Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work

Ragib Hasan
rhasan@ncsa.uiuc.edu

William Yurcik
byurcik@ncsa.uiuc.edu

National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign (UIUC) Urbana, IL 61801.

ABSTRACT

A welcome but unintended consequence of recent state disclosure laws in the U.S. (most notably California SB 1386), has been a continuous stream of privacy breaches reported in the mass media. In this paper, we provide empirical analysis of disclosed breaches for the period of 2005-2006 to better understand what is happening in aggregate (overall patterns and trends) beyond the often sensational individual cases reported in the media. By processing raw data from the best available sources, we have created an Internet-accessible database that can be queried for breach statistics and a data set that can be shared so that our analysis can be validated, as well as enable future analysis by other researchers. The statistical analysis we report here is a first step toward answering the important and complex questions of why privacy breaches are occurring and what may be the best practices to prevent and mitigate their effects. Policy formulation to address privacy breaches is already in process at the organization, state, and national levels largely driven by mass media coverage – it is our hope decision-makers take the empirical evidence we report here into consideration.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and Protection*; H.3.4 [**Information Systems**]: Information Storage and Retrieval—*Systems and Software*; D.4.2 [**Software**]: Operating Systems—*Storage Management*

Keywords

privacy breaches, breach disclosure laws, storage security

1. INTRODUCTION

What do these trios of organizations have in common?

1. Bank of America, Fidelity, and Bank of Bermuda
2. U.S. Departments of Agriculture, Treasury, and Veterans Affairs
3. Verizon, T-Mobile, and AOL
4. Ford, Boeing, and JetBlue
5. the Medical Centers of University of Washington, University of Pittsburgh, and Delta Blood Bank

These trios represent a wide range within five of the eight critical national infrastructures (in the U.S.) with disclosed privacy breaches that have been reported in the mass media between 2005-2006 [2, 3, 15]: (1) banking and finance, (2) government services, (3) telecommunications, (4) transportation, and (5) emergency services. [1] PrivacyRightsClearingHouse reports a total of 90 million records containing sensitive personal information have been compromised during this period [1].

Risks from releasing private information in a breach are twofold: (1) privacy risk and (2) identity theft fraud [14]. While the cost of personal information being revealed is specific to each individual and thus hard to quantify[2], the cost of identity theft *fraud* for individuals typically runs hundreds of dollars and several years to clear their name and the cost of identity theft *fraud* for organizations has been estimated to be in the tens of billions of dollars [5].

This is a new problem because third parties now control private data that used to be under an individual's direct control – data that used to be controlled exclusively by individuals physically within their own home – is now increasingly stored by third parties with Internet operations that may or may not invest in protecting private data [14]. For example, personal mail, finances, shopping behavior, and work/leisure activities that used to leave only physical traces that could

[1] PDD-63 identifies these eight critical infrastructures[8]. The critical infrastructures not represented in these trios are (6) electric power, (7) oil and gas, and (8) water.

[2] For example, the cost of making private medical information public is dependent on whether the person has a condition he or she wants to remain secret or not. Thus the cost to an individual for revealing private medical information may vary from zero to lifetime career earnings for medical conditions that, if exposed, could terminate a career.

be physically contained now leave Internet traces with third parties.

The only reason we know about most privacy breaches are new state laws mandating disclosure to affected parties of incidents that release private data due to security compromise. In the past, organizations did not notify affected parties when their private data was compromised, leaving them at risk for identity theft fraud often only to find out when it was too late. New state disclosure laws allow individuals to take proactive steps to safeguard their identities after a compromise has occurred – thus returning control of private data back to individuals.

Disclosure laws have done much more than giving individuals notice, they have also improved protection by providing metrics upon which to measure security where no metrics existed before. However, since there are typically no public disclosure requirements in state laws and disclosure laws have not been actively enforced, reporting in the mass media has been spotty and focused on the sensational rather than insightful analysis.

The goal of this paper is to provide both comprehensive and in-depth analysis of privacy breaches beyond mass media reports by processing raw data from a combination of best available sources for patterns and emerging trends. In previous work, we framed a storage security threat model which organized potential attacks into categories along multiple dimensions [11]. In this work, we seek to understand the risks from potential attacks by analyzing the mechanisms, frequency, and impact of privacy breaches from empirical data. While past experience may or may not be indicative of future attacks, understanding vulnerabilities that are being exploited in the current environment is an important starting point for future improvement. Future attacks are unpredictable, but known risks can be measured to serve as a foundation for looking ahead. Due diligence dictates that security investment to mitigate risks should be based on evidence; otherwise it will expose the organization to continuing privacy breaches and liability from shareholder/customer/third-party lawsuits [12].

The remainder of this paper is organized as follows: Section 2 introduces the current privacy disclosure laws in the U.S. (at the time of publication). Section 3 provides details about the best available data sources we use in this investigation. Section 4 presents statistical processing results (in multiple dimensions) describing the source data along with analysis. Section 5 provides a brief overview of related work. We end with a summary and future work in Section 6.

2. PRIVACY BREACH DISCLOSURE LAWS

In the U.S., 28 states have enacted privacy breach laws (at time of publication), see Table 3 at the end of the paper. These state laws are similar but may have different requirements for notice trigger, timing, content, and recipients [13]. While other federal laws[3] also require reporting of storage security status of different various forms, these federal laws are focused on compliance with financial requirements for companies and non-profit organizations to federal regulators. In contrast, when private information is compromised, privacy breach state laws typically require only direct notification between the third party organization with the compromise and each affected individual without involvement from federal/state regulators or any level of law enforcement. Private information is defined to be any of the following: social security numbers, drivers license number, bank account numbers, credit/debit card numbers, as well as any other personal identifying information.

While the compromise of any individual identity has the potential for fraud, it should be noted that experience indicates only a percentage of compromised private data will be involved in identity theft fraud. For example, criminal investigators have found only 800 cases of fraud among the 163,000 identities exposed by the ChoicePoint privacy breach in 2004 (less than 0.5%) [9]. Nearly all breach disclosure laws provide an exemption if the personal data was encrypted at the time of the compromise [13].

3. DATA SOURCES

Privacy breach disclosure laws are currently established only in the United States and are not enacted in every state. However, even in the growing number of states that have such laws, disclosure reporting is only required between the organization and the affected parties (employees, customers, etc.) and there is no requirement for public reporting. As a result, there is no comprehensive data source on privacy breaches although there are several lists of breach incidents actively maintained on websites [1, 3].

Potential costs to an organization for a privacy breach reported in the mass media includes damage to reputation, loss of current/future customers, liability from other state's laws, and possible lawsuits from shareholders/customers. In the privacy breaches that have been disclosed, many were reported in the mass media first before being disclosed; thus leading one to infer that many privacy breaches required to be disclosed by law are not being disclosed unless forced to do so.[4]

No organization has been sued for not disclosing a privacy breach they were required by law to disclose. However, several organizations (particularly ChoicePoint) have been sued for negligence by parties affected by privacy breaches that were disclosed. This provides an additional economic incentive not to disclose privacy breaches.

Since there is not a standard format for disclosures, information that would be valuable for analysis is reported inconsistently and often not reported at all. In this paper, we have attempted to provide the best available view of disclosed privacy breaches by merging data from the two leading sources of privacy breaches: PrivacyRights.org [1] and Attrition.org [2]. The time period of analysis is between January 1, 2005 and June 5, 2006.

PrivacyRights.org has 182 privacy breach incidents for this

[3] Federal laws relevant to reporting storage security status include: Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA. For example, within Sarbanes-Oxley Law of 2002, Section 404 requires companies to document the effectiveness of internal controls/procedures and Section 409 requires real-time disclosure of information that changes the financial condition or operation of the company [4].

[4] For example, ChoicePoint first disclosed its 2005 breach only to California residents which had the first disclosure law in the nation and later disclosed to residents in other states and the District of Columbia, as new state laws were enacted.

Disclosure Statistics (3 significant digits)	Frequency of disclosures per month	Record Size per month	Record Size per incident
Mean	12.11	5.74M	589K
Standard deviation	5.68	14.9M	3.8M
95% Confidence Interval around Mean	9.48 – 14.74	0 – 12.6M	26.6K – 1.15M
Median	12	913K	20K
High	21	57.8M	40M
Low	2	42K	13

Table 1: Overview of statistical information.

period. For each report, this data source provides date of the incident, organization name, type of breach, and number of records lost. Attrition.org has information on 183 privacy breach incidents for this same period. For each entry, it lists the following information: date, organization name, type of business, specific information about the business, type of data, specific nature of data, whether a third party was involved in data handling and loss, total records lost, and a reference to the notification or news item related to the breach.

We have manually merged these two lists into a single data set containing 219 breach reports for the time period and then manually entered this data set into a database system. This database containing disclosed privacy breaches 2005-2006 upon which our analysis is based is available for query via the Internet at the following URL: *url blinded for WESII'06 peer review.* To our knowledge, this is the most comprehensive data set on disclosed privacy breaches and its availability will both validate the results we report in this paper as well as enable future work by other researchers.

4. ANALYSIS

In this section, we analyze the data obtained from the two data source, and represent the data in various graphical formats in order to communicate the essence of the data set we have assembled. Unless otherwise noted, all values are rounded to the nearest integer.

Table 1 shows an overview of the nature of the data we analyzed. It shows the mean, median, standard deviation, confidence interval, and high / low values for the number of breach incidents and total records lost per month and per incident, during the chosen time interval.

It is interesting to see the large standard deviations from Table 1. This is because the data set contains two breach incidents which were vastly larger than the others, making the record size statistics highly skewed. The difference between the average values and the high values for record sizes reflects this, resulting in the large standard deviation.

Disclosure Statistics (3 significant digits)	Record Size per incident
Mean	201K
Standard deviation	982.5K
95% Confidence Interval around Mean	55K – 347K
Median	19000
High	12M
Low	13

Table 2: Overview of statistical information excluding the two extreme values.

4.1 Type of Organizations

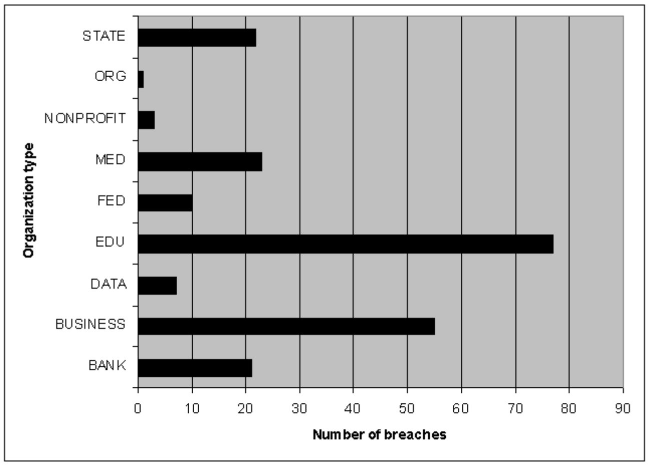

Figure 1: Reported privacy breach incidents by organization.

Fig. 1 and 2 show that educational institutions constituted the largest portion of reported security breaches. Out of 219 reported cases, we find that 35% of the cases were reported from educational institutions. Businesses accounted for 25% of reports, followed by Medical organizations (11%) , State organizations (10%), and banks (10%). Now, the large number of incidents from educational institutions can be explained in two ways: either the security considerations for records are not strict, or educational institutions are more likely to report breach incidents, even in absence of laws mandating breach reporting.

In Fig.4, we show the percentage of total records lost for each type of organization. While Fig. 1 shows that educational institutions reported the most breaches, they account for only 2% of total records lost. The largest number of records lost were from business institutions (35%), followed by federal agencies (30%).

4.2 Type of Data

Fig. 5 shows the types of data items lost through breaches. We categorized the type of records into the following categories: social security numbers (SSN), names and addresses (NAA), credit card numbers (CCN), medical records (MED),

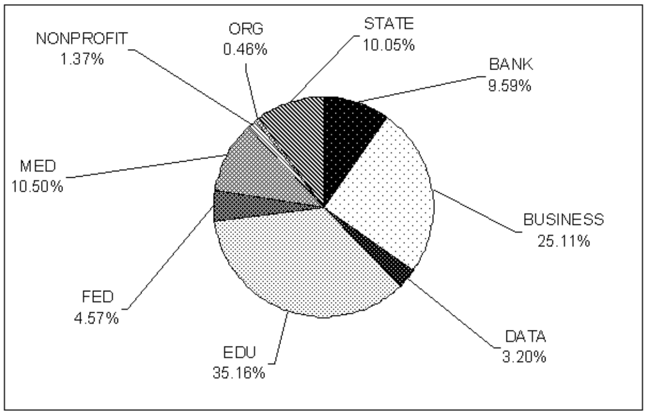

Figure 2: Breakdown of privacy breach incidents by organization.

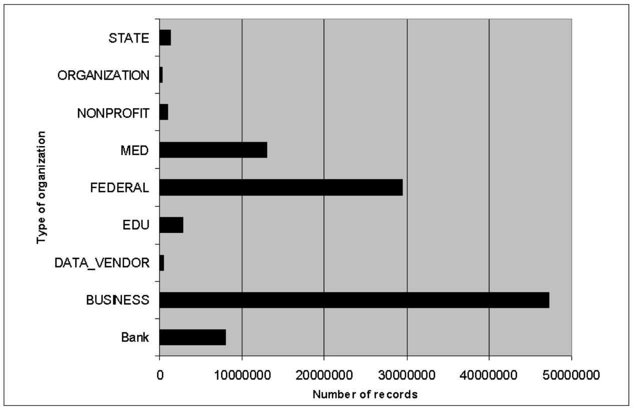

Figure 3: Reported privacy records lost by organizations.

account information (ACC), tax information (TAX), passwords (PASS), miscellaneous data (MISC), and unknown records (UNK).

From the figure, we can see that, social security numbers were by far the most common data stolen or lost. In 135 out of the 219 reported breaches (62%), SSN's were lost or stolen. This is understandable as social security numbers can be used effectively in various identity theft activities. The next most common type is name/address information, which amounted to 96 entries (44%). followed by credit card numbers, 15%, unknown record types, 11%, and account numbers 10%. Note that in many cases, more than one data types were among the lost/stolen records.

In Fig. 6, we look into the data type groups in the storage breach incidents. It shows that social security numbers, or a combination of social security numbers and name/address information are the most commonly lost data items during a storage breach incident. We also see that, in almost half of the incidents, there was only a single data type lost (49.5%). Similarly, 2 types of data records were lost in almost half of the cases (49.5%). There were only 2 cases where the data records included three or more types of data items.

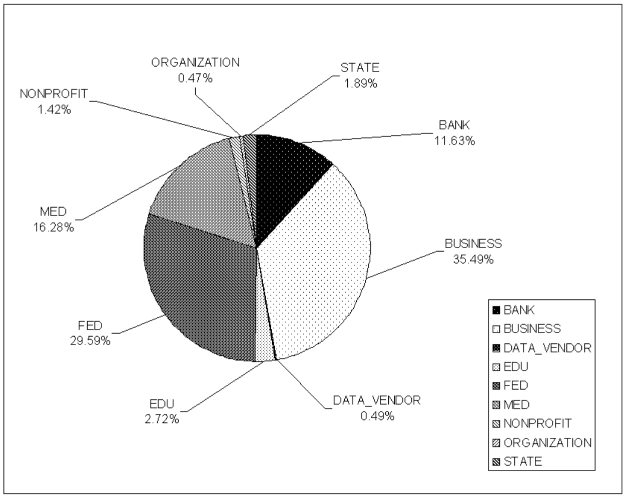

Figure 4: Reported privacy records lost by organization.

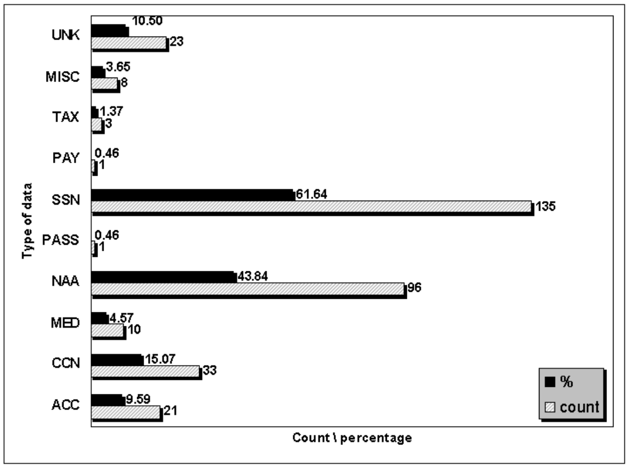

Figure 5: Reported Breaches by Data Type.

4.3 Type of breach

Fig. 7 shows the breakdown of different types of breaches. It shows that, 41% of the attacks occurred via external intrusion, implying a system breach or other type of malicious attack by external entities. The next most common type of breach was physical attack, covering 36% of total breaches. By this, we imply cases where loss ortheft of media (tapes, hard drives, portable drives) or hardware (laptops, computers) occurred. Out of these physical attacks, 73% happened due to theft or loss of laptops or desktops, while the rest of the 27% physical attacks happened due to loss of backup tapes. Interestingly, many of these physical losses were due to loss or theft of laptops or backup tapes, often from cars or employee residences. These could perhaps be easily prevented via strict security policies regarding transfer of data to laptops, not allowing data to be taken to employee residences, and mandatory encryption of all types of data in transit. Data breach due to mis-configuration covered 12% of total breaches; these are cases where the data records were

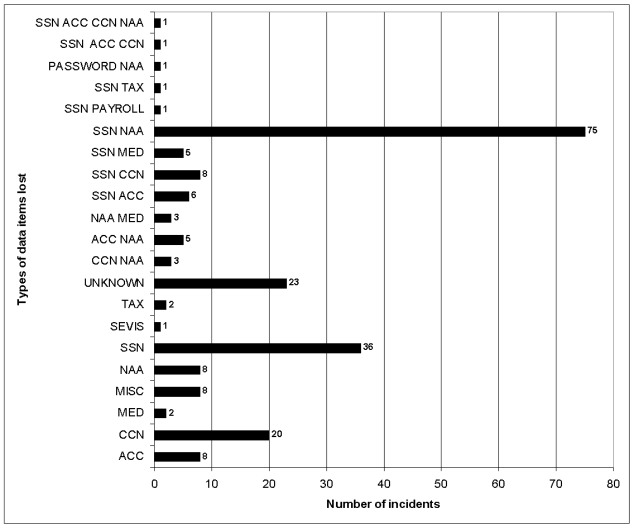

Figure 6: Breach incidents by groups of data items

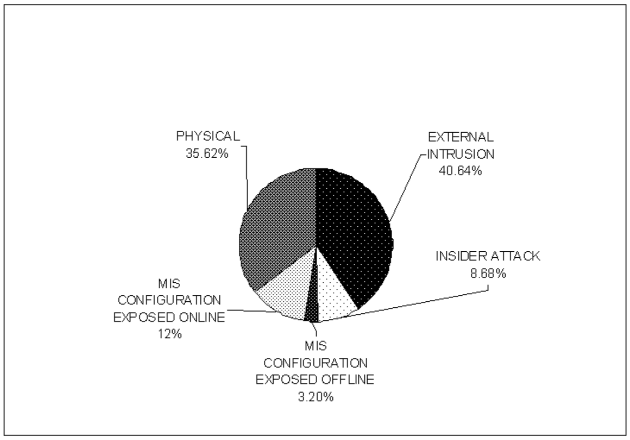

Figure 7: Type of breaches.

inadvertently exposed on the web or via email. Insider attacks by malicious insiders constitute 9% of the attacks, while accidental data loss via offline methods (e.g. SSN printed on mail labels) was the least of all – covering only 3% of total breaches.

4.4 Times of breach

Here, Fig. 8 shows the breakdown of number of reported breaches per month. Interestingly, the number of breaches per month shows a periodicity – with a peak attained in June 2005 followed by a fall in October 2005, before peaking again in February / March 2006. While there is no clear explanation for this, a possibility is the lapse in security during the end of the financial year.

Fig. 9 shows the percentage of number of records affected per month. The figure shows two spikes - one in June 2005, and the other in May 2006. The former refers to a breach of CardSystems, resulting in loss of 40 million credit card records. The latter is the recent breach of social security numbers and other information of the U.S. Department of Veterans Affairs. Fig. 10 shows corresponding spikes in average number of records lost per month on a log scale so months with non-spike events are more visible. It also shows that the average number of records/month is approximately 10^6.

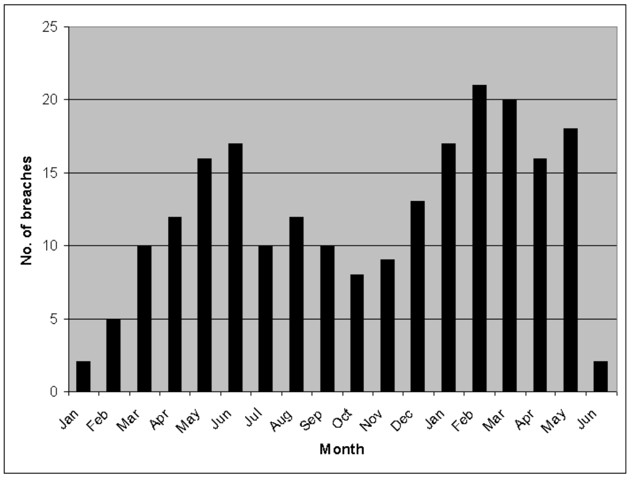

Figure 8: Breach incidents per month (Jan 2005-Jun 2006.

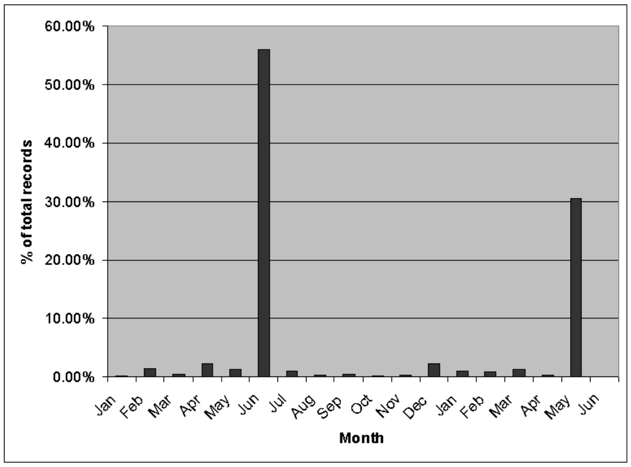

Figure 9: Percentage of records lost per month (Jan 2005-Jun 2006.

4.5 Breach Sizes

The appendix of this paper has four scatter diagrams to better understand sizes. Fig. 11 is a scatter diagram of record size lost by date and shows peak events in early summer and a continuous clustering at mid-levels throughout the year.

Fig. 14 is a scatter diagram of record size lost by breach type and clearly shows physical breaches have a higher tendency than external breaches. Inside attacks are widely distributed while offline/online exposure are sparsely clustered at mid-levels.

Fig. 12 is a scatter diagram of distribution of different categories of data types throughout the time period.

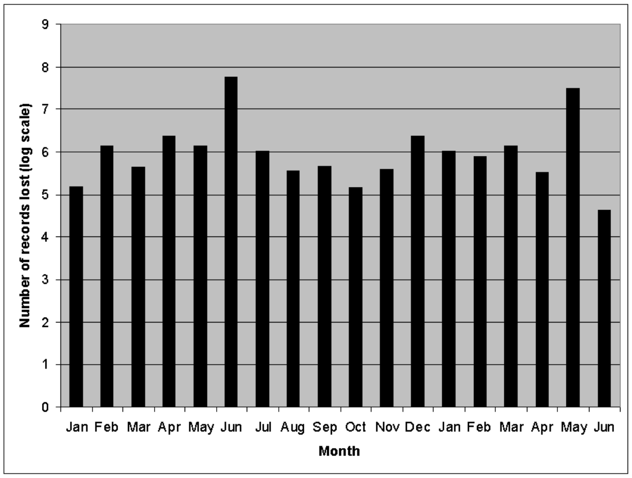

Figure 10: Number of records lost per month (log scale), Jan 2005-Jun 2006.

Fig. 15 is a scatter diagram of record size lost per organization type and clearly shows education and businesses similarly clustered with more events than other organizations although businesses has some high volume events with no counterparts in educational organizations.

4.6 Case Study Across Organizational Types

The appendix of this paper has four sets of figures to compare different characteristics of privacy breaches across the top four different organization types in terms of number of breaches: (1) educational, (2) businesses, (3) banks, and (4) medical institutions.

Figs. 17-20 show reported breaches over the period of study – while reported breaches for banks and medical institutions are relatively constant in volume, the reported breaches for education and businesses is more cyclical reflecting the nature of their operations.

Figs. 21-24 show reported records lost per month – businesses peak to lose the most records while education has a steady level on non-peak records lost (note Y-axis is not the same between education and business).

Figs. 25-28 show reported breaches by breach type – while banks and medical institutions are dominated by physical breaches, businesses are relatively balanced between physical and external intrusions, and education is dominated by external intrusions.

Figs. 29-32 show reported breaches per data type – while education and banks are dominated by SSN breaches, businesses are dominated by credit card breaches, and medical institutions are dominated by miscellaneous medical identifiers. It must be noted that the data type in this category is not mutually exclusive, multiple data types can be lost in a single breach. The breach data type may be the closest distinguishing characteristic for types of different organizations.

5. RELATED WORK

We are aware of only three related efforts to analyze privacy security breaches. First, in [15] the authors summarize selected privacy security incidents reported in the press since 2000. At present [15] is limited in its analysis due to the small set of incidents and biased sampling but the authors state the report will be updated regularly so time will show the value of this work.

In [15], it is claimed that *almost half of the security breaches occurred at institutions of higher education.* Fig.2 shows that, considering the number of breach incidents, educational institutions indeed are the most vulnerable to privacy breaches (with 35% of total breaches). However, this does not take into account the number of total records affected. Fig. 4 shows the fraction of total affected records to be the highest in case of business entities (35%), while educational institutions account for only 3%. This is because, typically, the number of records lost from an educational institutions is not as high as that from business entities. [15] also claims that, *In 2005, a stolen computer (desktop, laptop, or hard drive) was the cause of the security breach 20% of the time.* Our analysis in Fig. 7 shows that 36% of breaches were due to such thefts which is a consistent although not exact result.

Second, from the State Government of California, [6] recommends best practices for organizations responsible for protecting personal information including making breach notifications to individuals. In addition to recommendations, [6] also includes lessons learned from studying breach notifications in California.[5] It makes several claims based on experience of being the first state to have enacted a privacy breach disclosure law in 2003. The report suggests more precautions should be taken to prevent physical losses, the most prevalent form of privacy breach (53%) in California. As shown in Fig. 7, the nationwide average for physical privacy breach is 36%. Next, the report claims that in California, loss of social security numbers are the most common type of data breach at 85%). Fig. 5 shows the nationwide figure we report is 61.64%, distantly followed by credit card numbers (15%), name and address (10%), and account information (10%). Thus our results are similar to both findings from the State of California.

Third, [7] studies the impact of privacy breaches on stock market valuation. The events used in [7] are limited to those affecting publicly traded firms and include different types of security incidents not limited to privacy breach disclosures.[6] While firms are an important part, they are still only part of the overall security breach picture. By excluding non-profit organizations (e.g. universities, hospitals, etc) and government agencies, and focusing on many different types of security events (not just privacy breaches), the data analysis in [7] cannot be compared directly to our work which focuses exclusively on privacy breaches across all organizations.

6. SUMMARY

There is in progress a multi-level response to the privacy breaches reported in the mass media. At the national level, the U.S. Office of Management and Budget has issued recent security directives that all Federal agencies encrypt classi-

[5] Of course this analysis is limited to the unique environment within the State of California although many/most of the businesses in question with privacy breach disclosures have national presence.

[6] the [7] source data includes websites, mailing lists, news feeds, and blogs and was not made publicly available.

fied/sensitive data on a laptop (or other handheld device), implement two-factor authentication for all remote data access, require remote or wireless users to re-authenticate after 30 minutes of inactivity, and the reporting of privacy breaches within one hour.[10] At the State level, U.S. states are either enacting a new law where there was no law previously or amending current laws with a variety of special requirements. Lastly organizations are now labeling data and protecting it with security solutions increasingly similar to classified environments.

While personal data on networked devices will always be subject to some risk, with investment the level of risk can be managed. This work is only a start to preventing and mitigating privacy breaches by analyzing and thus better understanding the demonstrated risks in the current environment January 2005 – June 2006. Recommending the type and level security solutions should have direct relationship to potential threats (threat modeling), probability of event occurrence (empirical event data analysis), potential event impact (empirical event data analysis) along with the tradeoffs and risk posture unique to different organizational environments. To do otherwise invites disaster in that chosen security solutions may not match the actual threats resulting in wasted investment, performance degradation, service denial, civil/criminal liability, and continued data compromise. We have carefully restrained ourselves from recommending security solutions since that is a next study to build upon this empirical event analysis.

Acknowledgments

We acknowledge special insights on privacy breaches from (in alphabetical order): Arshad Noor (StrongAuth, Inc.), Umash Prasad (State of California Criminal Justice Statistics Center - Special Requests Unit) and Prof. Marianne Winslett (UIUC). We anticipate the constructive criticism of anonymous WESII'06 reviewers which we plan to incorporate to improve this paper.

7. REFERENCES

[1] A chronology of data breaches reported since the choicepoint incident (list). *Privacy Rights Clearinghouse* http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[2] Dataloss mailing list. *Attrition.org* http://attrition.org/security/dataloss.html.

[3] Entities that suffered large personal data incidents (list). *Attrition.org* http://attrition.org/errata/dataloss.

[4] Sarbanes-Oxley Act of 2002. *U.S. Securities and Exchange Commission*, http://www.sarbanes-oxley-forum.com.

[5] 2006 identity fraud survey report. *Better Business Bureau/Javelin National Survey*, http://www.javelinstrategy.com/research, 2006.

[6] Recommended practices on notice of security breach involving personal information. *State of California Department of Consumer Affairs/Office of Privacy Protection*, April 2006.

[7] A. Acquisti, A. Friedman, and R. Telang. Is there a cost to privacy breaches? an event study. In *Workshop on the Economics of Information Security (WEIS)*, 2006.

[8] W. J. Clinton. Presidential Decision Directive/NSC-63 (PDD-63). May 22, 1998.

[9] C. Conkey. Identity theft: Shielding yourself. July 14, 2006.

[10] L. Greenemeier. After a lucky break with va laptop, feds tighten up. *InformationWeek*, July 3, 2006.

[11] R. Hasan, S. Myagmar, A. J. Lee, and W. Yurcik. Toward a threat model for storage systems. In *ACM International Workshop on Storage Security and Survivability (StorageSS)*, pages 94–102, 2005.

[12] M. Hines. Data losses may spark lawsuits. In *eWeek*, June 12, 2006.

[13] P. Mueller. How to survive data breach laws. *Network Computing*, June 8, 2006.

[14] B. Schneier. Risks of third-party data. *Communications of the ACM*, May 2005.

[15] R. Tehan. Personal Data Security Breaches: Context and Incident Summaries. In *Congressional Research Service Report for Congress*, December 16, 2005.

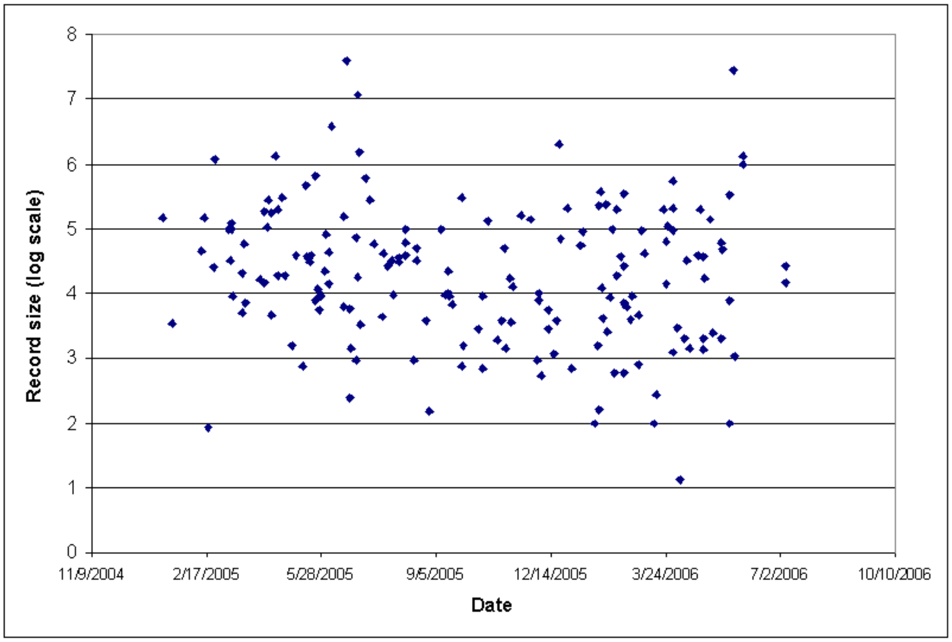

Figure 11: Scatter diagram for number of records lost by date.

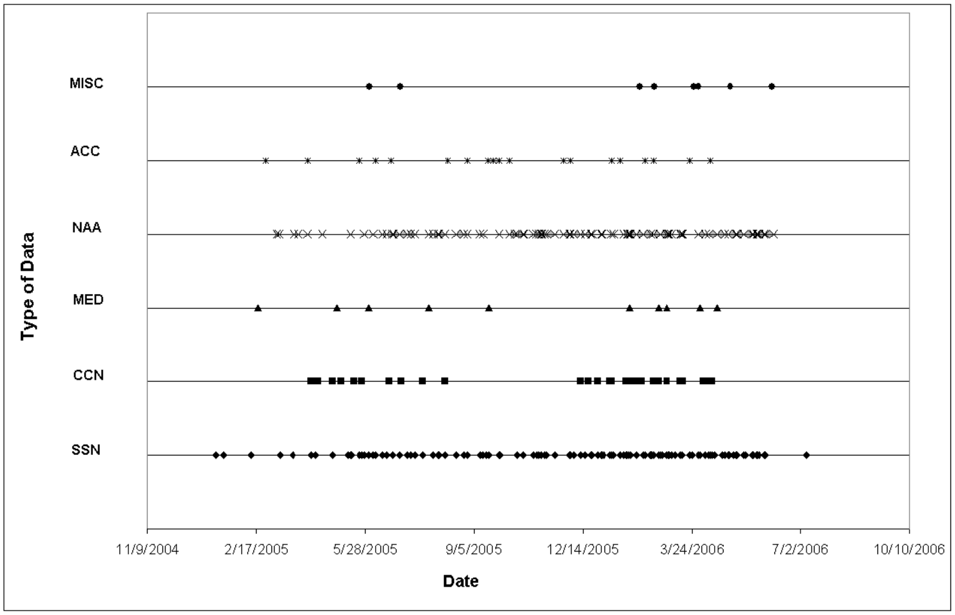

Figure 12: Scatter diagram for data types lost by date.

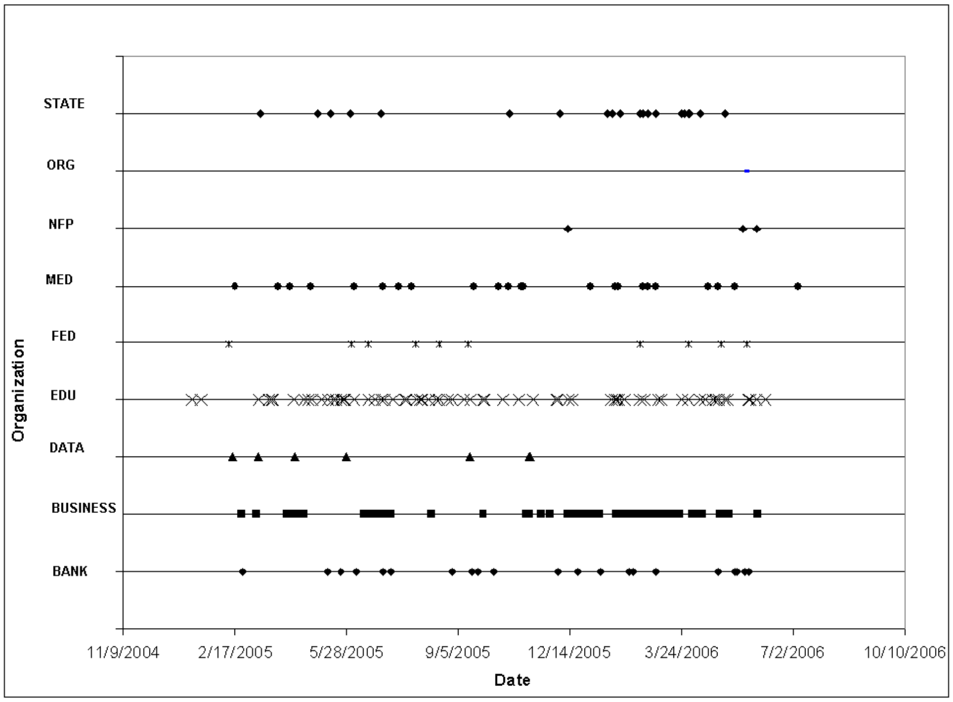

Figure 13: Scatter diagram for data loss in organizations by date.

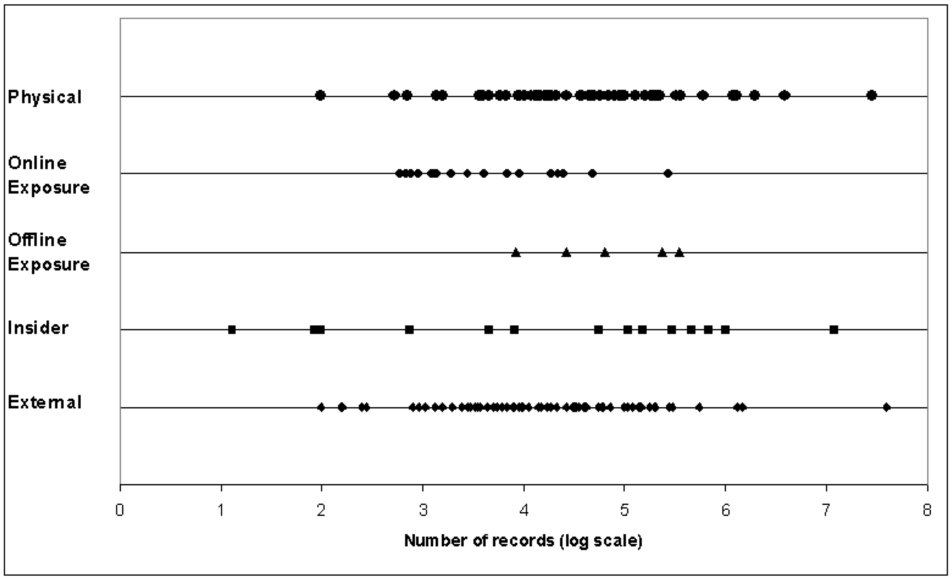

Figure 14: Scatter diagram for number of records lost by breach types.

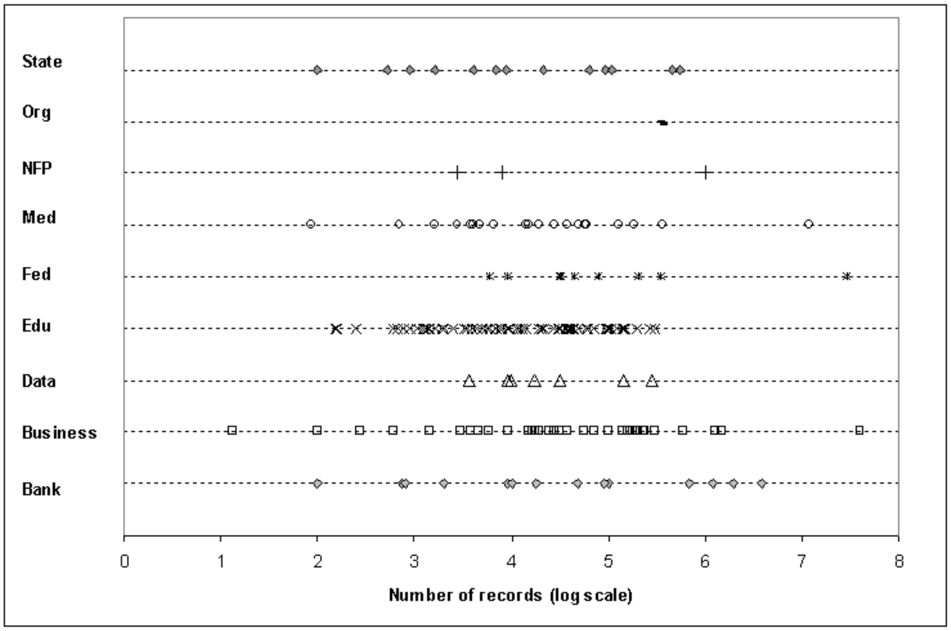

Figure 15: Scatter diagram for number of records lost by organization type.

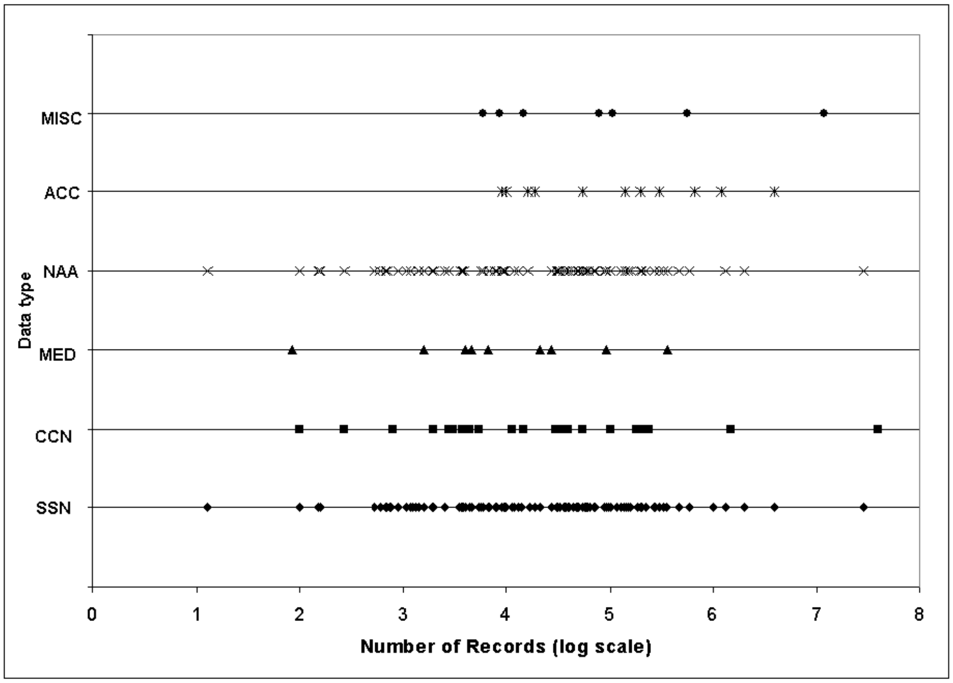

Figure 16: Scatter diagram for number of records lost by data type.

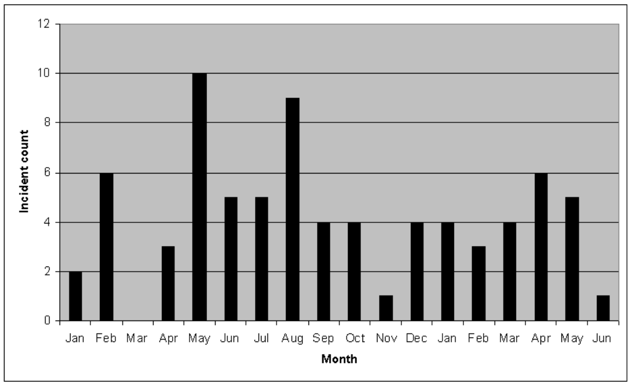

Figure 17: Reported breaches per month: Educational institutions.

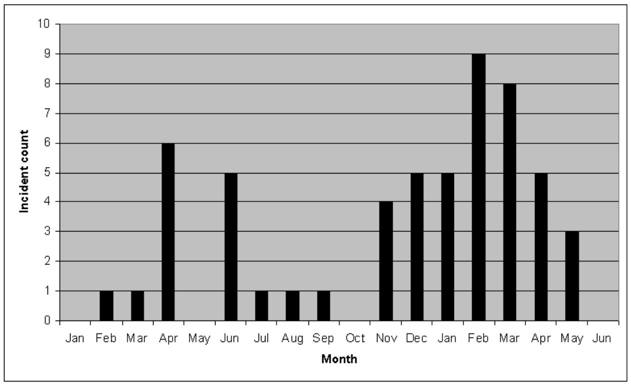

Figure 18: Reported breaches per month: business institutions

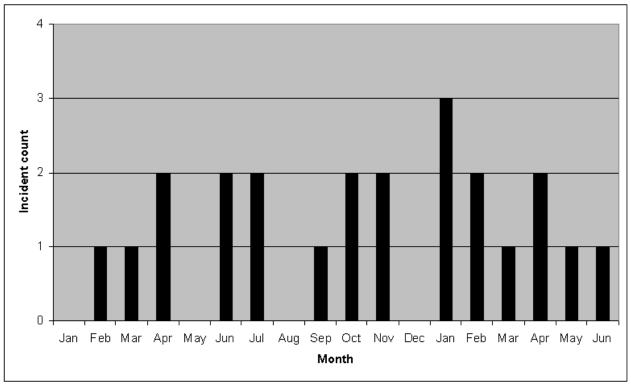

Figure 19: Reported breaches per month: banks

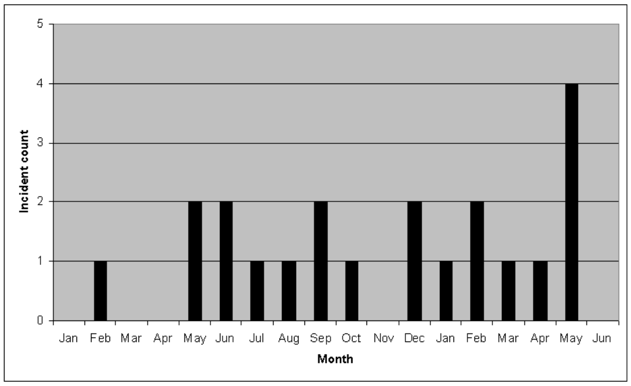

Figure 20: Reported breaches per month: medical institutions

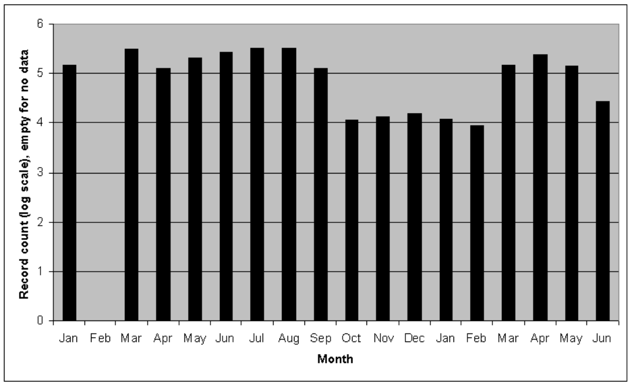

Figure 21: Reported records lost per month: Educational institutions.

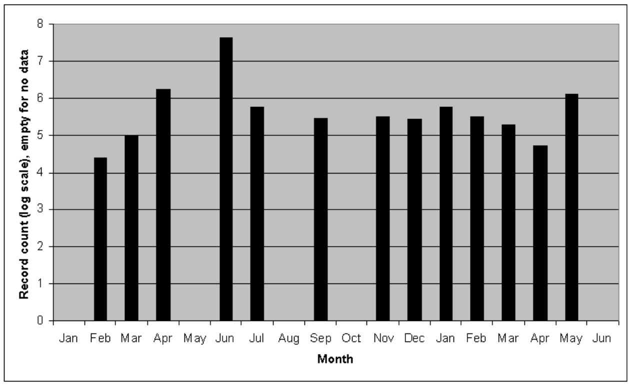

Figure 22: Reported records lost per month: business institutions

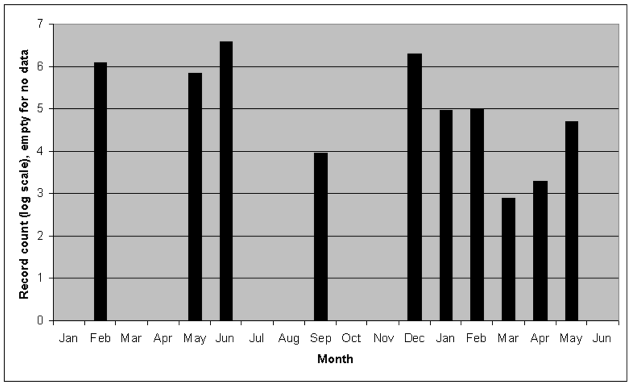

Figure 23: Reported records lost per month: banks

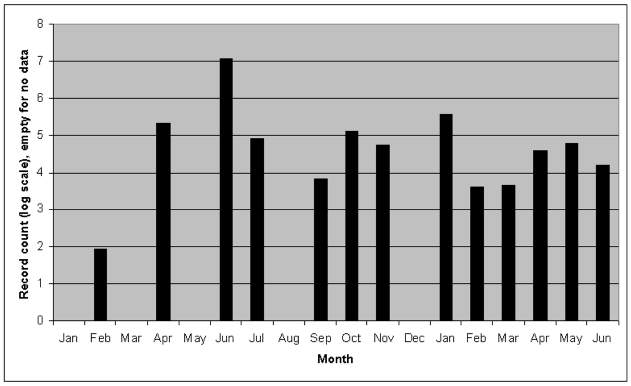

Figure 24: Reported records lost per month: medical institutions

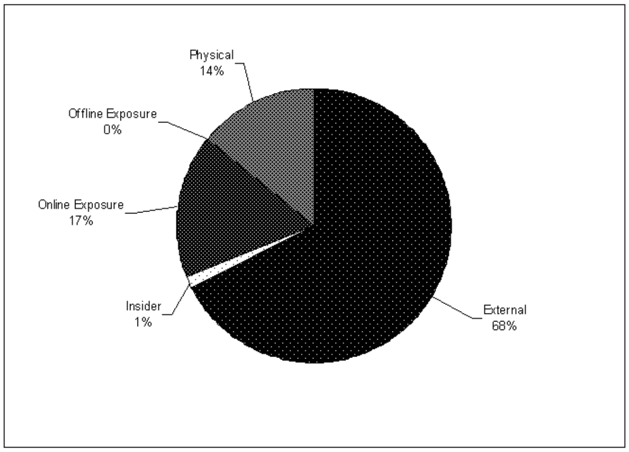

Figure 25: Reported breaches by breach type: educational institutions.

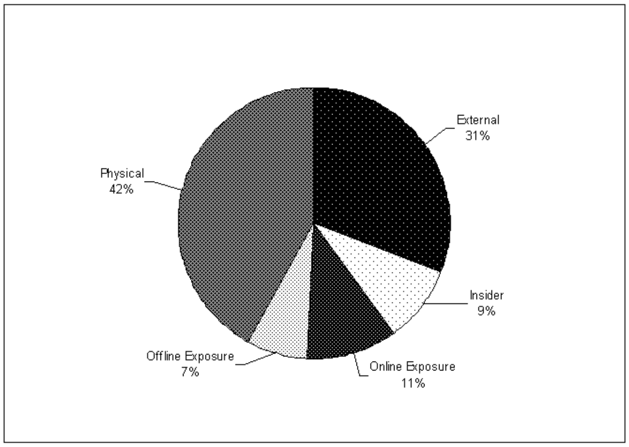

Figure 26: Reported breaches by breach type: business institutions

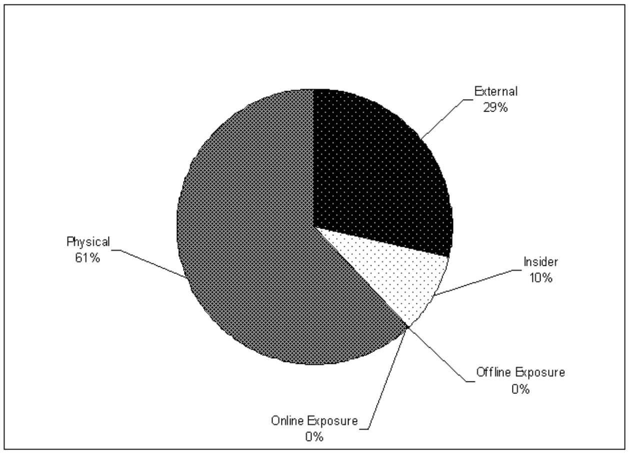

Figure 27: Reported breaches by breach type: banks

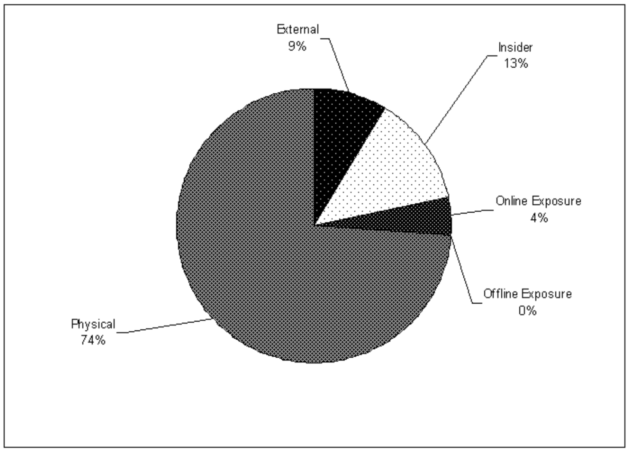

Figure 28: Reported breaches by breach type: medical institutions

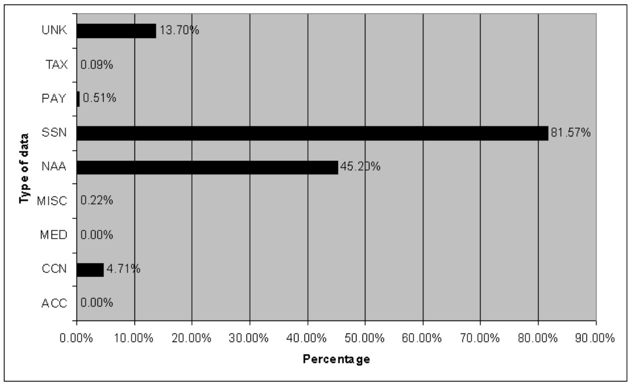

Figure 29: Reported breaches by data type: Educational institutions.

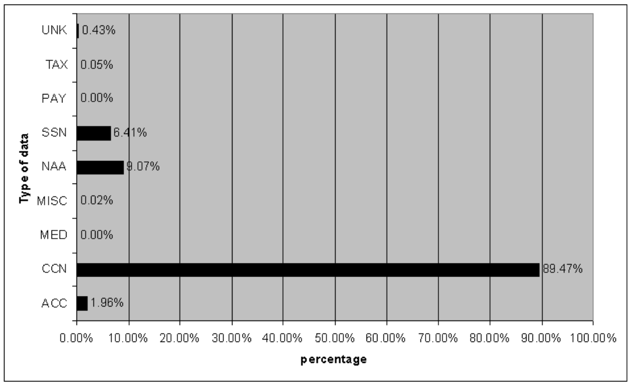

Figure 30: Reported breaches by data type: business institutions

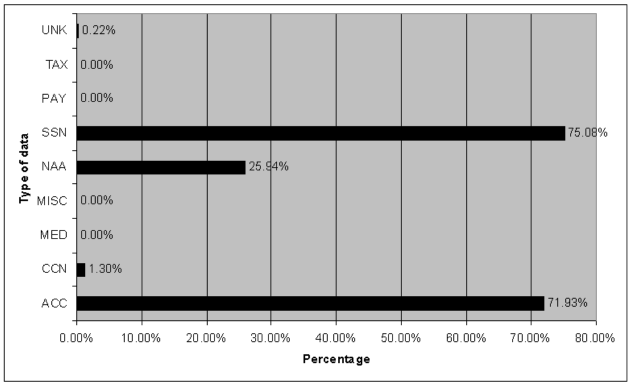

Figure 31: Reported breaches by data type: banks

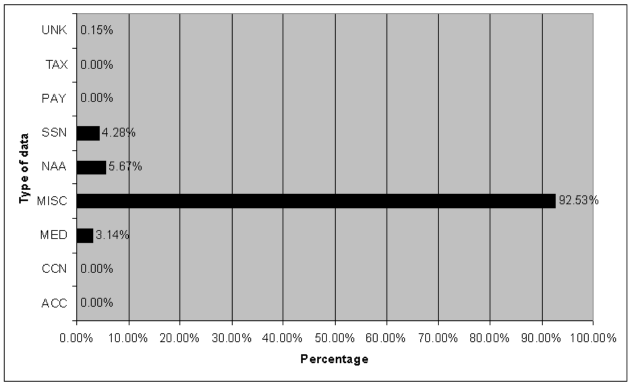

Figure 32: Reported breaches by data type: medical institutions

States	**Start Date**	**State Law**	**Responsible Party**	**Likelihood of Harm Threshold**	**Best Practices Required**
(1) California	07/01/03	SB 1386	entities conducting business, separate section for state agencies	no	yes
(2) Arkansas	03/31/05	SB 1167	entities conducting business	yes	yes
(3) Georgia	05/06/05	SB 230	data brokers only, excludes state agencies	no	no
(4) North Dakota	06/01/05	SB 2251	entities conducting business	no	no
(5) Delaware	06/28/05	HB 116	entities conducting business	no	no
(6) Florida	07/01/05	HB 481	entities conducting business	yes	no
(6) Tennessee	07/01/05	HB 2170	"information holder" including people, business, or state agency	yes	no
(8) Washington	07/24/05	SB 6043	any person or business, plus state agencies	yes	no
(9) Texas	09/01/05	SB 122	a person that conducts business	no	yes
(10) Nevada	12/01/05	SB 347	data collectors, including all entities and state agencies	yes	yes
(10) North Carolina	12/01/05	SB 1048	any person or state agency	no	no
(12) New York	12/08/05	SB 5827	any person or business	no	no
(13) Connecticut	01/01/06	SB 650	any person that conducts business	yes	no
(13) Illinois	01/01/06	HB 1633	data collectors, including all entities and state agencies	no	no
(13) Louisiana	01/01/06	SB 205	any person or agency	yes	no
(13) Minnesota	01/01/06	HF 2121	entities conducting business, section for state agencies	no	no
(13) New Jersey	01/01/06	A4001	a business or public entity	yes	yes
(18) Maine	01/31/06	LD 1671	data brokers only, excludes state agencies	no	no
(19) Ohio	02/15/06	HB 104	any person or state agency	yes	no
(20) Montana	03/01/06	HB 732	entities conducting business, plus special requirements for insurers	yes	yes
(20) Rhode Island	03/01/06	HB 6191	any state agency or person, including all businesses]	yes	yes
(22) Wisconsin	03/31/06	SB 164	entities conducting business	no	no
(23) Oklahoma	06/08/06	HB 2357	only state entities	no	no
(24) Indiana	06/30/06	503	person or government agency	no	no
(24) Pennsylvania	06/30/06	SB 712	any entity	yes	no
(26) Idaho	07/01/06	28-51-104	entities conducting business	yes	no
(27) Nebraska	07/13/06	LB 876	entities conducting business	yes	no
(28) Colorado	09/01/06	6-1-7161a	entities conducting business	yes	no
(29) Arizona	12/31/06	SB 1338	entities conducting business	yes	yes
(30) Hawaii	01/01/07	SB 2290	entities conducting business	no	no
(30) Kansas	01/01/07	SB 196	entities conducting business	yes	no
(30) New Hampshire	01/01/07	HB 1660	entities conducting business	yes	no
(30) Utah	01/01/07	SB 69	entities conducting business	yes	no
(30) Vermont	01/01/07	SB 284	entities conducting business	no	no

Table 3: Summary of State Laws for Privacy Breach Disclosures adapted from: (1) "State Laws Governing Security Breach Notification", Crowell Moring LLP, 01/25/06. http://www.crowell.com/; (2) "Security Breach Notice Legislation: Effective Dates, and Security Breach Notification Chart," Perkins Cole Attorneys Al Gidari, Barry Reingold, and Matt Staples; and (3) "Notice of Security Breach State Laws," Consumer Union, June 27, 2006.