

Privacy Data Loss An Operational Risk Approach

Michael Aiello
Polytechnic University
FE675 Operational Risk

Private Information

- Customer Records (Paper or Electronic)
- California Senate Bill 1386 requires institutions to disclose to their California customers' if their information is exposed to non-trusted 3rd parties.
 - Legal impact
 - Impact on Reputation
- An event where a customer's private information is exposed should be considered a loss event and accounted for when calculating operational risk

Available Data

- ChoicePoint data set
 - May have interest in keeping counts high

1/05	Christus St. Joseph Hospital, Houston Texas	16,000
	- Published reports on 4/26 said the hospital had sent letters to 16,000 patients saying their medical records and SSNs may have been compromised due to the theft of a computer in a January burglary.	
1/05	Kaiser Permanente	140
	- Health care company in March begins notifying patients that a disgruntled former employee had posted confidential information about them on the Internet. U.S. Office of Civil Rights had discovered the breach in January.	
1/18/05	University of California at San Diego	3,500
	- Officials reveal a mid-November breach may have compromised names and SSNs of students and alumni.	
1/20/05	University of Northern Colorado	30,000
	- University announces the apparent theft of a computer hard drive containing names, addresses, SSNs, bank account numbers, dates of birth and pay schedules for students and staff members and potentially their beneficiaries.	
1/25/05	Science Applications International (SAIC)	Unknown/Not disclosed
	- Division computers were stolen from the offices of SAIC, a research and engineering company, compromising personal information of current and past stockholders.	
1/26/05	GMAC Financial Services	200,000

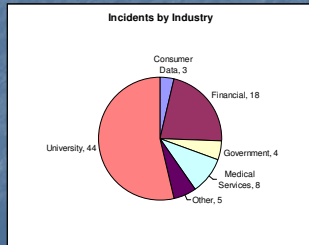
Available Data

- PrivacyRights.org
 - May be more objective about events

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint	Bogus accounts established by ID thieves	145,000
Feb. 25, 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures	Hacking	100,000
March 10, 2005	LexisNexis	Passwords compromised	32,000
March	Univ. of CA, Berkeley	Stolen laptop	98,400

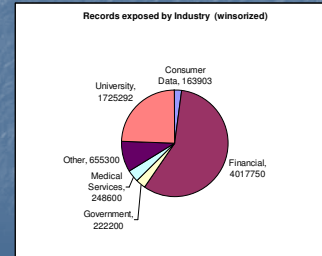
Impact

- 232 days of data
- 83 loss events (18 for financial sector)
- 35% chance of loss event each day.



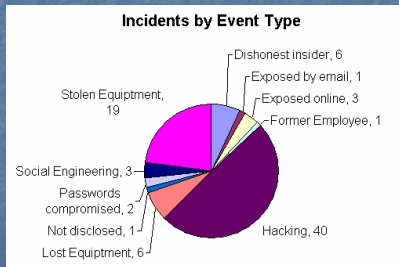
Impact

- One incident involving 40M records and another affecting 4M (not counted in these statistics)
- 7M records compromised (4.3M for the financial sector)
- 18803 records lost per day



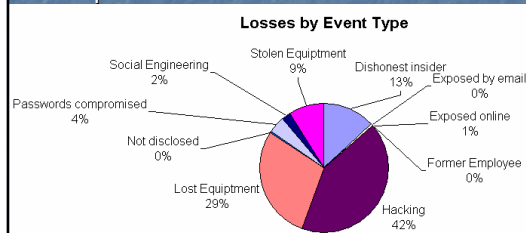
Impact By Incident

- Mostly "hacking" in both number of events and impact of events



Impact By Incident

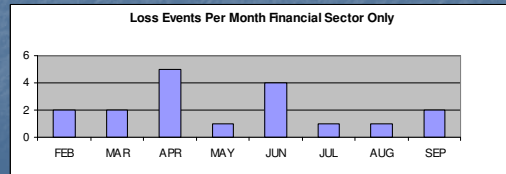
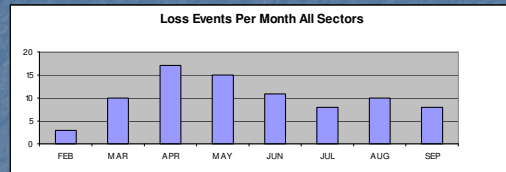
- Mostly "hacking" in both number of events and impact of events



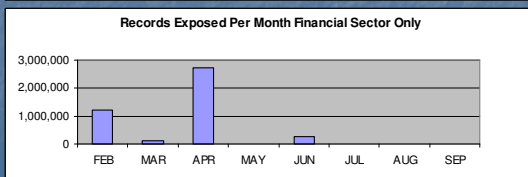
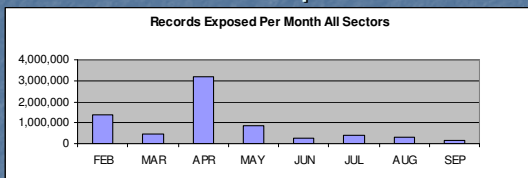
Operational Risk Approach

- View Monthly snapshot of events and impact
- Understand probability of X events occurring in a given month
- Understand probability of Y customer records lost in a given month
- Determine if these are independent.
- Focus on the financial sector

Loss Events



Records Exposed



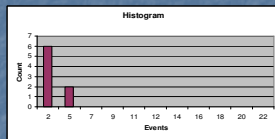
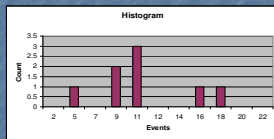
Realization

- There is no significant correlation between number of events and number of records lost.
- Must attempt to predict loss events and amounts independently.

Statistical Analysis – Exposure Events

All Sectors

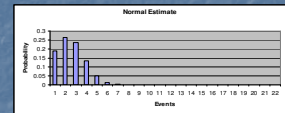
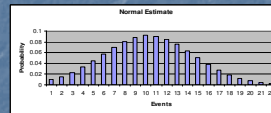
Financial Sector



Statistical Analysis – Exposure Events

All Sectors

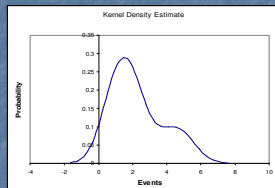
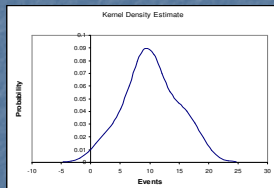
Financial Sector



Statistical Analysis – Exposure Events

All Sectors

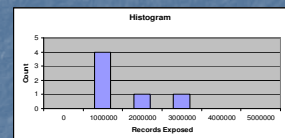
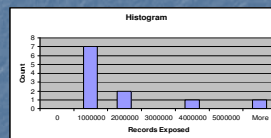
Financial Sector



Statistical Analysis – Records Exposed

All Sectors

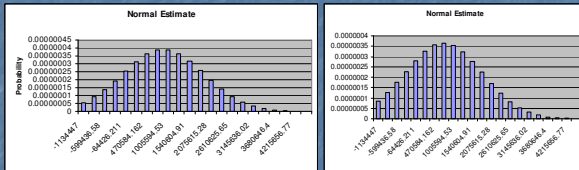
Financial Sector



Statistical Analysis – Records Exposed

All Sectors

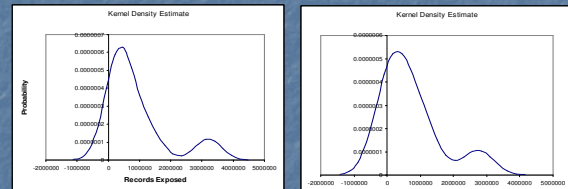
Financial Sector



Statistical Analysis – Records Exposed

All Sectors

Financial Sector



Conclusions

- Significant problem of customer data exposure across industries that handle such data
- Minimal relationship between # of events and records lost
- The incident and loss curves for the finance sector are similar to the industry as a whole
 - This type of comparison may help in the understanding the financial sector's risk (particularly with small data sets)

Concerns

- Validity of raw data
- Trends in legislation enforcement (more?)
- Amount of customer information is not a function of the gross revenue of an institution
- Reputational Risk = Hazard + Outrage. Outrage of an individual may be significantly less if millions of records were exposed as opposed to only a few.
 - Orders of magnitude difference in amount of lost data may only have minimal impact.
- Impact may vary by type of data lost.