

An Operational Risk Based Approach to Private Data Loss

Introduction

California Senate Bill 1386 requires financial institutions to release information and evidence related to identity theft to a victim with a police report or to the victim's law enforcement representative. In the event of a privacy breach, this law essentially implies that any institution that has customers in California must disclose that they have had a privacy breach directly to their customers. As of now, most institutions choose to notify all of the customer's involved in the breach regardless of origin. Other states are implementing similar legislation requiring disclosure.

In today's highly competitive banking environment, a financial institution's reputation for maintaining confidentiality of their customer's information becomes an asset. An incident where confidential information is lost can be considered an operational risk because it is likely to result in legal losses (directly) and in sales losses (indirectly).

This paper attempts to describe risk measurement oriented trends in the recent history of privacy exposure events which have been brought to the public because of Senate Bill 1386.

A context for private information

Private information describes a large range of data and is considered private only within a certain disclosure context. When a customer gives information to an institution to open an account, the customer is wholly entrusting the institution with such information. There are situations where the institution may then release the information

to vendors for processing. The risk to reputation due to the loss of data is still incurred by the original institution, even though the exposed copy of the data may actually be held by a vendor. Customers have little sympathy towards the institution during instances when it is not the originating institution itself that exposes information but is rather a third party. It is therefore important to examine the industry as a whole when describing potential losses due to customer data exposure.

A review of privacy exposure data

To the author's knowledge, only two groups maintain posted public aggregated lists of privacy loss instances including those cited under California Senate Bill 1386.

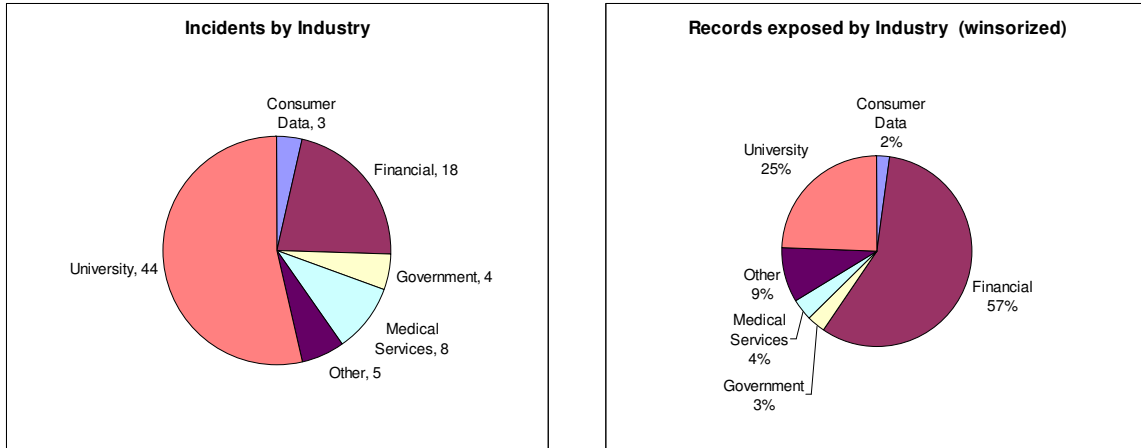
<http://www.privacychoicepoint.com/common/pdfs/Datadisclosures2005.pdf>

<http://www.privacyrights.org/ar/ChronDataBreaches.htm> (used in this report)

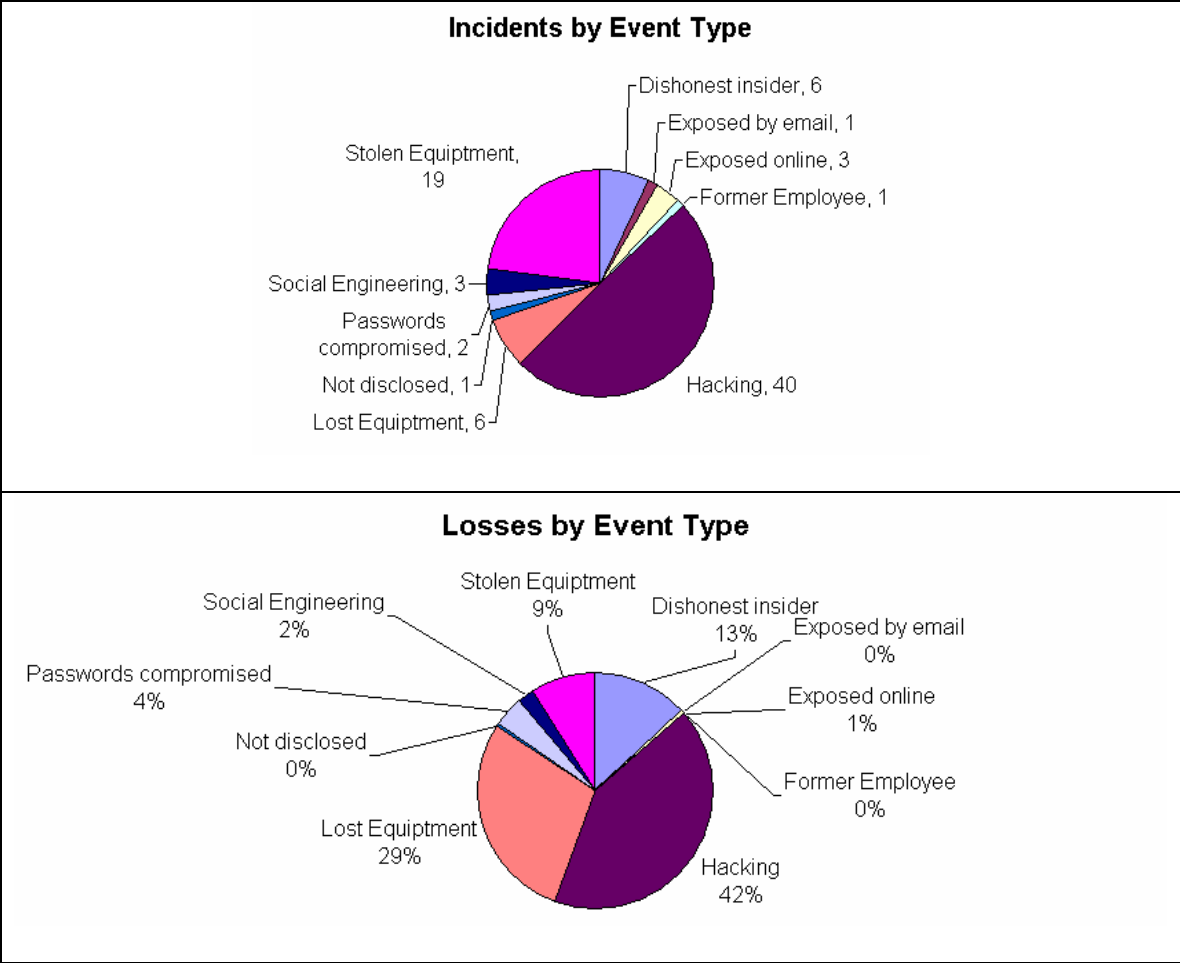
The groups began collecting the data after a large consumer privacy loss incident at ChoicePoint in February of 2005. The second set of data was chosen because the maintainer of the first set is part of the first set. The latest verified privacy information loss event occurred at the end of September 2005. This information occasionally contains entries which refer to incomplete disclosures or give ranges for amounts of privacy information lost. In instances where a range was given, the middle of the range was used as a data point for the event.

An initial snapshot of privacy loss data

The 83 recorded loss events were categorized by loss event type and by industry sector. The data is relevant over 232 days. This yields a probability of a loss event occurring in any sector on any given day 35.7%. If only events affecting financial services institutions are counted, the probability is 7.5% (18/232).

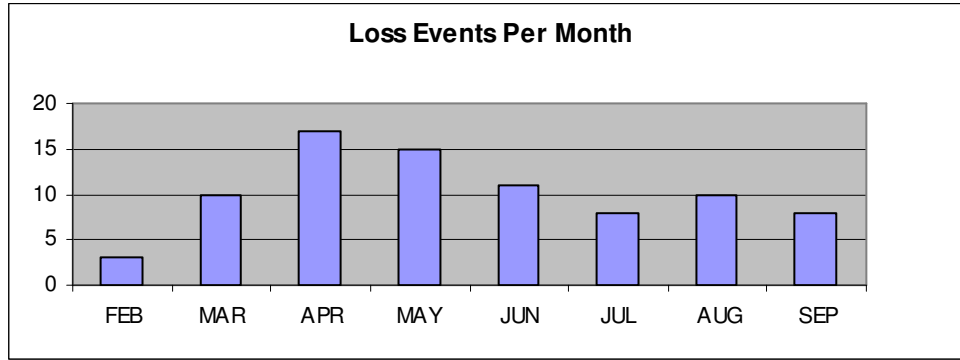


Universities account for the majority of incidents where records are exposed. However, if we examine the number of records exposed due to these incidents, the financial sector surpasses all others. 7033045 records have been exposed since February of 2005 (an average of 30315 records per day). For the financial sector, 4362300 records were exposed over the 232 day span with an average of 18803 per day.

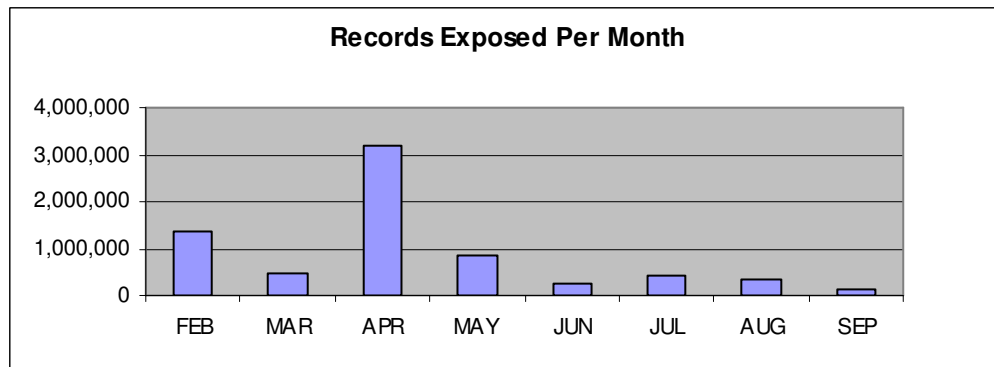


If the events are broken down by type, generic “hacking” events make up the majority of both events and loss amounts. It is important to realize the independence of these variables. Because of hacking’s influence in both breakdowns (total losses and count of loss events).

A monthly breakdown of loss events was performed in order to compute, based on historical data, the probability of loss events occurring in a single month and the amounts of such losses. There has been an average of 10 events per month, with the maximum occurring in April at 17 events.



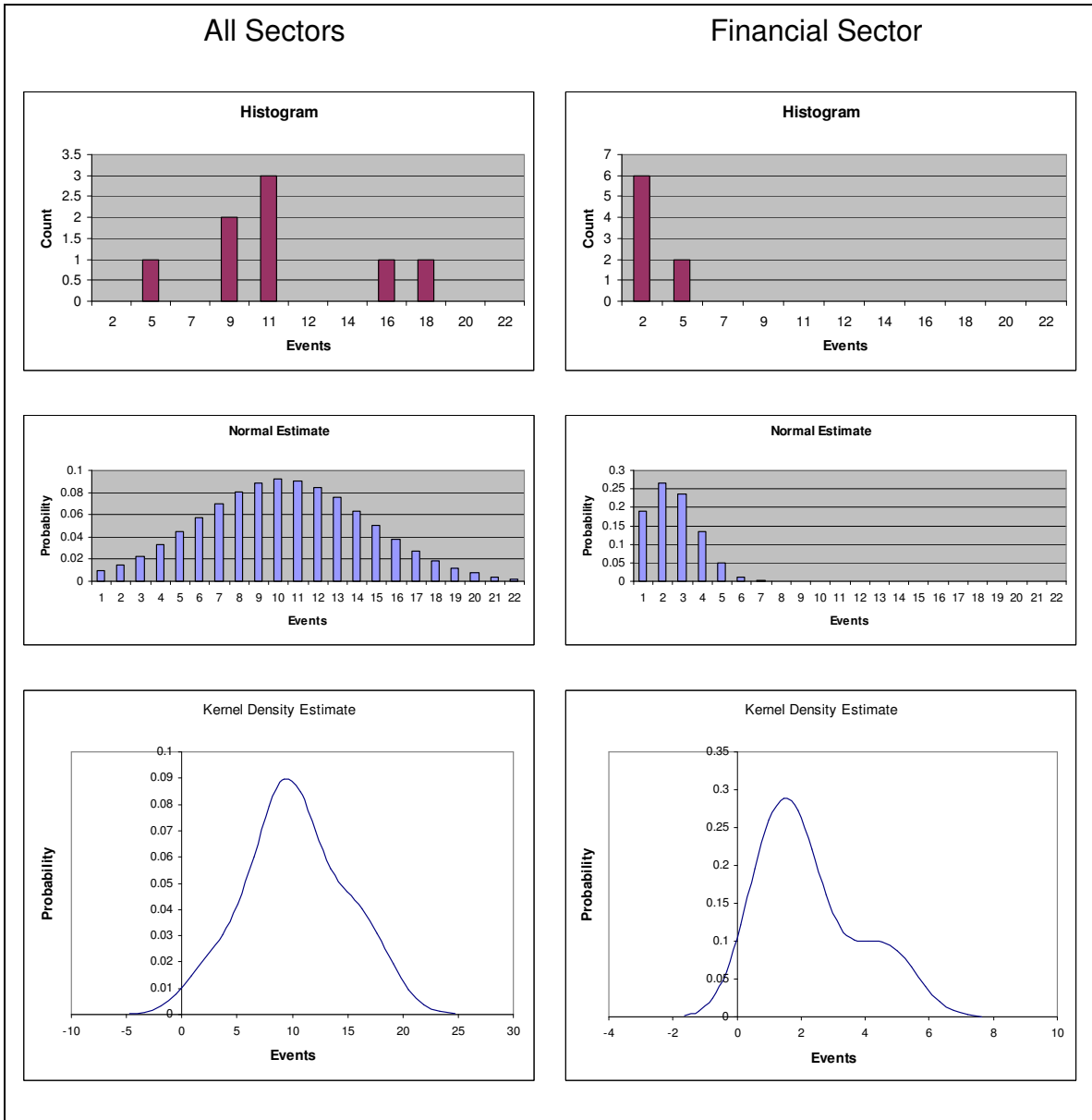
If we look at the amount lost per month, we are able to see that there is not a strong correlation with a high amount of incidents predicting a large loss amount (over the period of a month).



The operational risk of these events is the damage to the institutions reputation. For these institutions, the author believes that there is minimal difference between exposing 1000 or 5000 records in an incident, the impact on the reputation will be the same. This is, however, relative to the size of the organization and the number of records they handle. A more appropriate metric would be the percentage of total records a company handles that are exposed in each incident. Unfortunately, like most operational risk data, this is not available. The analysis is therefore concentrated on understanding

the probability of X events occurring over the period and the probability of Y records being exposed, independently during the month.

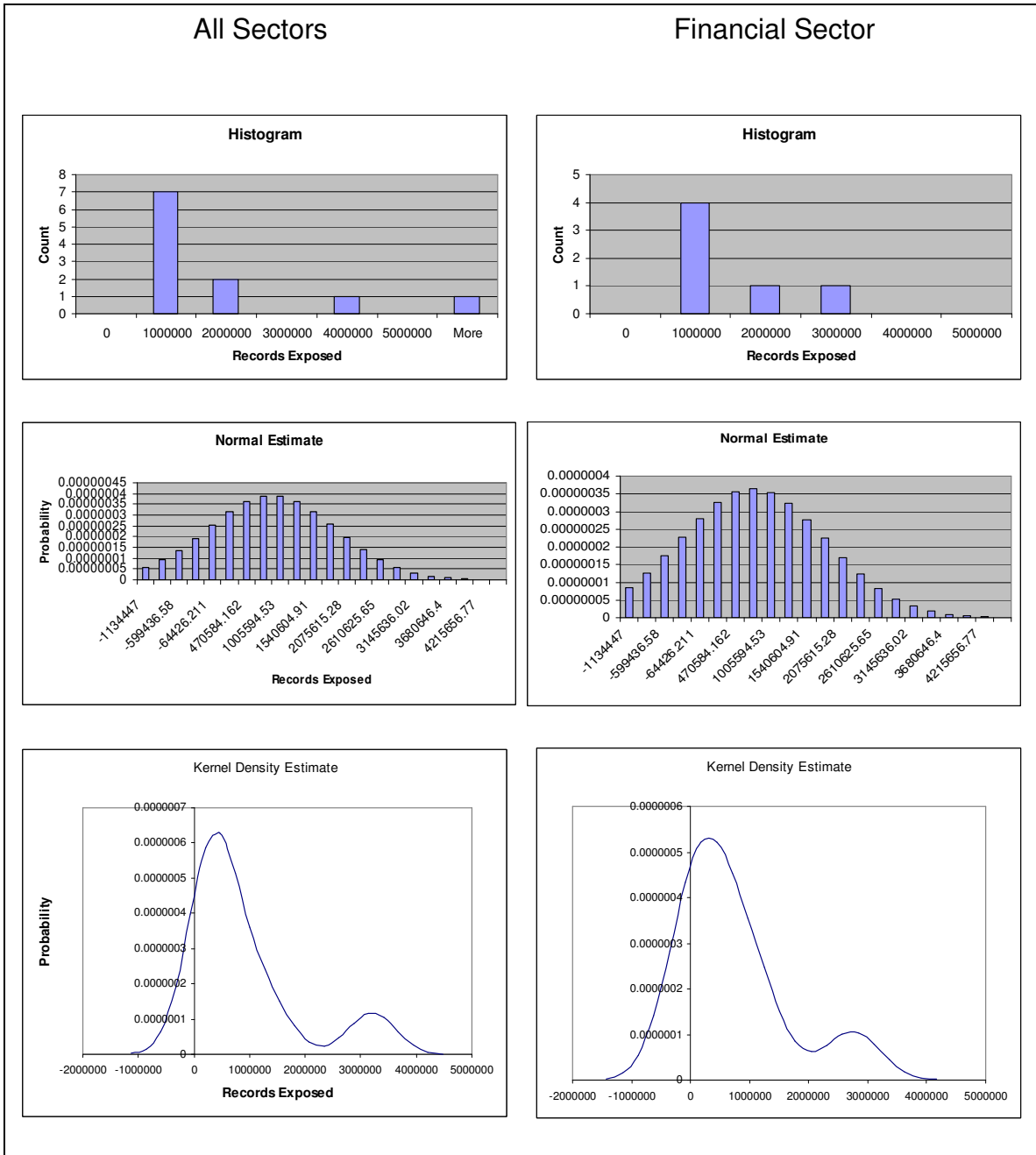
Exposure Events



Based on the above data, across all sectors, we can expect to have about 10 incidents per month with very few months having more than 20 incidents or less than 5.

Although fewer events are expected, the curve for the number of events in a month for the financial sector is similar to that of the industry as a whole.

Records Exposed



We can expect to have 1M records lost per month with few months where less than 500,000 or more than 3M records are lost. As in the event occurrence probabilities, the financial sector's probability curve follows that of the industry as a whole.

The operational impact of exposing customer records varies by industry and by institution. In order for an institution to best judge how much to spend, both in terms of information security and ease of accessibility to the customer, it must evaluate its individual impact of a loss event when attempting to prevent data exposure.