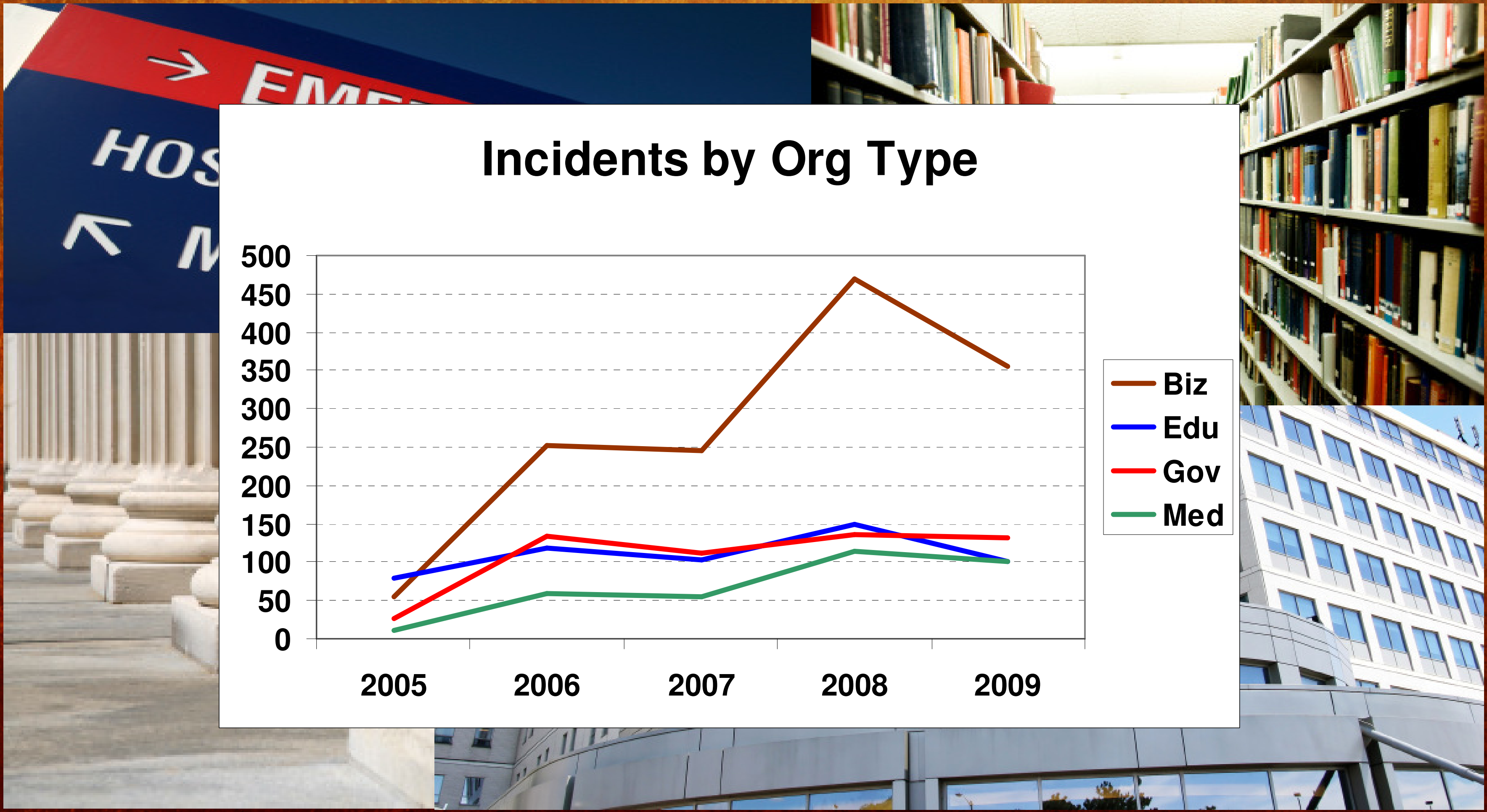
Findings

Data Breach Incidents

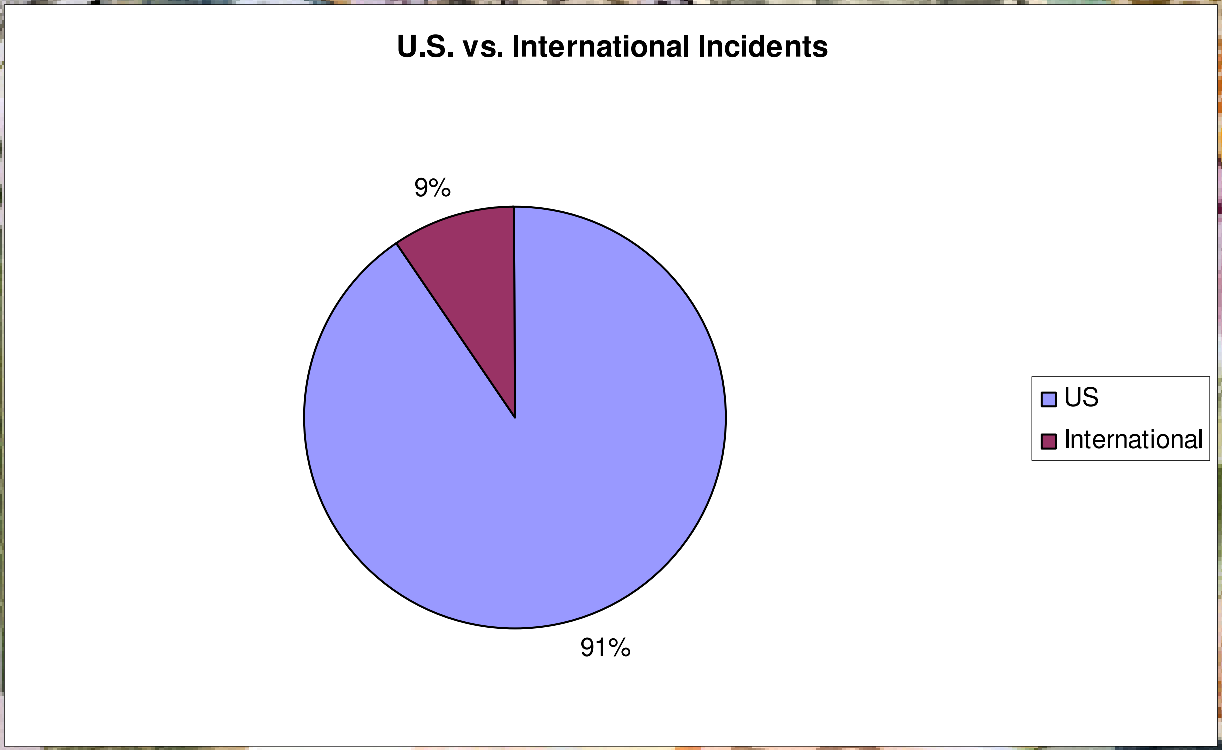
Number of Incidents



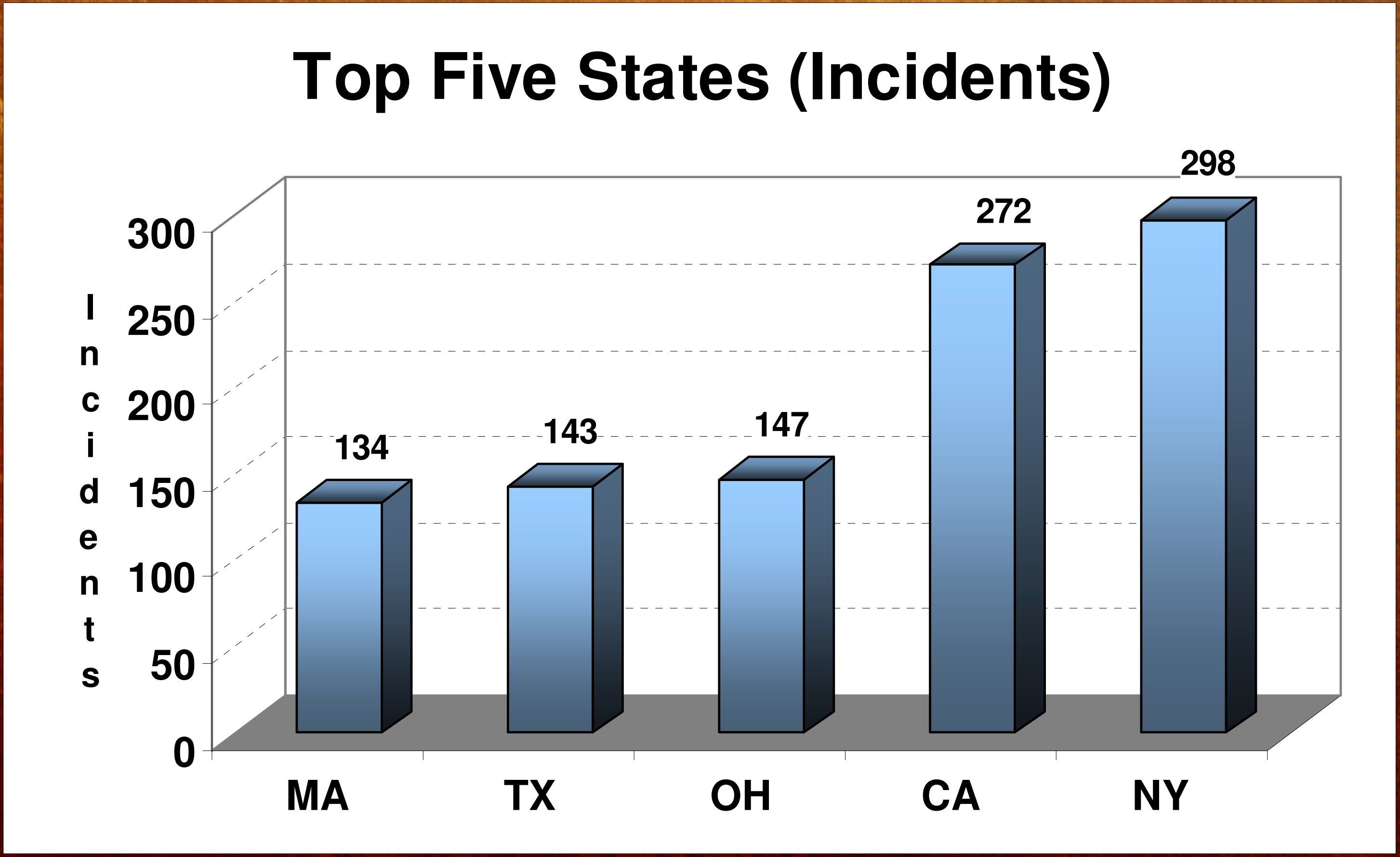
Incidents by Organization Type



U.S. vs. International

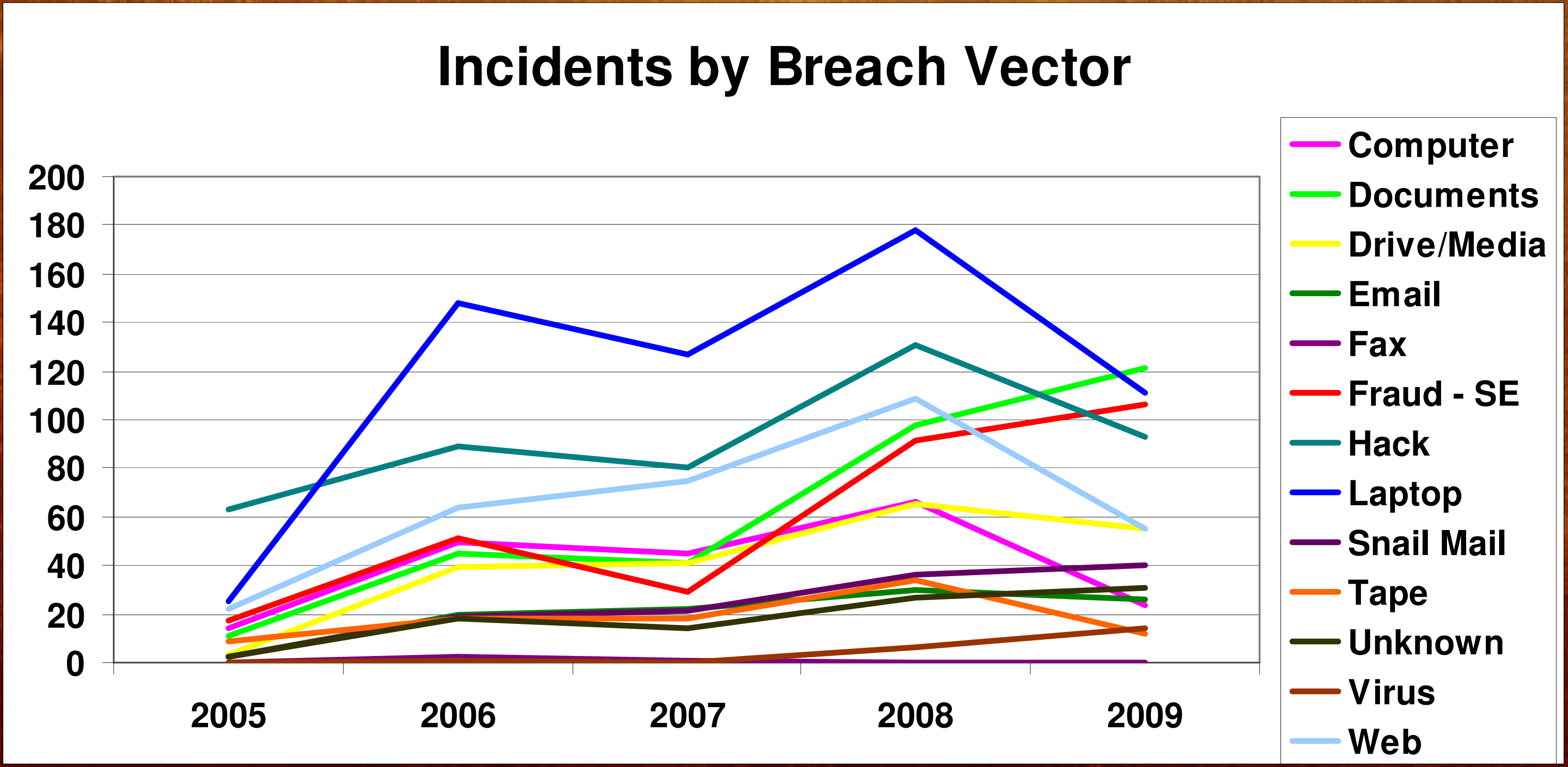


Incidents by State



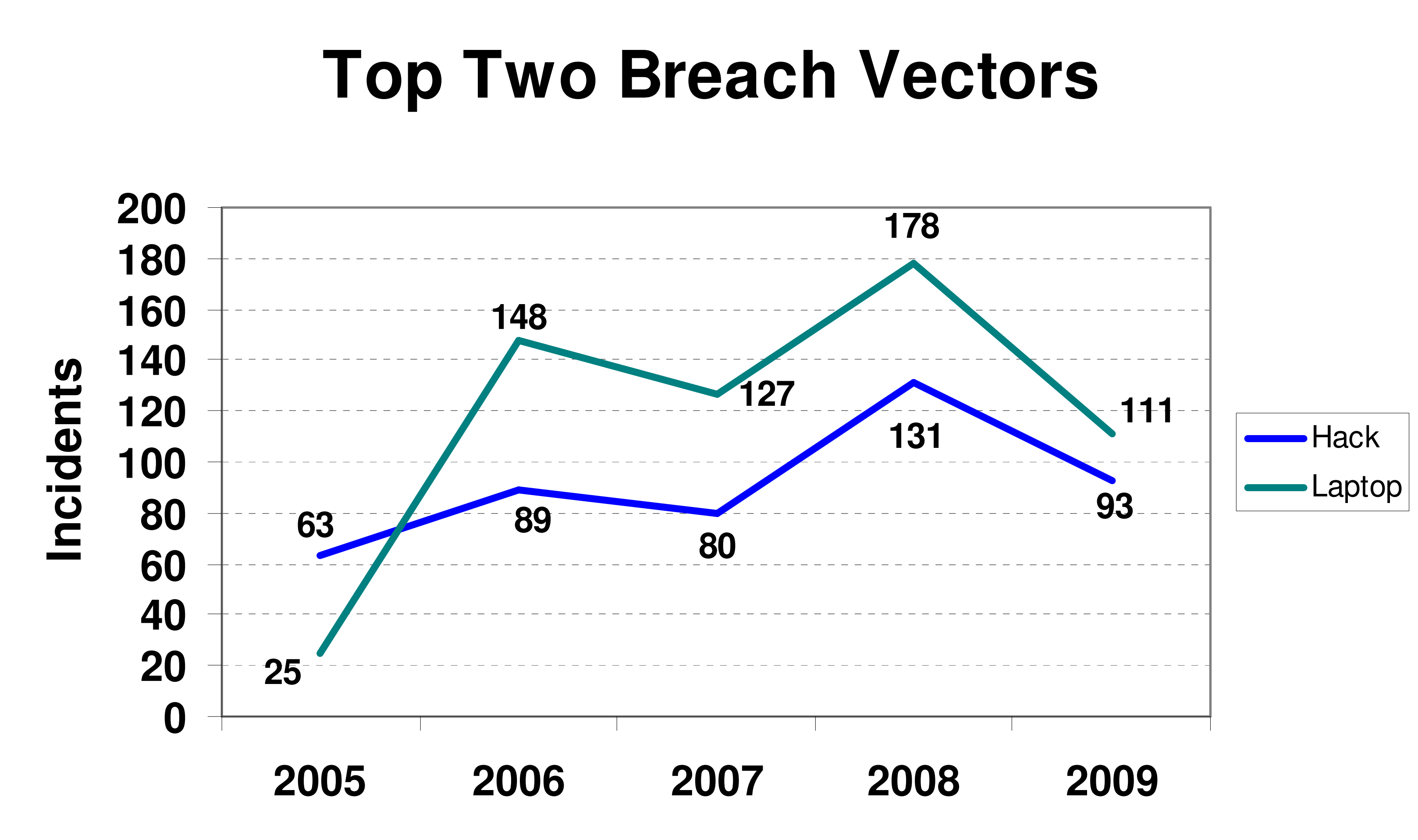
© Suzanne Widup 2010

Breach Vectors

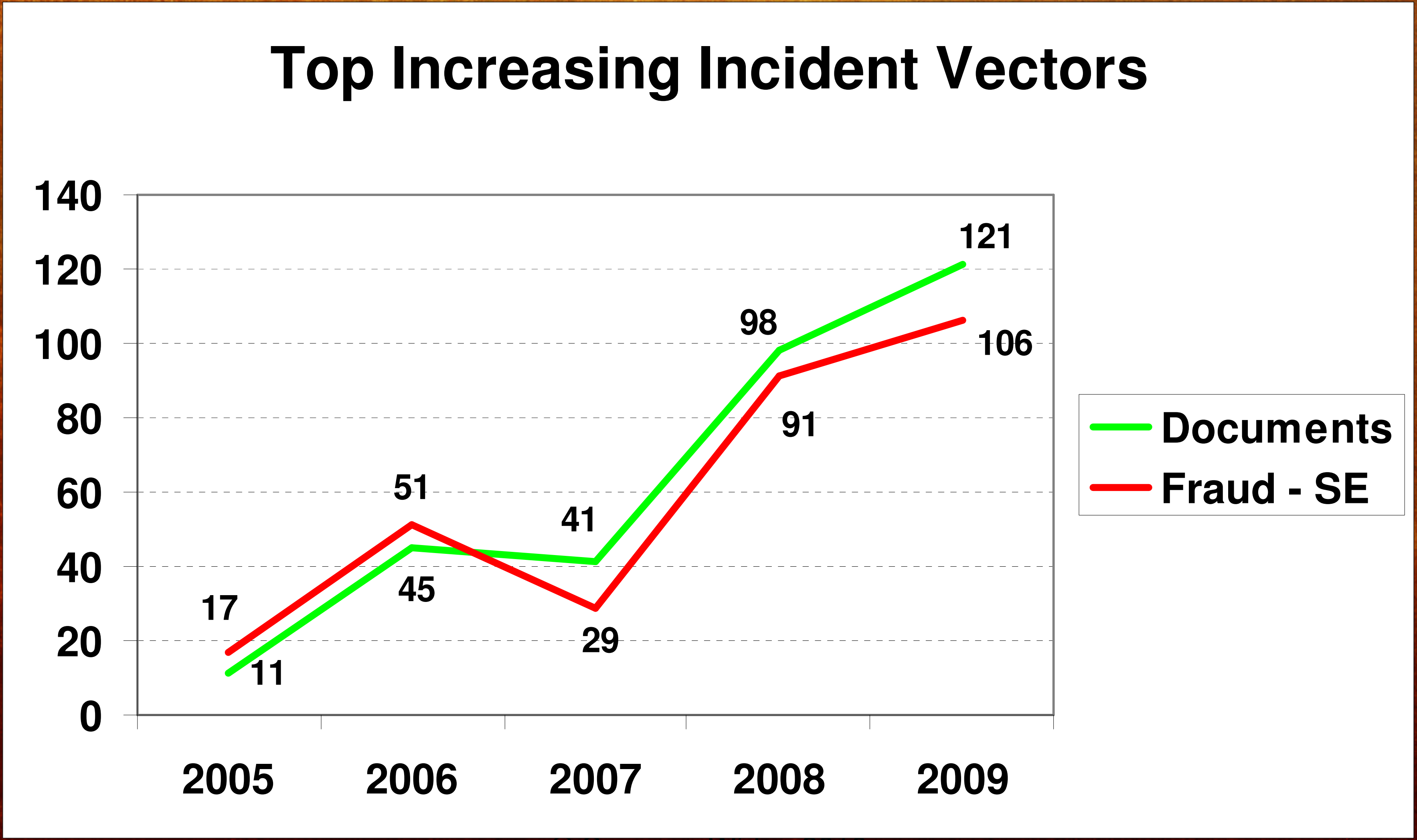


© Suzanne Widup 2010

Top Two Breach Vectors

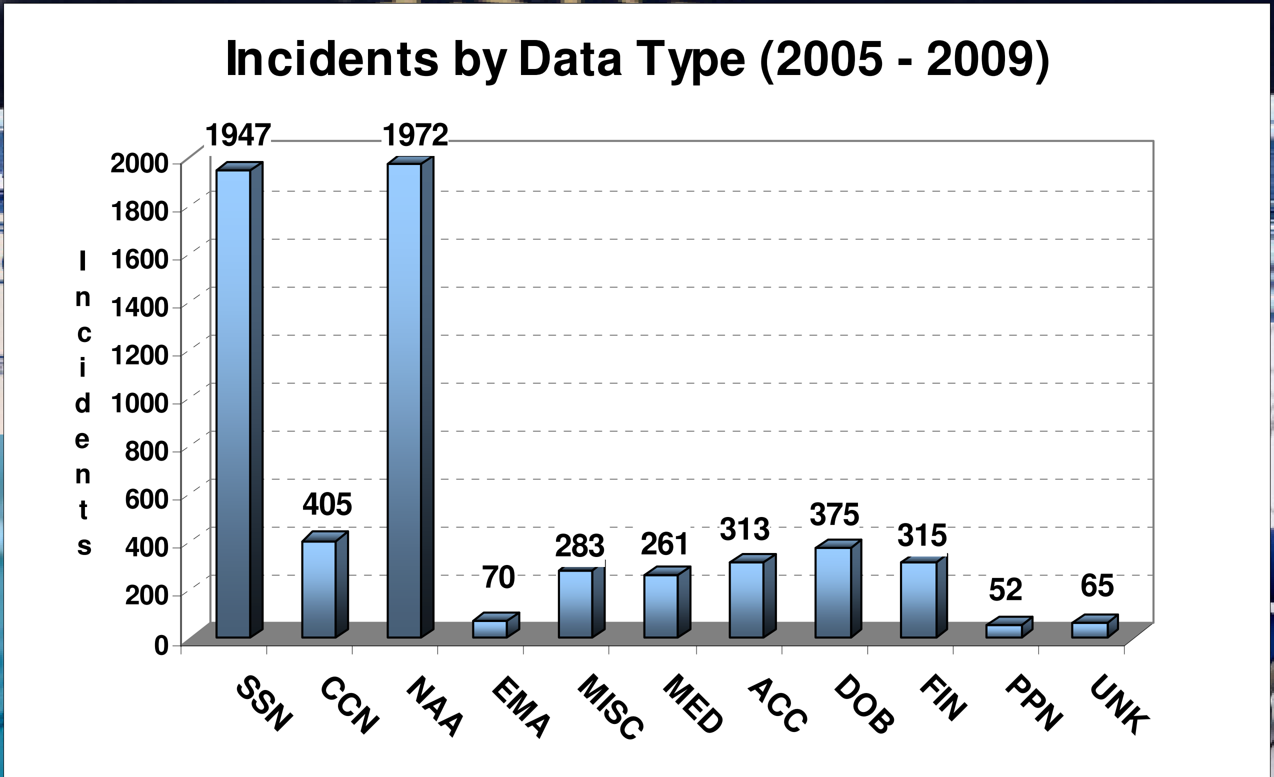


Top Increasing Incident Vectors



© Suzanne Widup 2010

Incidents by Data Type

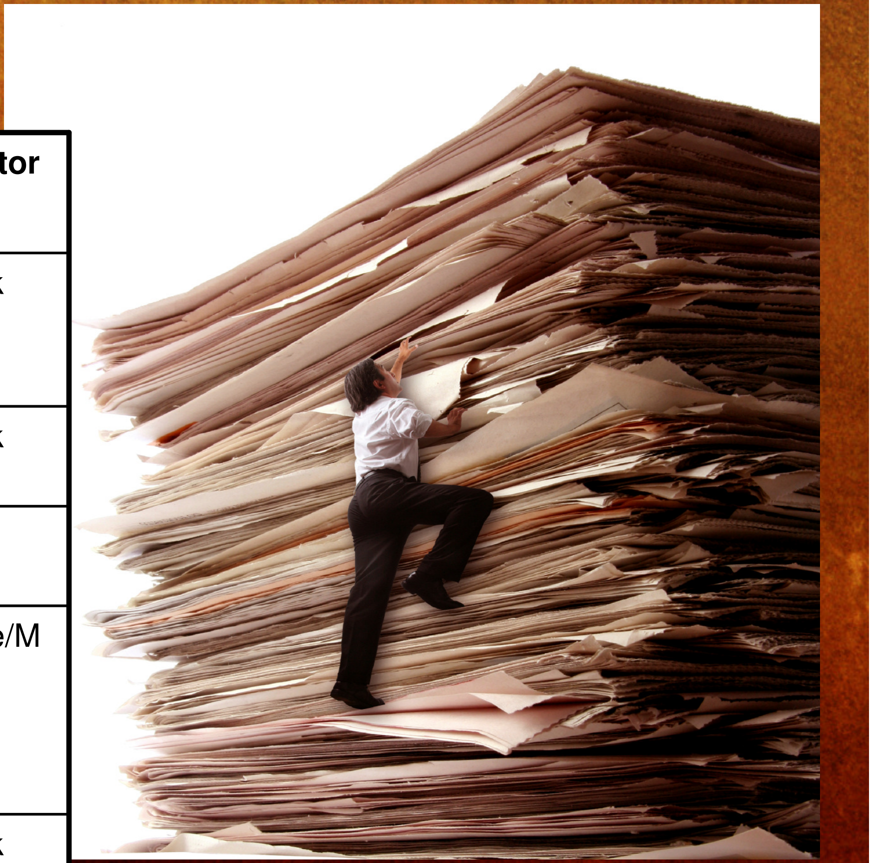


Records Disclosed

Top 5 Largest Incidents

These top 5 incidents account for 59% of records lost.

Records	Year	Organization	Vector
130,000,000	2009	Heartland Payment Systems	Hack
94,000,000	2007	TJX Companies Inc.	Hack
80,000,000	2008	Facebook	Web
76,000,000	2009	National Archives and Records Administration	Drive/Media
40,000,000	2005	CardSystems	Hack

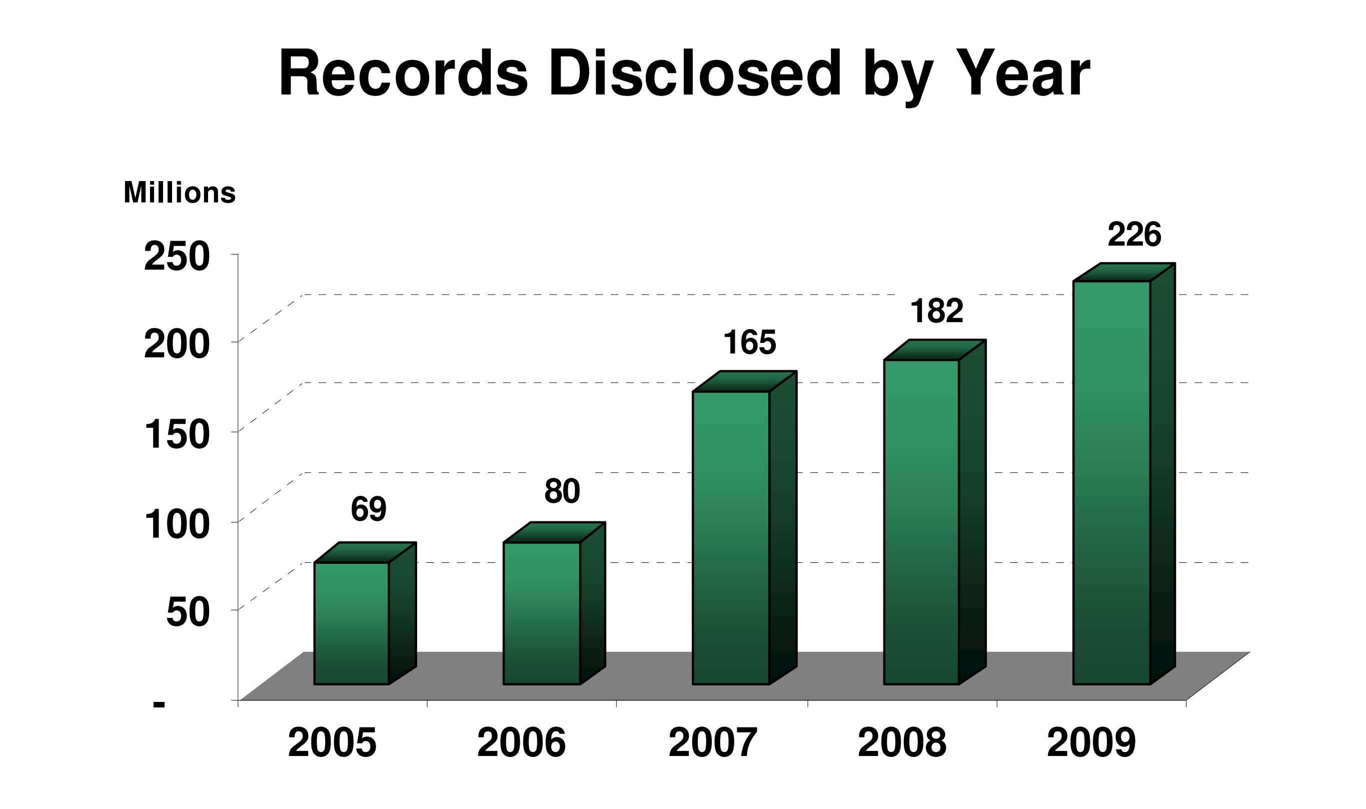


Records Disclosed Per Day

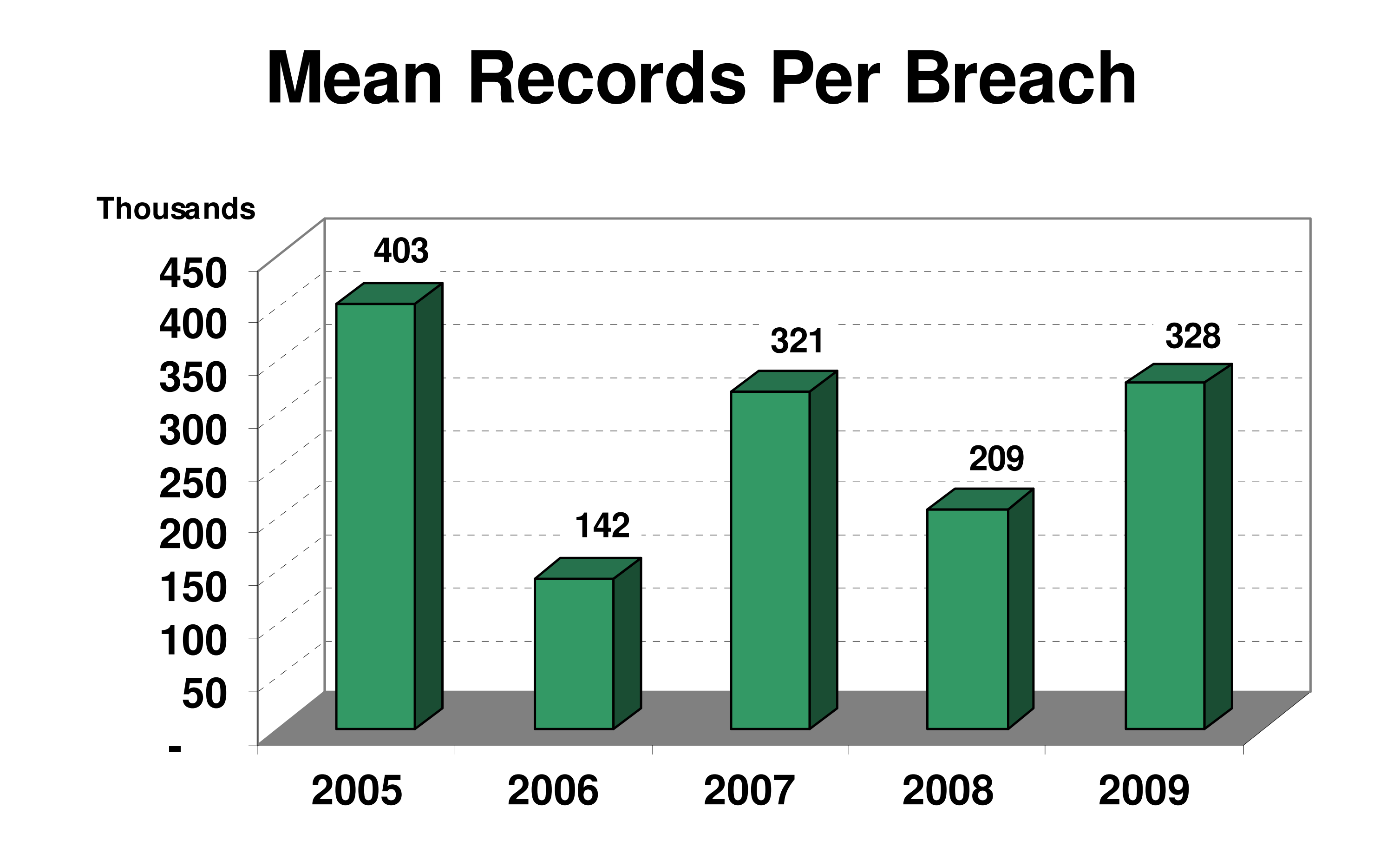
388,342 records every day for the last 5 years

Number of Records Disclosed

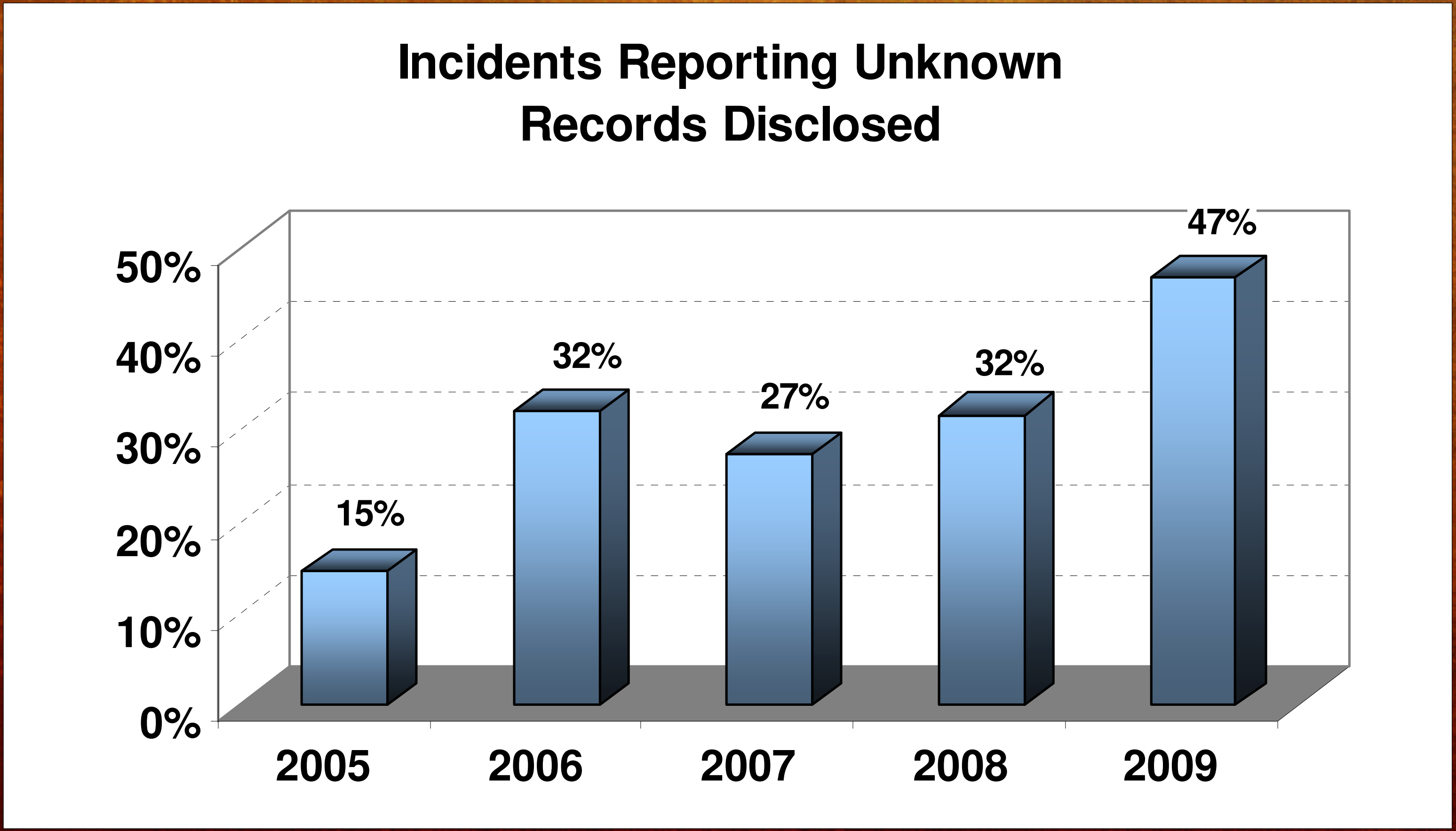
The known number of records disclosed is over **721 million**.



Mean Records/Breach

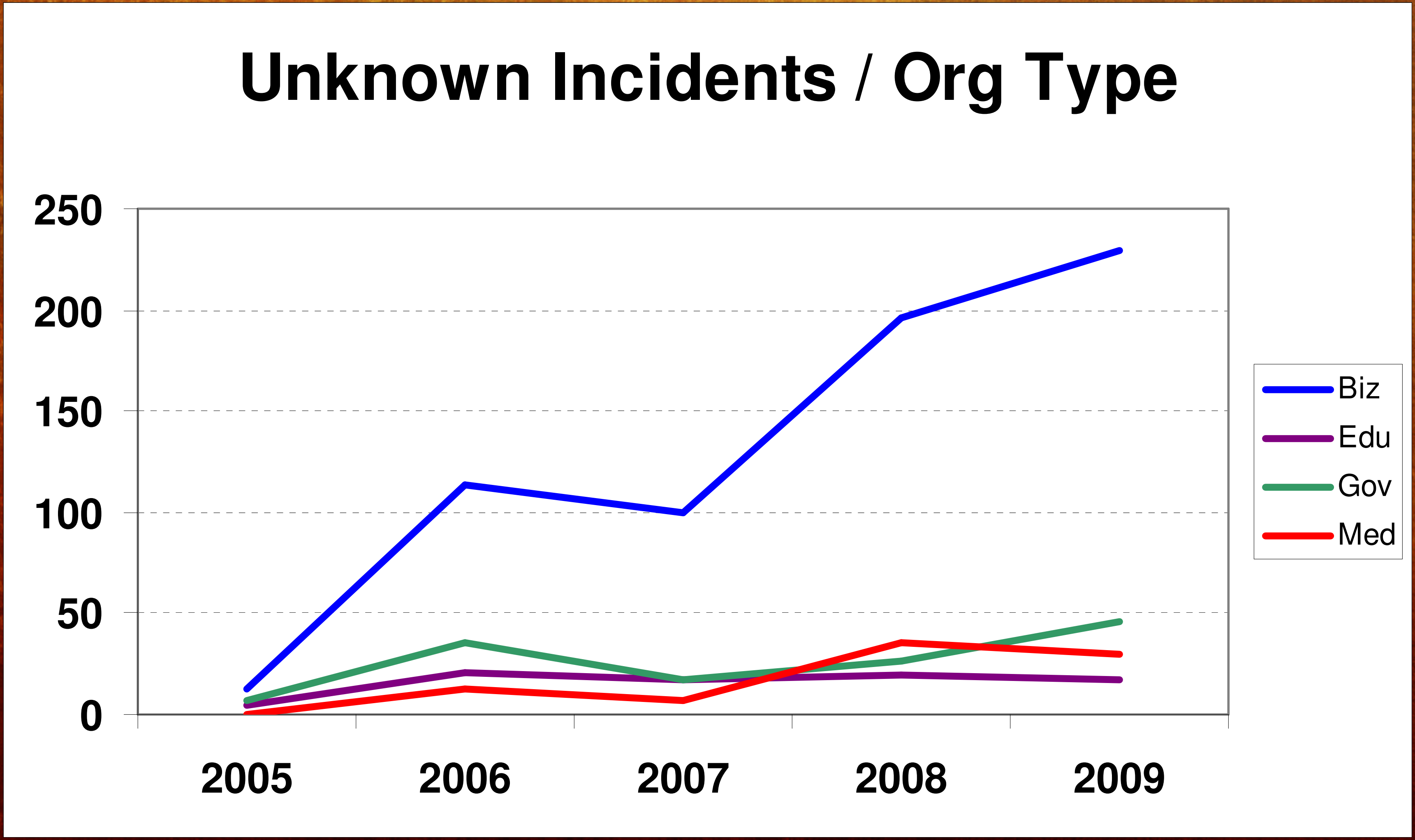


“Unknown” Records



© Suzanne Widup 2010

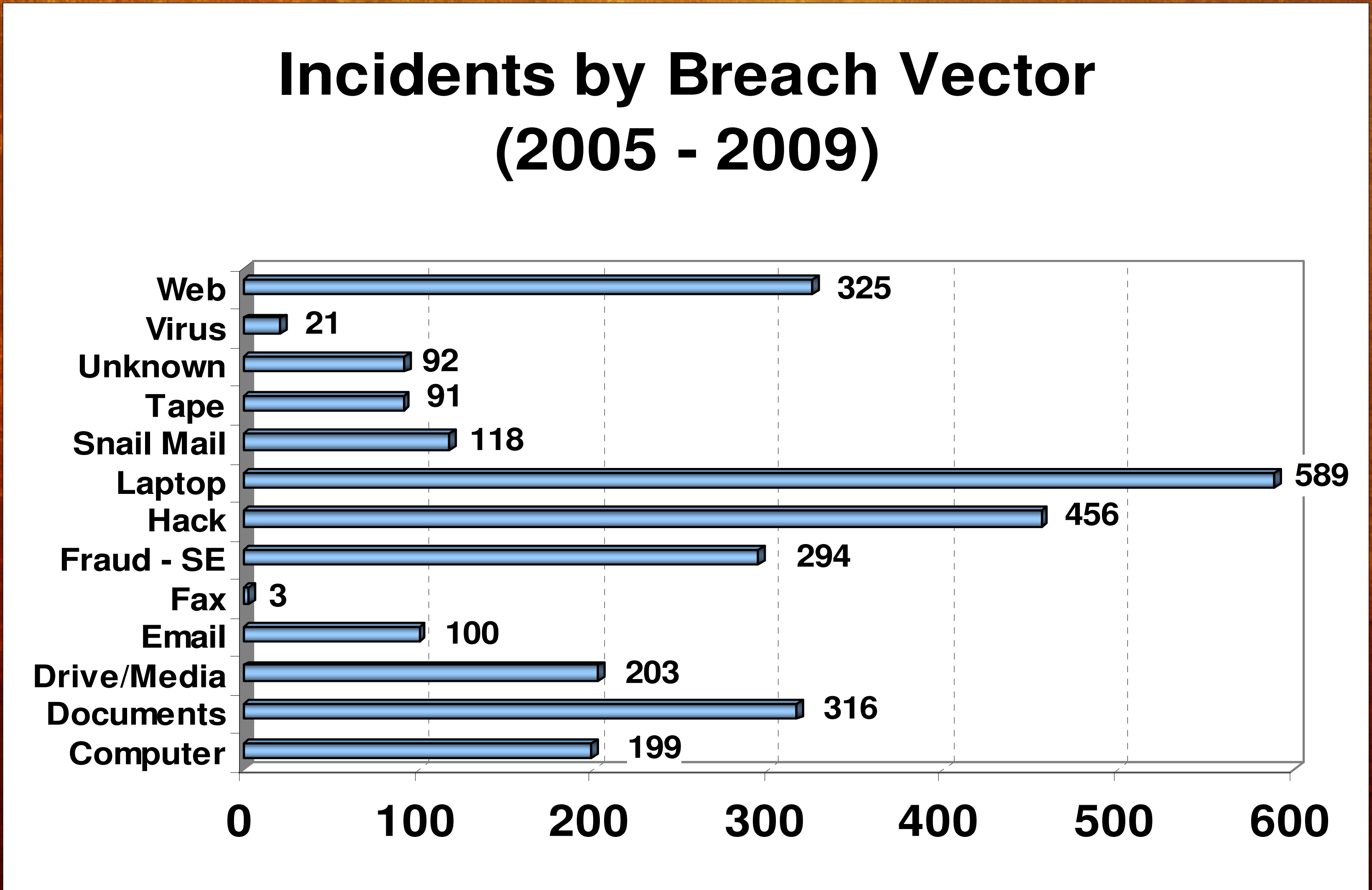
By Organizational Type



© Suzanne Widup 2010

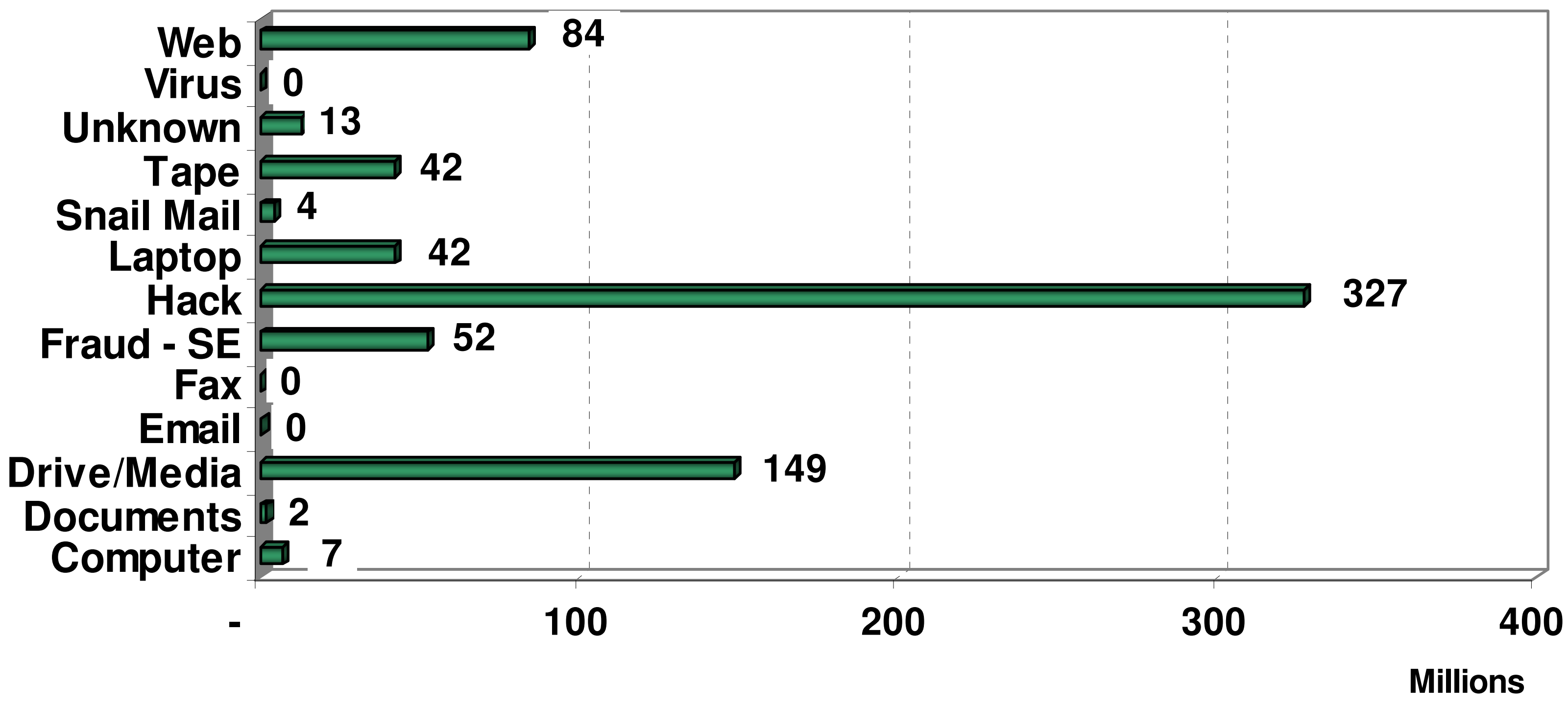
Breach Vectors

Incident Vectors



Record Vectors

Records by Breach Vector (2005 - 2009)



Breach Vectors: Laptop

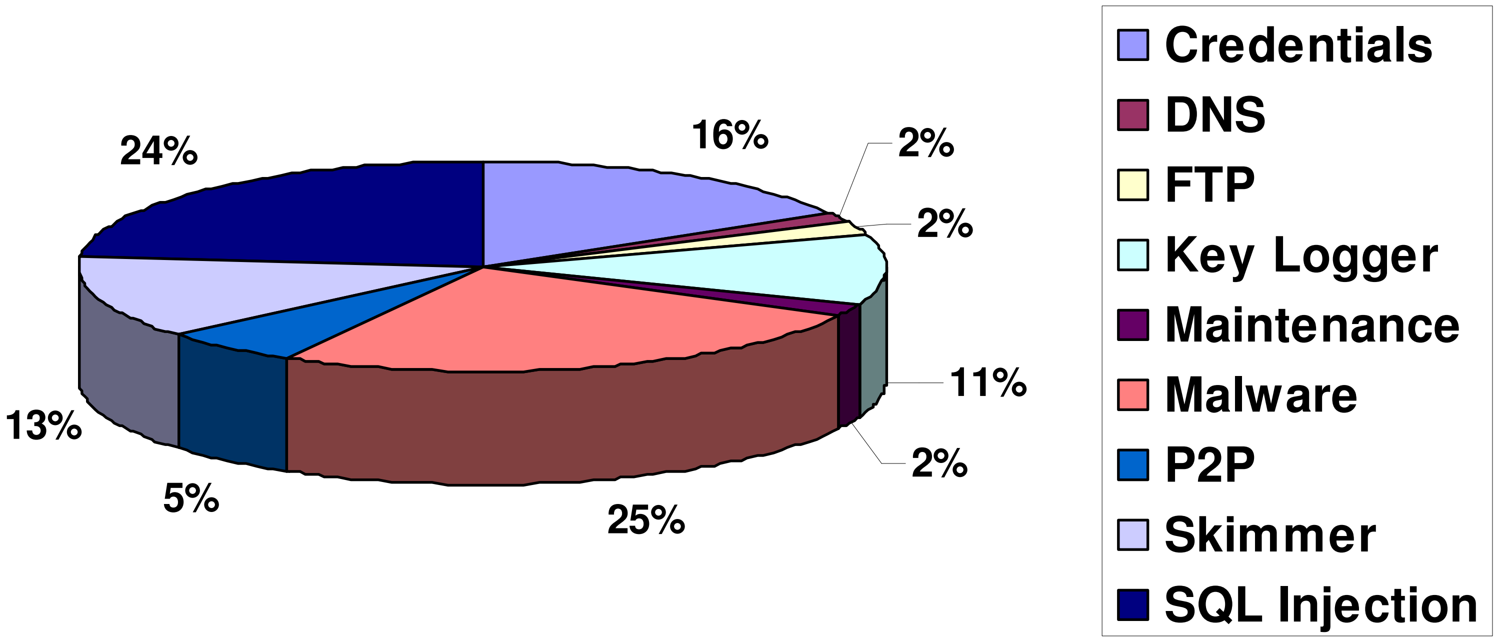
- Incident leader at 21% of breaches (589 incidents).
- Highly under-reported vector

Breach Vectors: Hacking

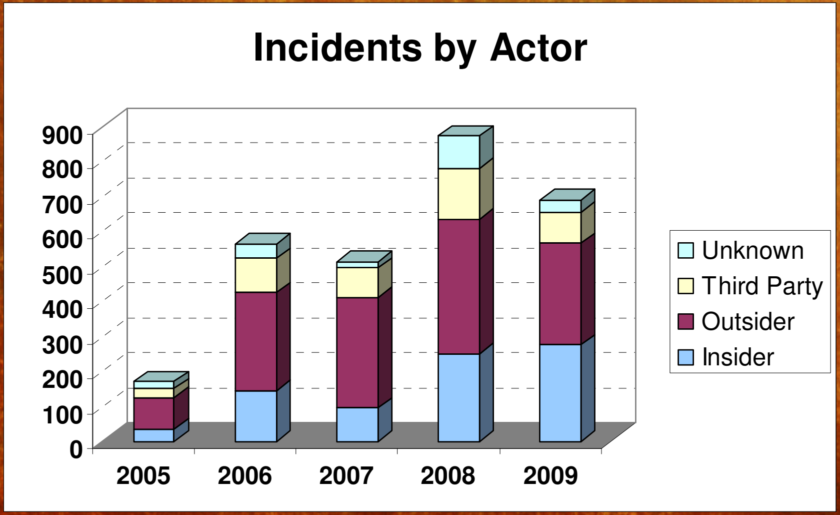
- Record loss leader at 45% of records disclosed
- Accounts for only 16% of the incidents

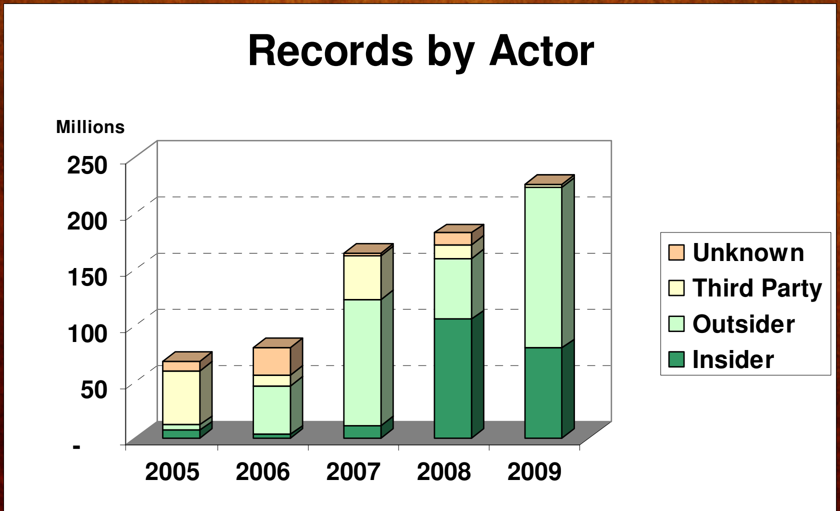
Hacking Methods

Hacking Methods - Incidents (2005 - 2009)

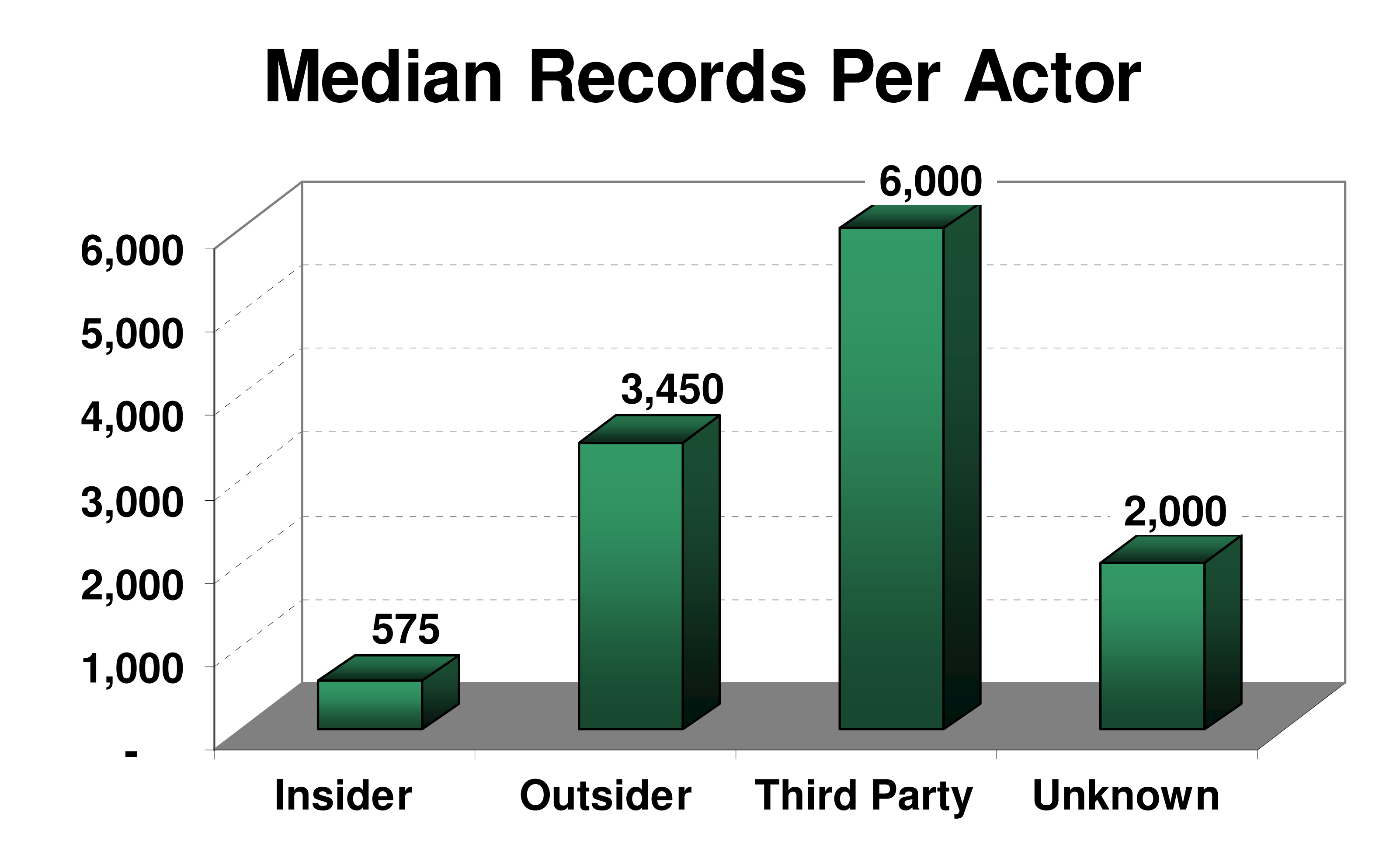


Insider/Outsider/Third Party





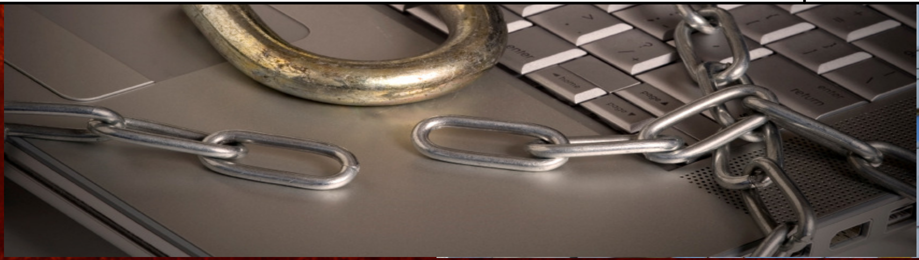
Insider/Outsider/Third Party

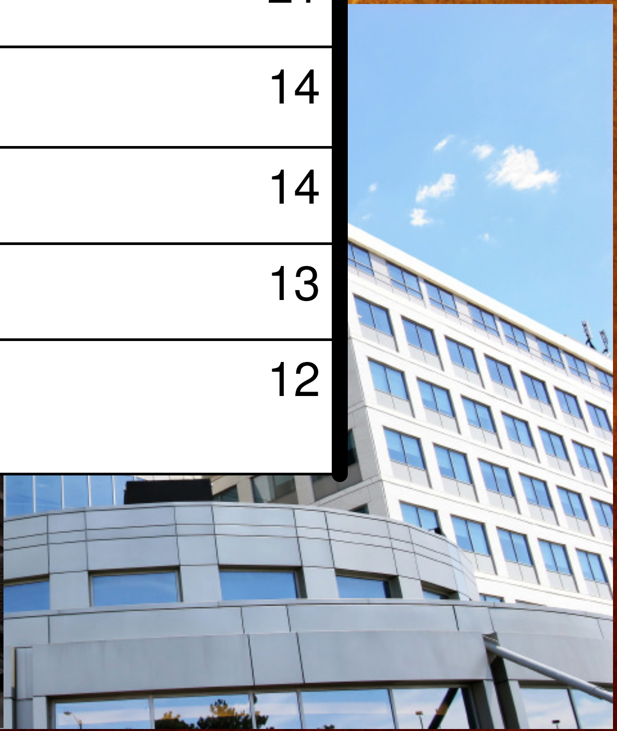


Organizational Sectors

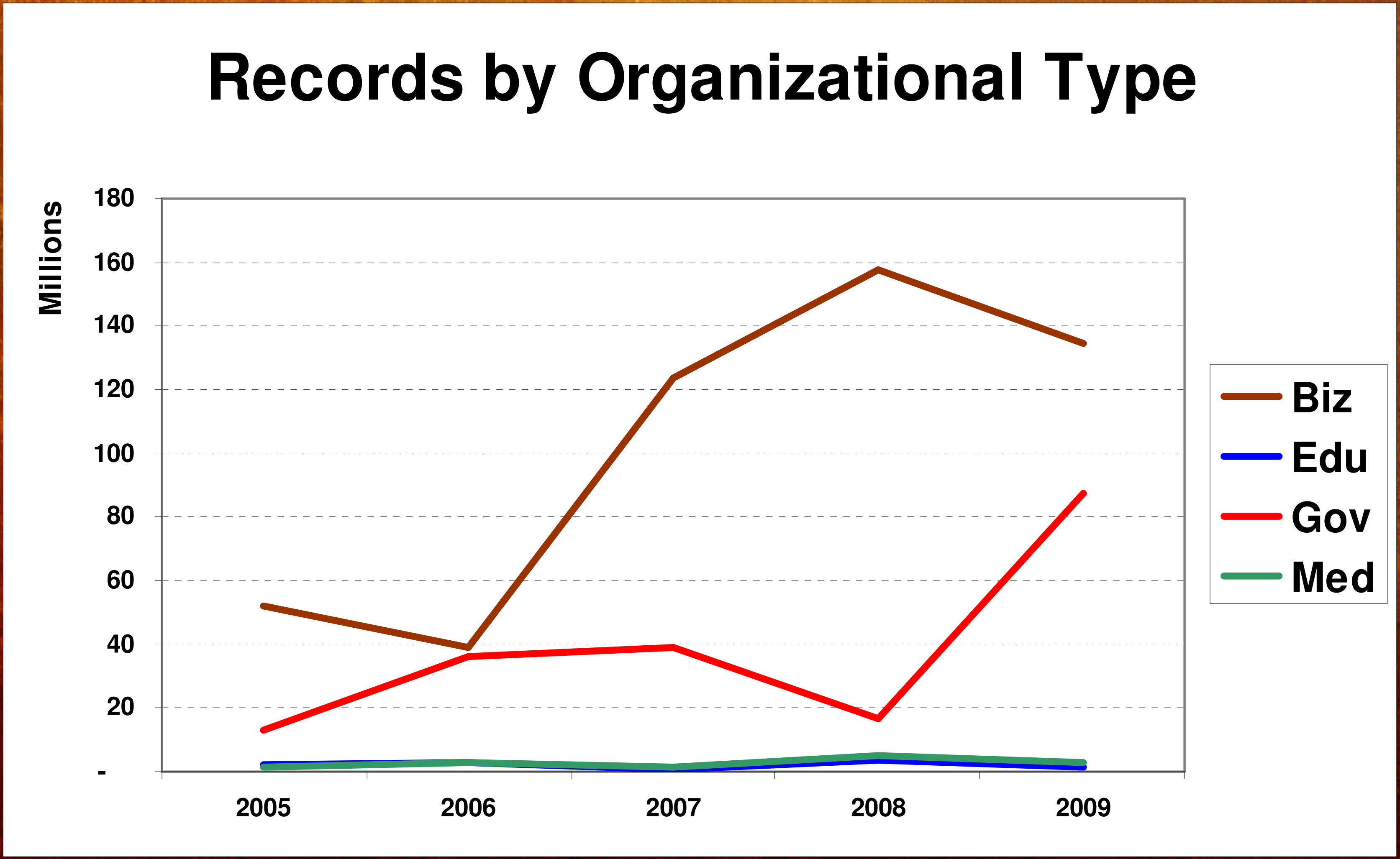
Top 5 Organizations for Number of Incidents

Organization	# Incidents
University of California System	21
LPL Financial	14
Blue Cross Blue Shield	14
Experian	13
Bank of America	12

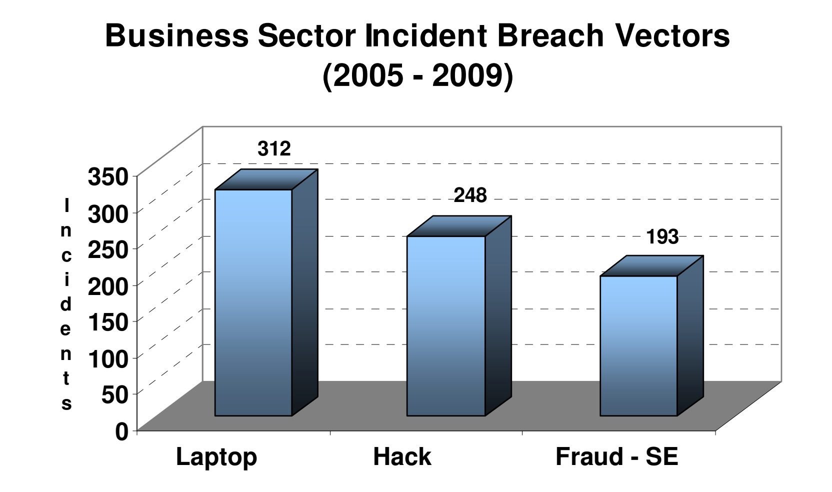


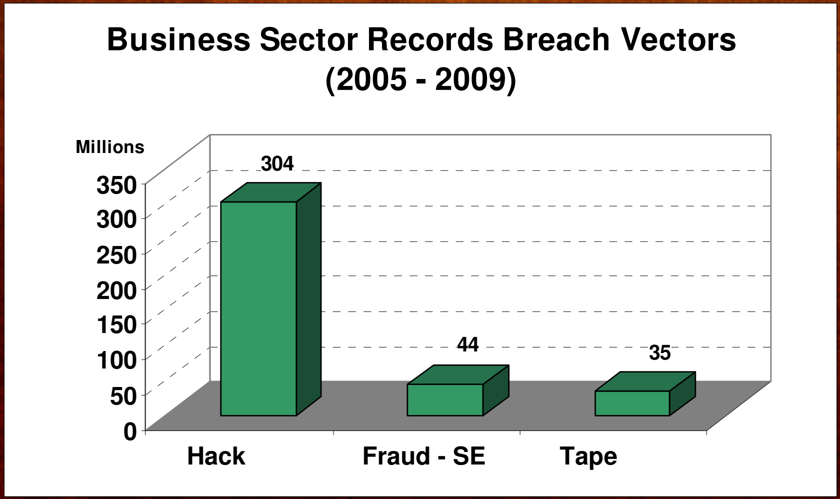


Records by Org Type

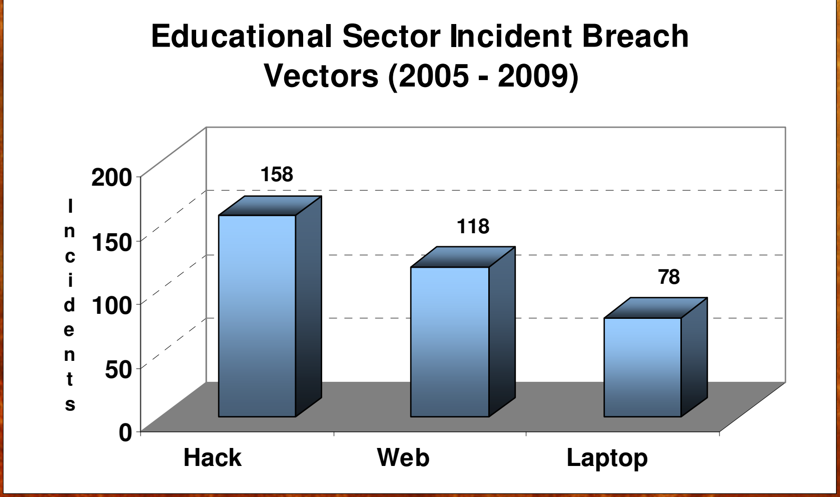


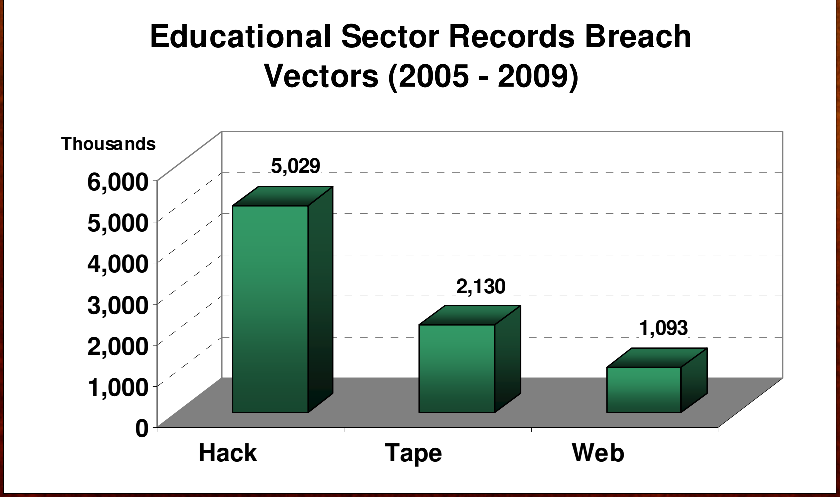
Business Sector



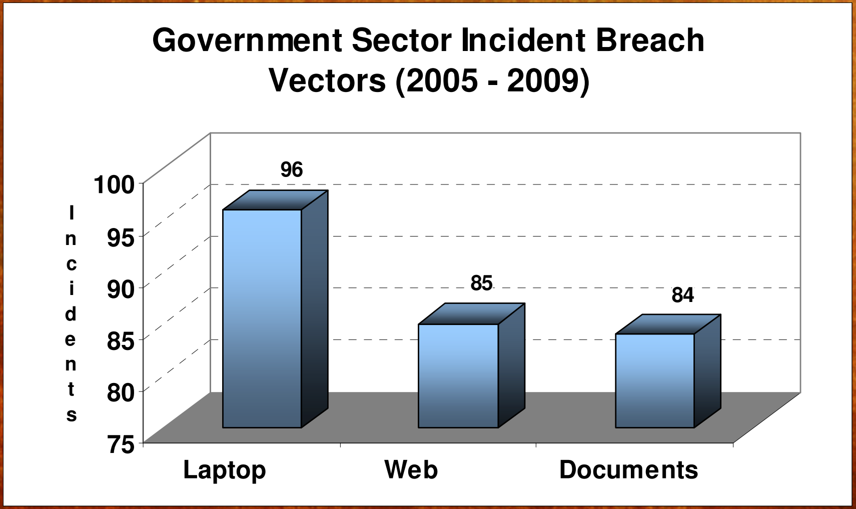


Educational Sector

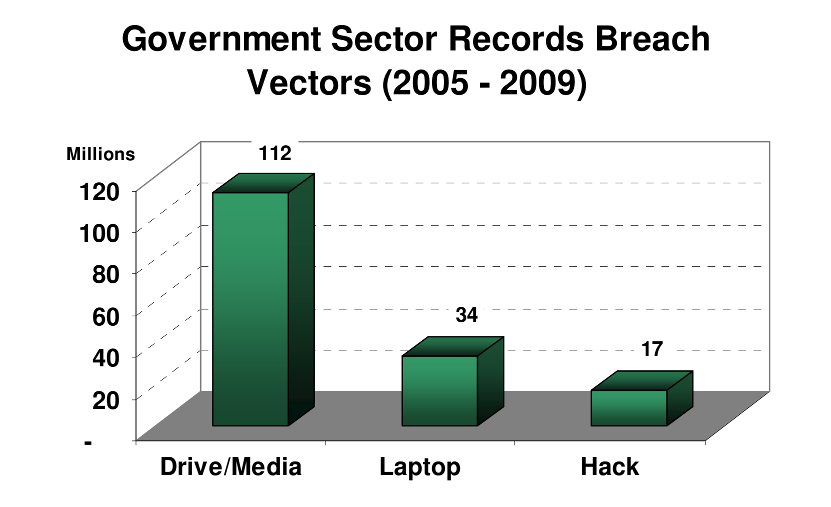




Government Sector

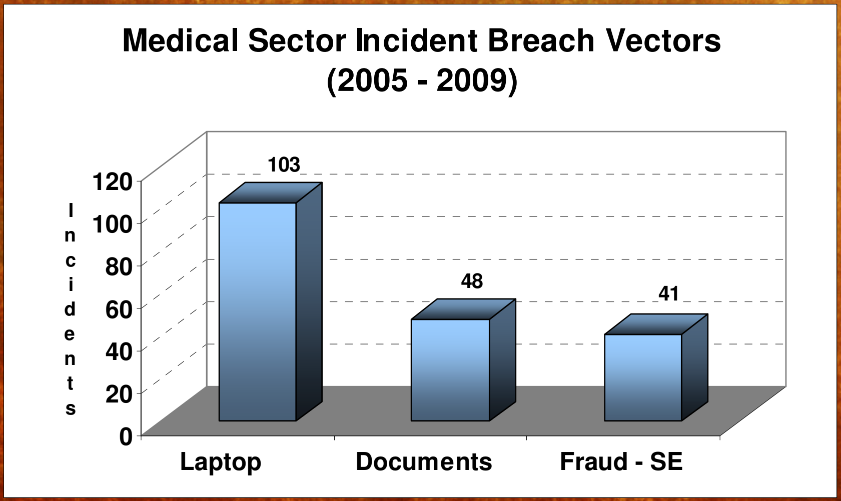


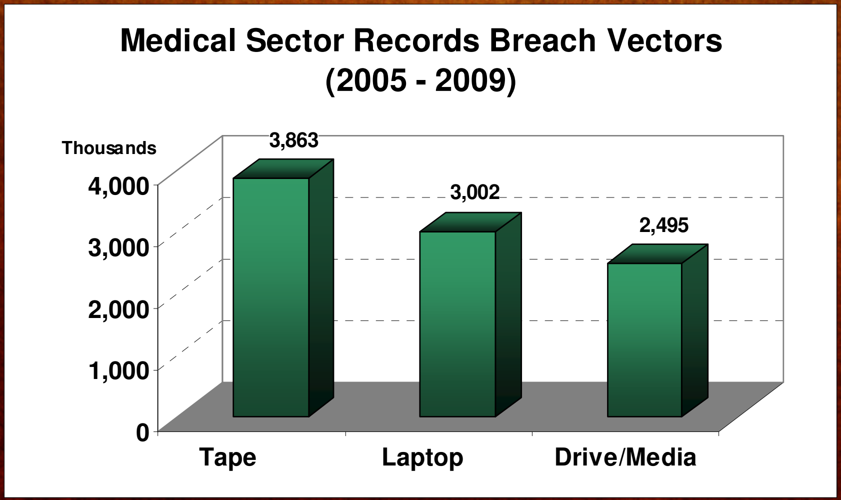
Government Sector Incident Breach Vectors (2005 - 2009)



Government Sector Records Breach Vectors (2005 - 2009)

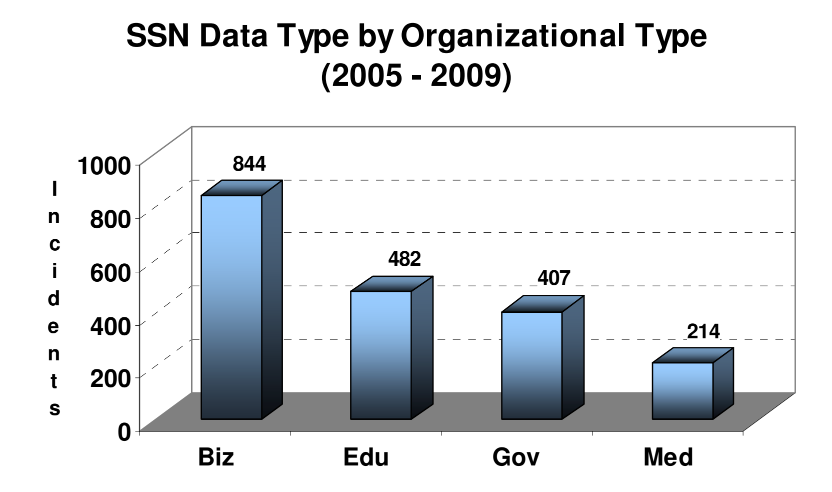
Medical Sector

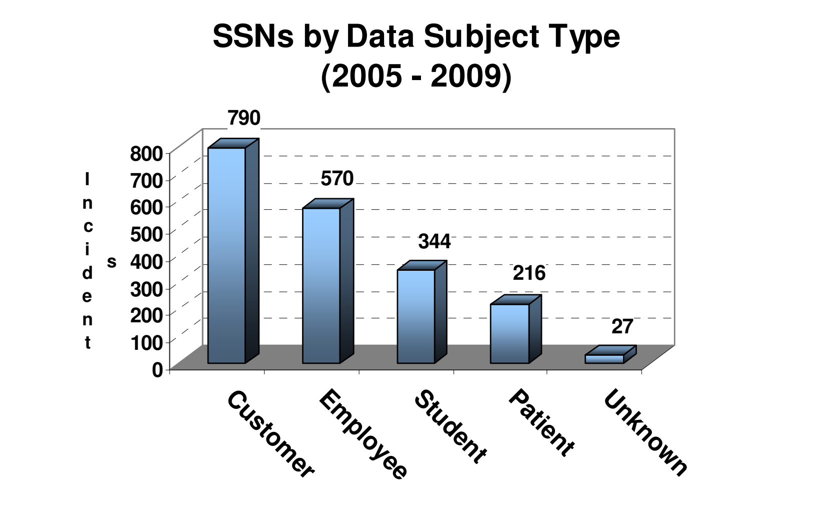




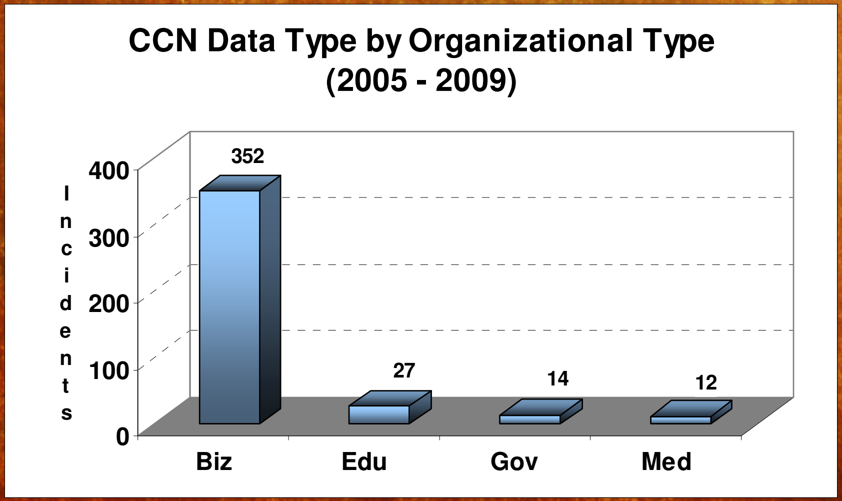
Data Types

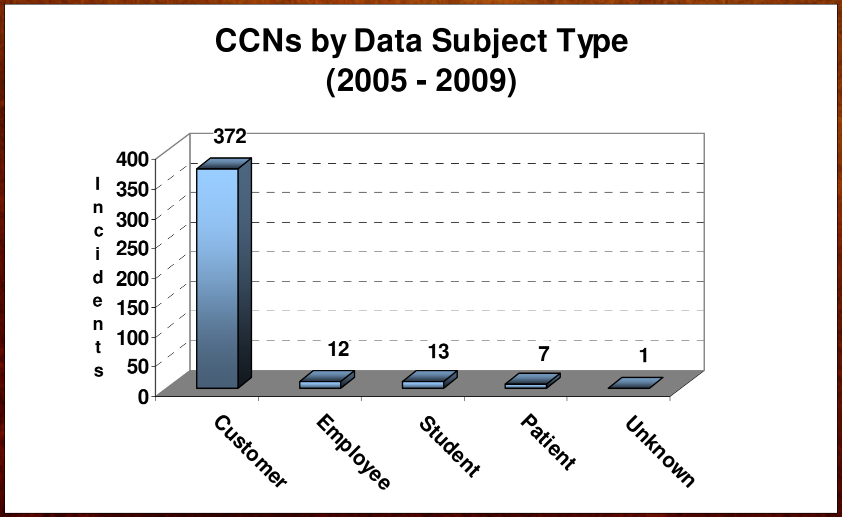
Social Security Numbers



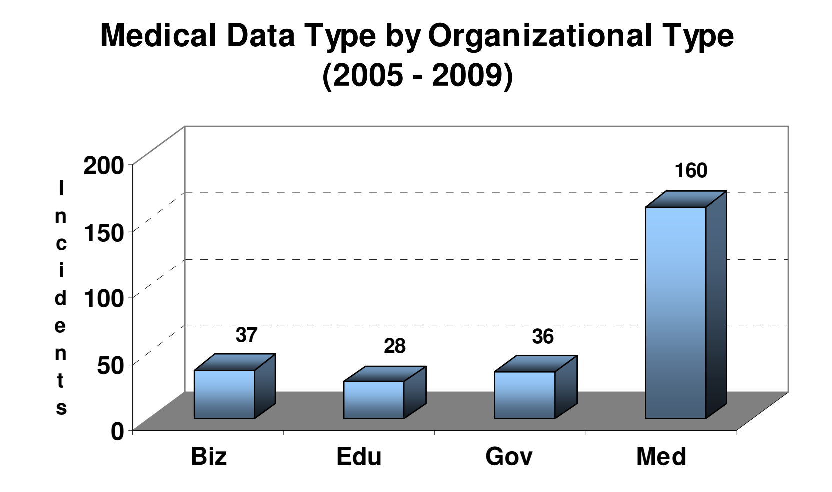


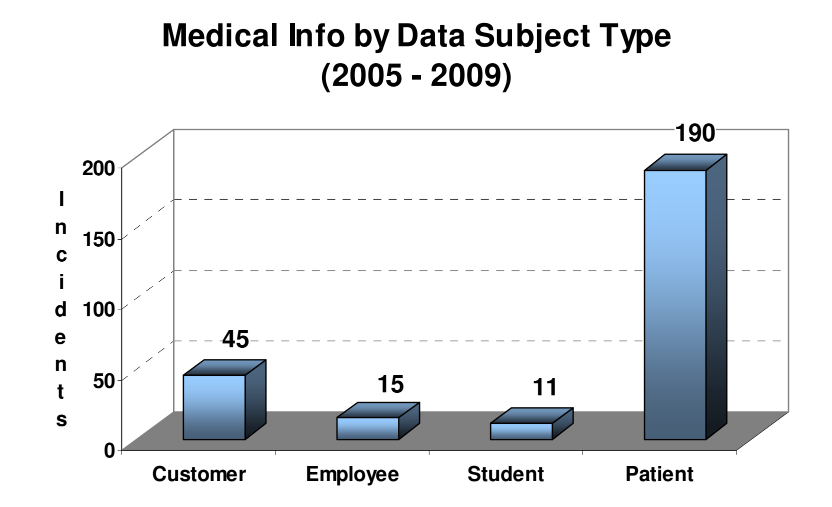
Credit Card Numbers





Medical Information





ID Theft Critical Elements

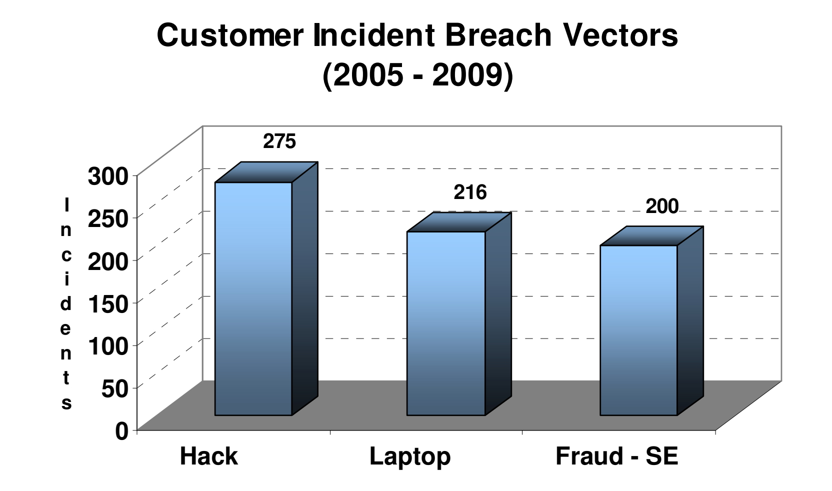
- Name and address combined with:
  - SSN
  - DOB

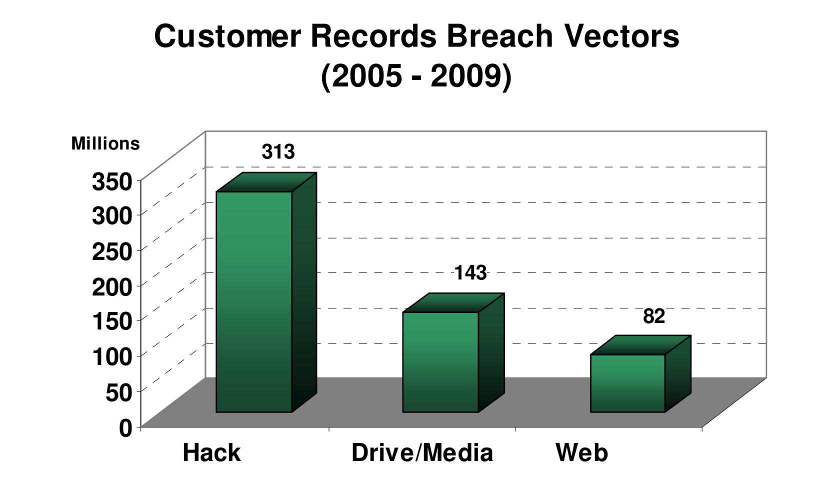
Relationships

Data Subjects and Victim Companies

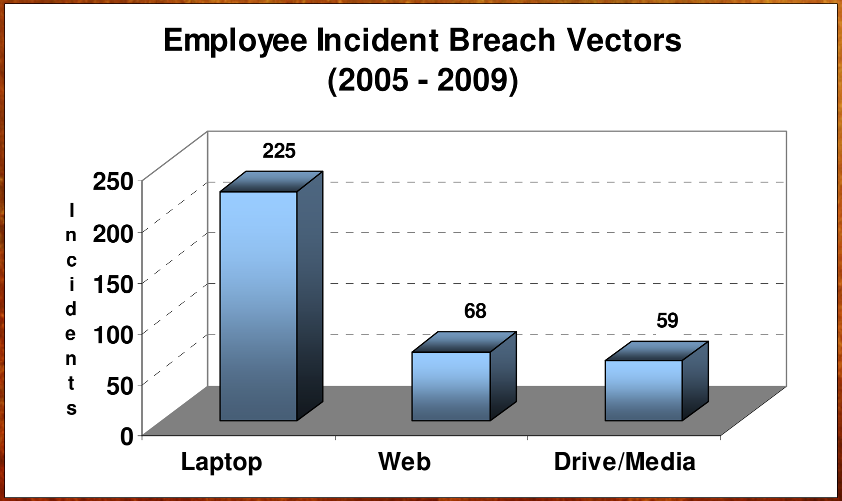
- The data subject is the person the data describes. You are the data subject in any record owned by an organization that contains data describing you.
- The relationships tracked are:
  - Customer
  - Employee
  - Patient
  - Student
  - Unknown

Customer Data

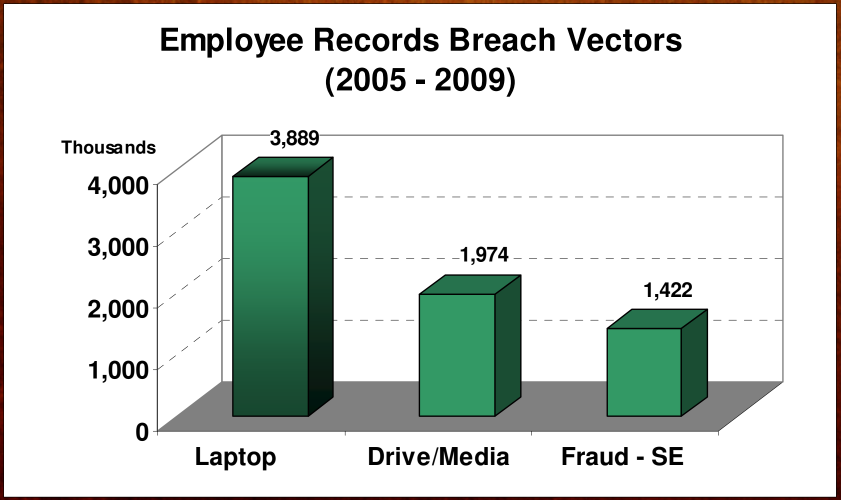




Employee Data

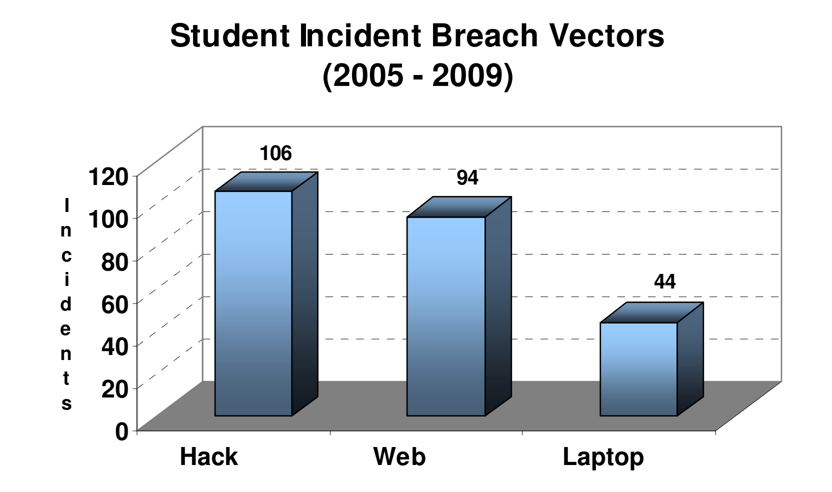


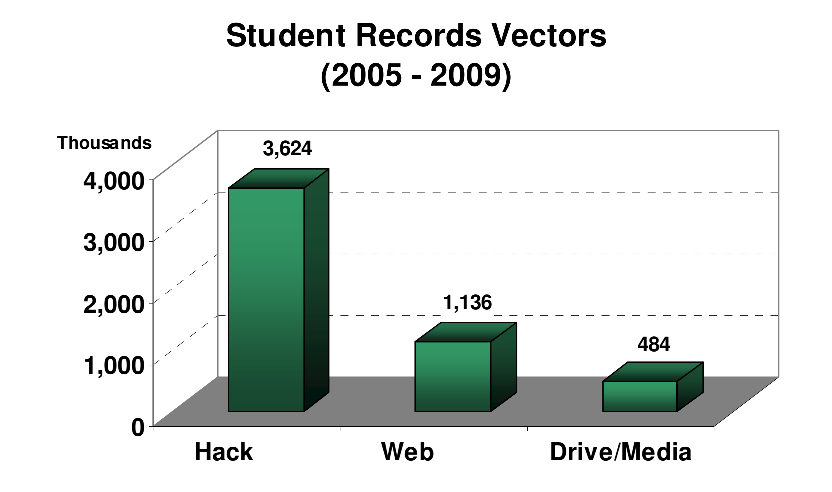
Employee Incident Breach Vectors (2005 - 2009)



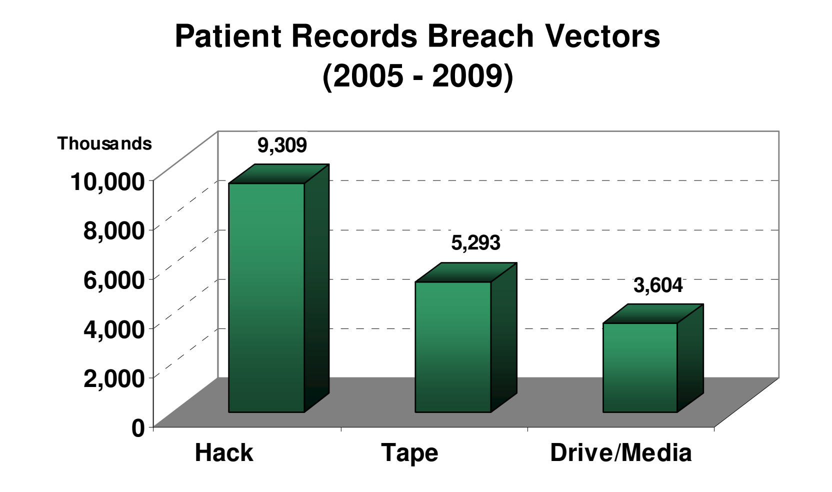
Employee Records Breach Vectors (2005 - 2009)

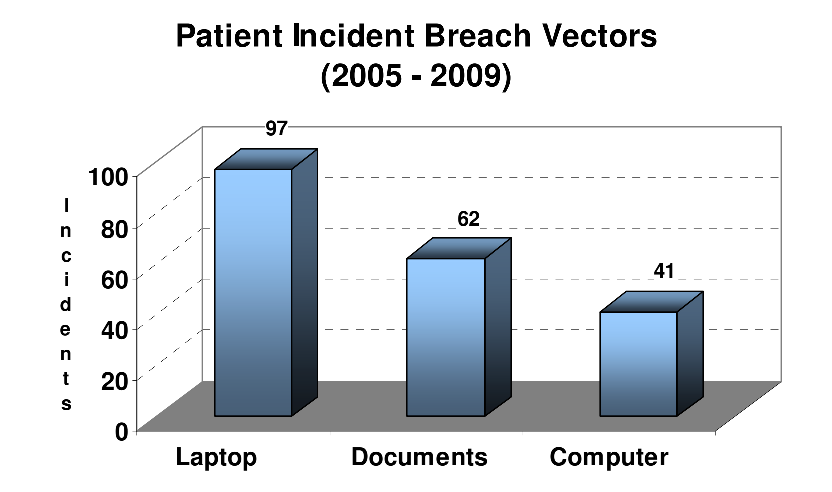
Student Data



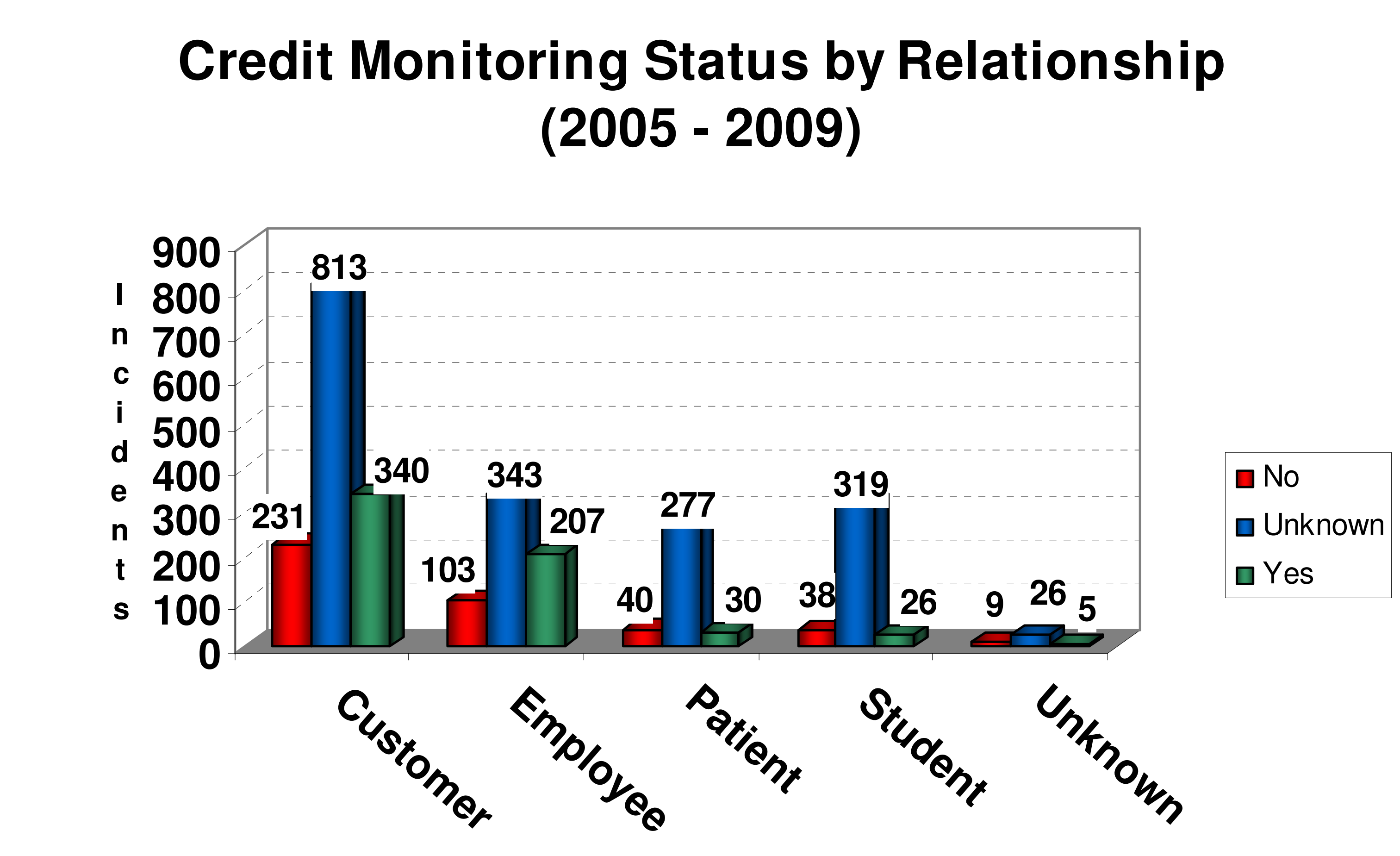


Patient Data





Credit Monitoring



Recommendations

Summary of Recommendations

- Data lifecycle management
- Information Security Awareness program
- Defense in Depth
- Third-party management
- Contingency plan
- Code Reviews

Questions?