

IDENTITY THEFT AND FINANCIAL FRAUD BREACHES
An Analysis based on ITFF/ROC Reading Room Data
(itffroc.org)

Anthony Flarisee

INF 790

May 6, 2011

Introduction/Sample.....	2
Graphs and Comments.....	2
Categories	2
Comments	6
Organization Types.....	6
Comments	9
Conclusion	10

Introduction/Sample

Data breach information used in the graphing sample are from new ITFFROC reading room entries (submitted in March and April 2011) with breaches occurring from January 2010 to March 2011. In some cases, breaches actually occurred prior to January 2010, but were first reported to the public on a date within our sample range. Approximately 20 entries were collected for each month, with the most notable outlier being the month of February, with 31 entries. The only new reading room entries not included in the graphing process were the few entries that reported multiple breaches of various characteristics.

In graphing we provide a clear distinction between a single breach *instance* and the actual *number of records* lost by a breach. Our first set of graphs will display breaches instances and the number of records breached according to the category of breach that occurred. Our second set of graphs will display breach instances and the number of records breached according to the organization type in which the breach occurred.

Graphs and Comments

Categories

Accidental Disclosure – Confidential/sensitive information is mistakenly exposed publically. This includes situations involving private data, such as addresses or social security numbers, being posted on publically accessible websites. The information often remains posted for months or even years, sometimes coming to a halt when an individual enters their own name in a search engine, only to be linked to websites displaying the sensitive information. Mailing errors are common among accidental disclosures. Sometimes postal mail or e-mail is sent to the wrong address. In other instances, confidential information may be printed on the outside of an envelope, clearly visible to all parties.

Credit or Debit Card Fraud – This category describes breaches in which a credit/debit card skimmer was used to obtain another’s card information. Restaurant employees are common culprits, but were not included under “Insider”. Those insiders who viewed customer/associate card information and exploited it were included in the Insider category, if they did not use a card skimmer. Other common culprits of skimming were individuals who targeted public ATMs and gas station payment machines, attaching their skimming device and collecting card data from random users.

Hack – Scenarios in which an offender breached information electronically, without physically stealing a data storing device. Mostly deals with server/database breaches by outside parties.

Insider – Situations in which employees or business associates view and/or exploit confidential data. An offender may view customer credit card information housed in a database and use it to make fraudulent purchases. In several cases the confidential information would be sold to any interested identity thief.

Lost/Discarded Documents – Cases in which physical documents containing sensitive information are lost or left exposed to the public. The most common scenarios include the improper disposal (no shredding) of confidential documents. Sensitive papers are often found in dumpsters or recycle bins. This category also includes scenarios involving stolen physical documents, but this is more rare than cases of loss and discarding.

Lost/Stolen Device – The “device” here refers to an electronic device of some kind that stores data. The usual include flash drives, laptops, handhelds, and servers/PCs, with laptops being the most frequently stolen. Unlike the “Hack” category, this category deals with physical loss or theft.

Unknown – Cases in which data seems to have been breached, but the source of the breach is unknown. For example, sometimes customers who visited a particular restaurant may begin to experience identity theft. However, the source could range from a dishonest employee with a card skimmer, to a hacked server, or to a stolen laptop.

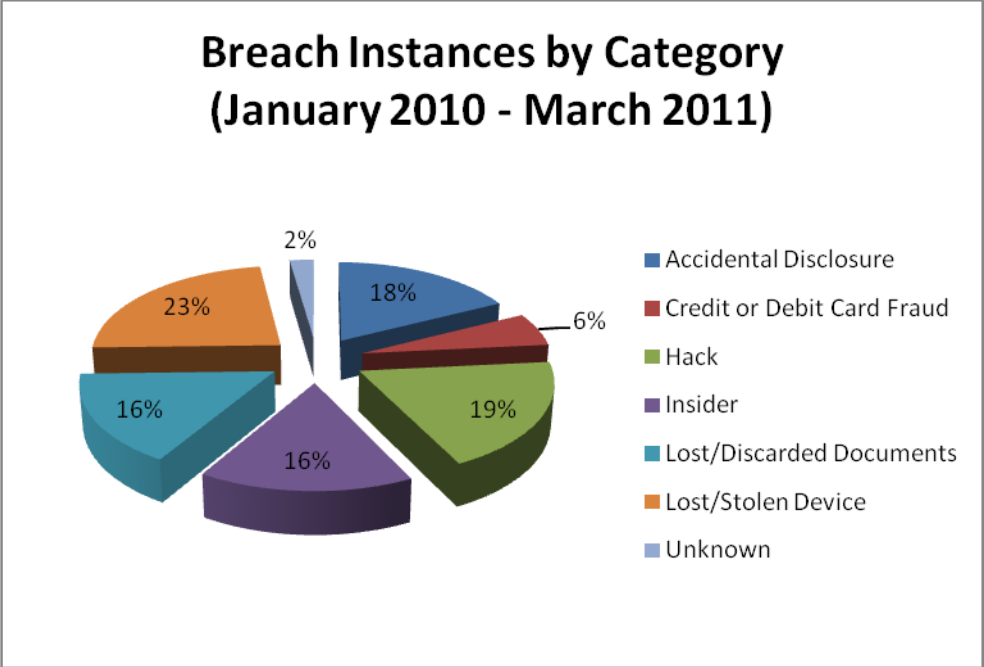


Figure 1: Beach Instances by Category

Number of Breach Instances by Category (January 2010 – March 2011)

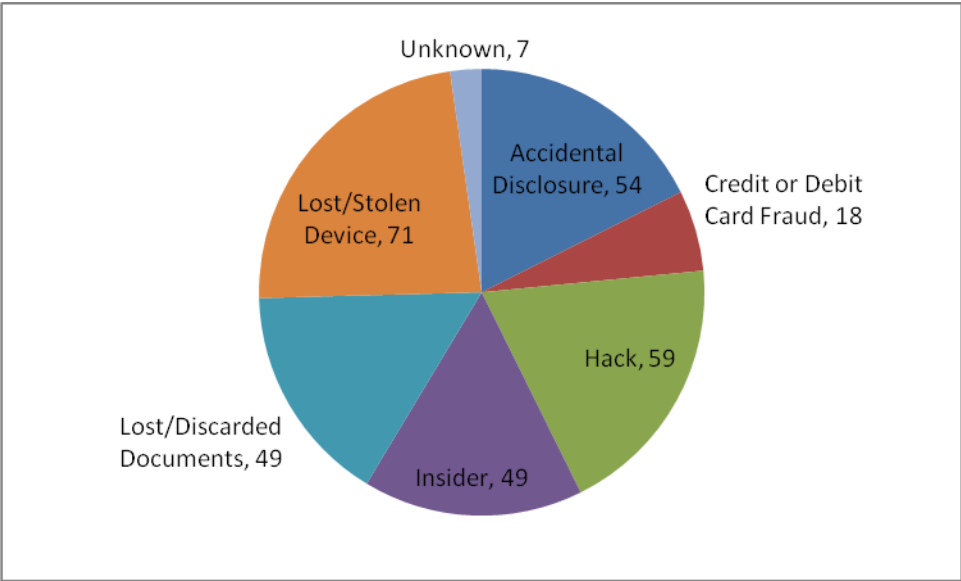


Figure 2: Number of Breach Instances by Category

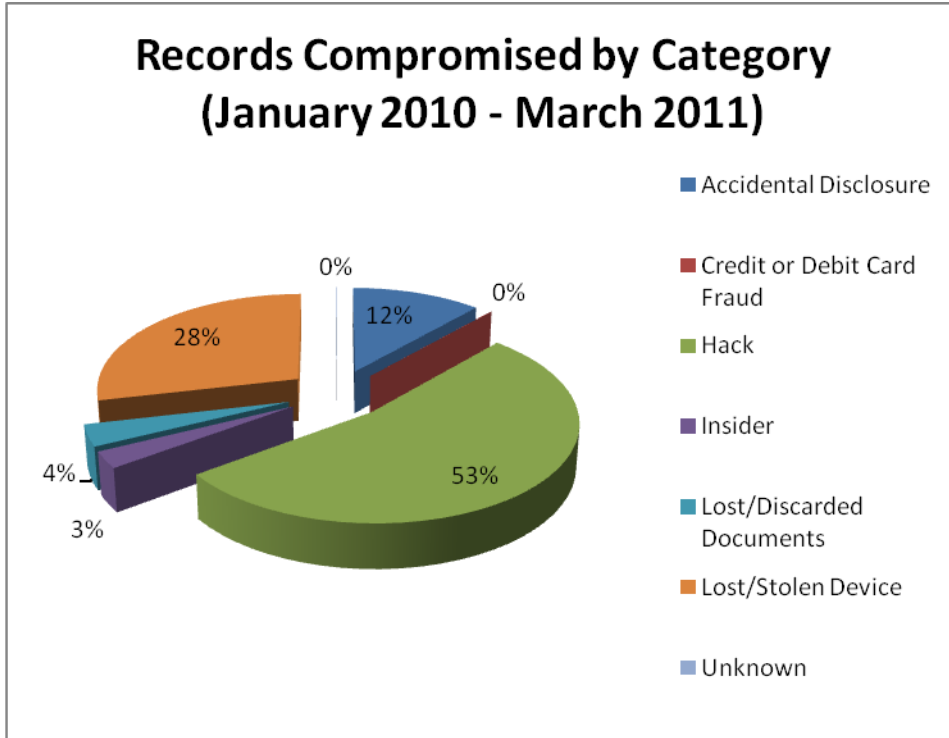


Figure 3: Records Compromised by Category

Number of Records Compromised by Category (January 2010 – March 2011)

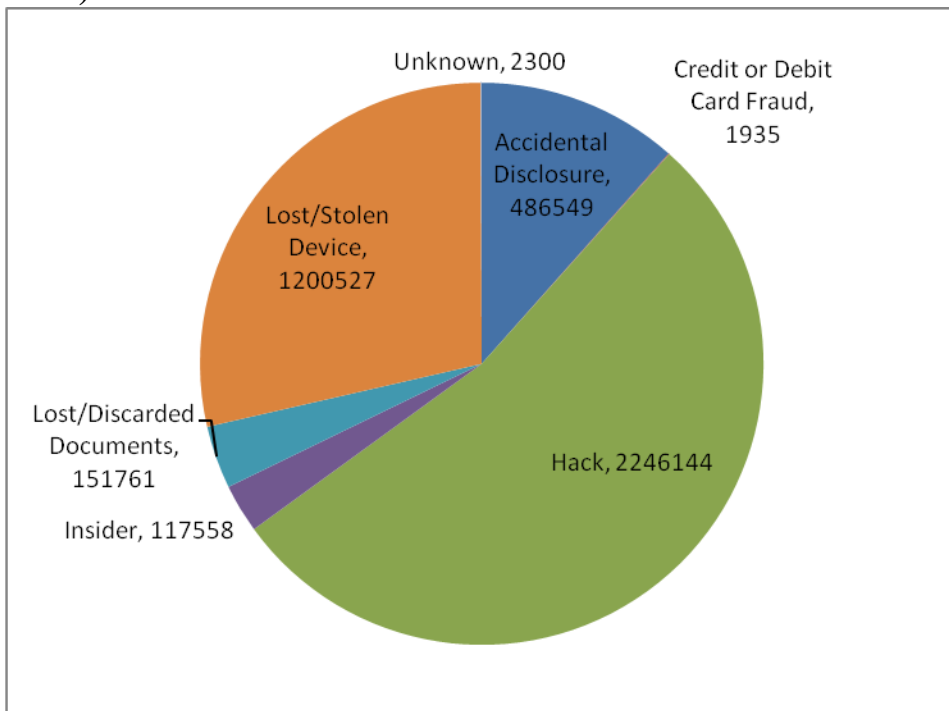


Figure 4: Number of Records Compromised by Category

Comments

Breach instances are shown to be fairly evenly distributed, with instances of lost/stolen devices being the most common. In regards to actual compromised records, it takes second place to hacking. The results have to be considered fairly predictable. Instances of electronic breaches may not be much larger than those of non-electronic breaches, but the number of records involved is usually far greater. Electronic sources often carry a large volume of personal data. The information held in one database or portable drive will likely exceed that which can be physically stolen or lost in most reasonable scenarios.

It should be noted that more than half of the records exposed due to hacking were involved in one single incident. The incident, in which 1.3 million records were exposed, was the breach of the Gawker website database by the hacker group known of Gnosis. Even without this instance, records exposed by hacking were extremely high, and would be even higher if *every* hacking breach (some not yet recorded in the reading room) from the last 15 months were included in our sample. Simply including the recent Playstation Network and Sony Online Entertainment (SOE) breaches, in which a reported 100 millions records were compromised, would almost completely trivialize an attempt to include the “hack” category in graphs such as those above.

Organization Types

Educational Institutions – Includes schools from all grade levels, including K-12, college, and trade school studies.

Financial and Insurer Services – Includes banks and insurance companies.

Government – Any government agency, including both state and federal.

Medical Providers – Usually hospitals, but includes nursing homes, hospices, etc.

Nonprofit Organizations – Organizations such as charities, trade unions, trade associations, etc.

Retail/Merchant Businesses – Simple profit based businesses, including stores, restaurants, online stores, etc.

Other – Businesses not included in the other categories. Hotels for example, fall under organization type “Other”.

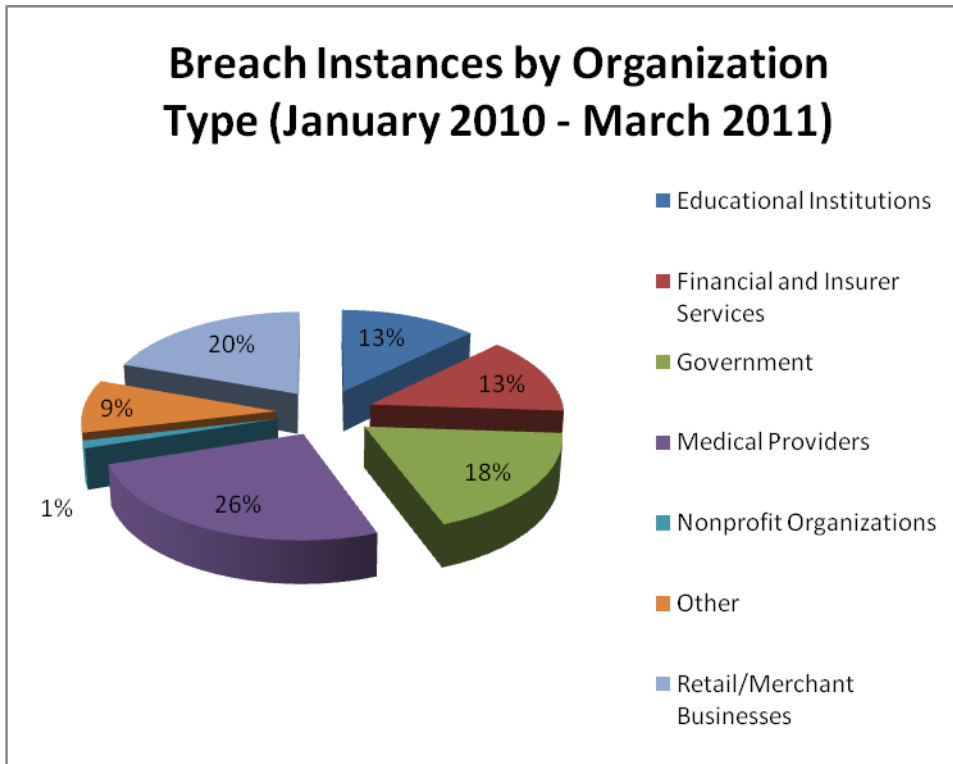


Figure 5: Breach Instances by Organization Type

Number of Breach Instances by Organization Type (January 2010 – March 2011)

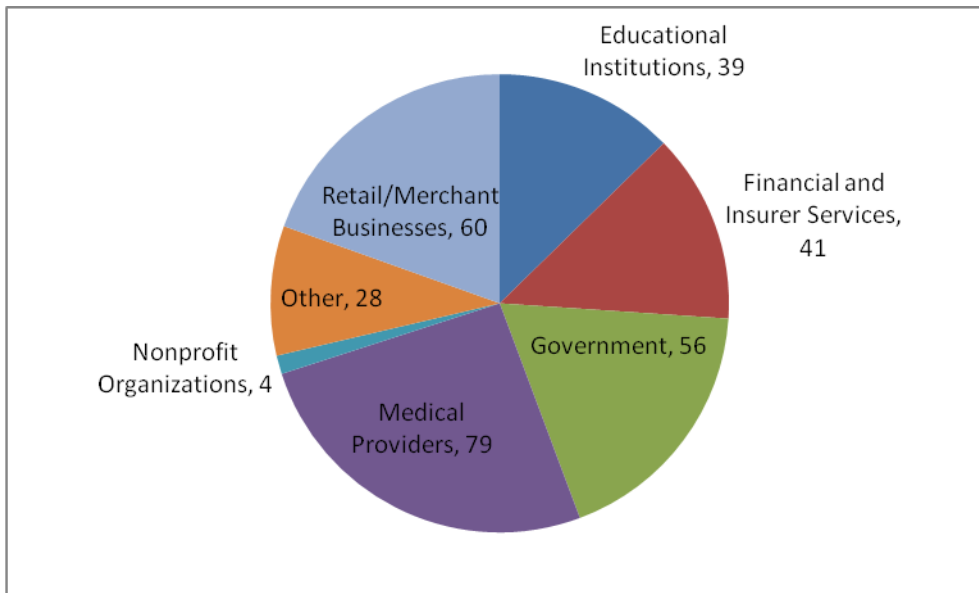


Figure 6: Number of Breach Instances by Organization

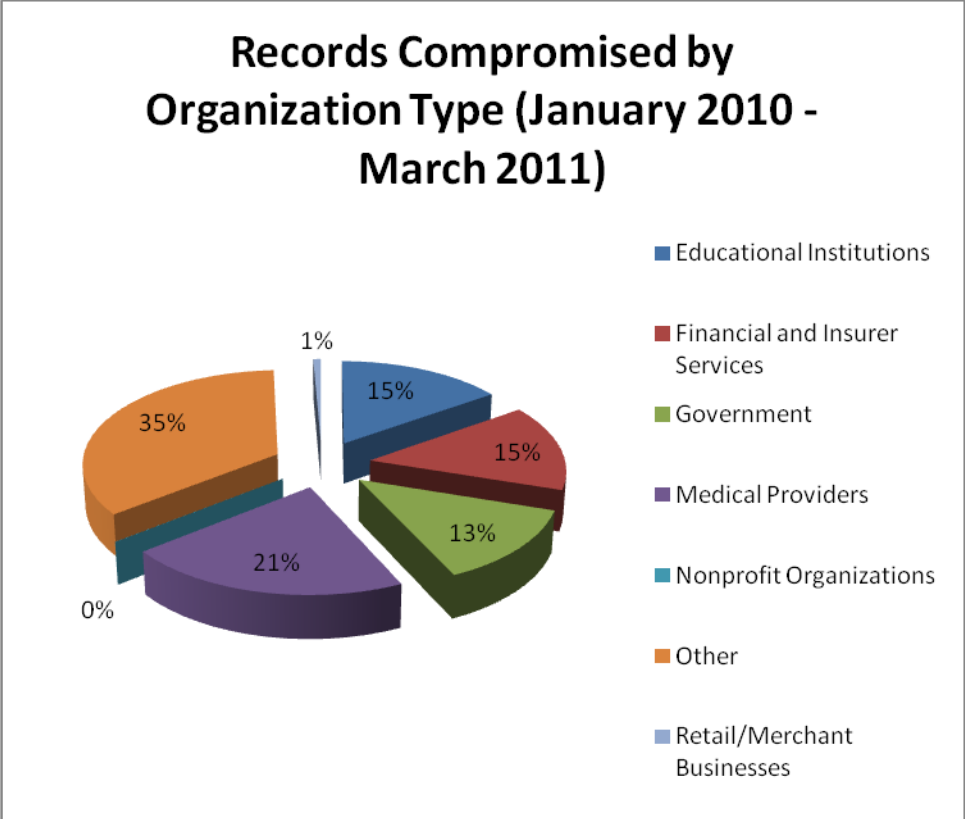


Figure 7: Records Compromised by Organization Type

Number of Records Compromised by Organization Type (January 2010 – March 2011)

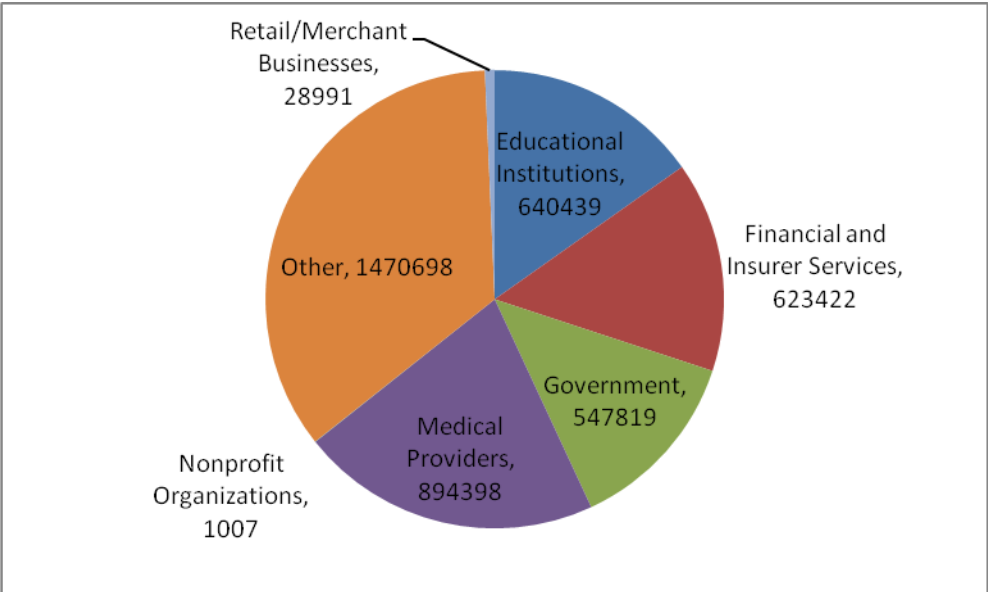


Figure 8: Number of Records Compromised by Organization Type

Comments

Both sets of graphs are fairly evenly distributed. The 1.4 million records lost by “Other” is largely due to the previously mentioned breach of the Gawker website, in which 1.3 million records were lost. Overall, medical providers account for the largest number of data breaches reported and the largest number of records lost. Attempting to provide a particular reason for this may prove difficult, but the word “reported” may be significant. One might point to strict laws based on the Health Insurance Portability and Accountability Act (HIPAA), for instilling in providers strict codes of conduct in regards to reporting breaches. Providers that do not abide by the law face heavy fines and perhaps other punishments.

Interestingly enough, a very small amount of records were reported as breached in relation to retail businesses. This is despite the actual instances of breaches being fairly high (second only to medical providers). The reason may simply be that retailers have little reason to store customer information, and therefore large quantities of records are rarely breached. Online stores have increased the usage of payment methods that do not require a customer to register to make a one-time purchase. In addition, a fair amount of retail breaches involve dishonest employees skimming card information. In these cases, the number of records breached is usually “Unknown”, and even if it was not, it’s unlikely that retail skimming would result in a very high volume of record breaches (relative to the other types of breaches).

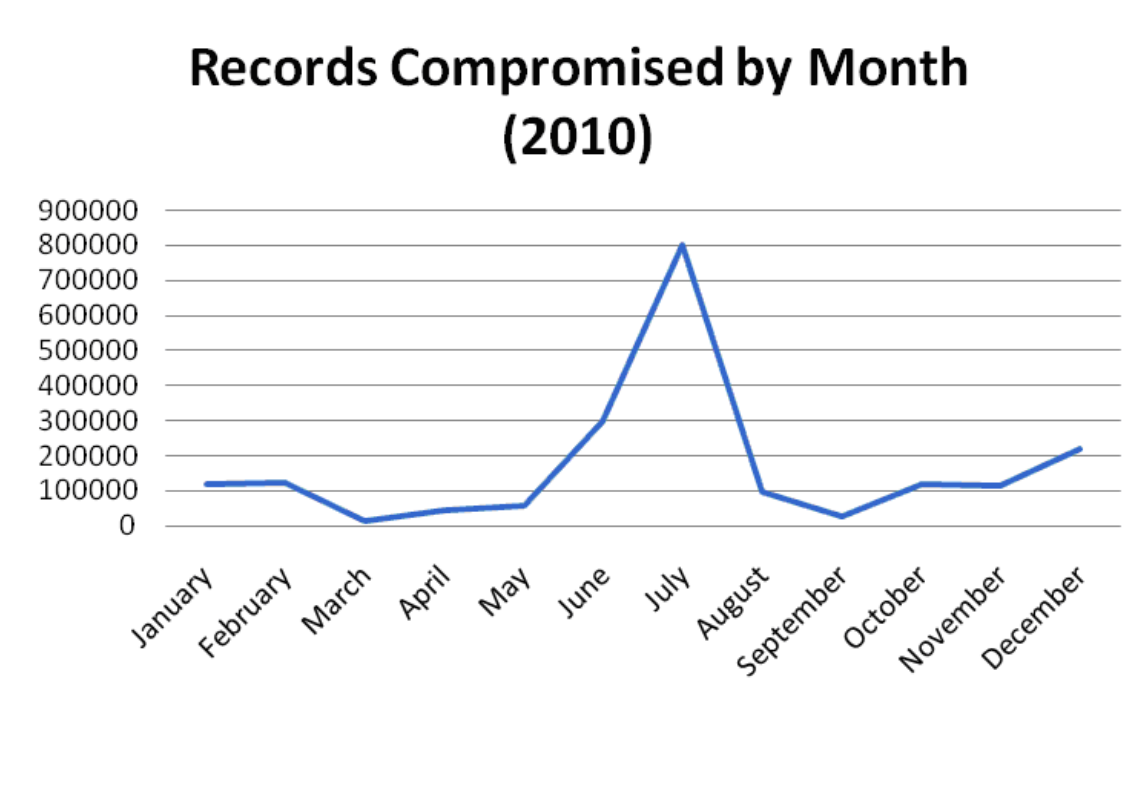


Figure 9: Records Compromised by Month

Seventeen entries per month were randomly selected to be in the sample for the graph shown above (due to there only being a total of seventeen entries for March 2010). Interestingly, the large spikes in June and July are not only attributed to single breach instances, but mostly to a number of instances involving lost/stolen devices and hacking during that time. As we know, these are the types of breaches that can be expected to involve the highest volume of record losses. One may also point out that December is the third highest month for record breaches, even though the Gawker instance (1.3 million records) was excluded. While this ultimately would make sense, as financial transaction activity likely increases over the holiday, we can attribute the high volume of December record losses to a single database leak incident, in which 200,000 records were compromised. All in all, our sample size of 17 is likely far too small to come to a conclusion about any relationship between information breaches and the time of year.

Conclusion

Ultimately, hacking related breaches and the loss/theft of storage devices, especially those that are portable, are the most devastating in terms of record volume. Such results highlight the need for the use of strong encryption when storing large quantities of personal data. This is especially true given how many of these instances are the result of stolen laptops. Their portable nature will likely make it difficult to ever fully prevent physical theft, so ensuring that the data held within is protected should always be the number one priority.

We should also point out that roughly one third of breach incidences involve either an insider or lost documents, emphasizing the need for companies to instill firm security/privacy policies to protect employee and client data. When accounting for insider skimming (card fraud) and accidental disclosures, we can point to insider errors or foul play as the primary cause of most data breaches. This fact only reinforces what is already known by most security experts. Simply put, the constant threat of outside attacks must always be accounted for, but not without simultaneously protecting against dangers from within.