

# A Framework for the Evaluation of State Breach Reporting Laws

Benjamin J. Brooker, Jonathan Crawford, and Barry M. Horowitz

**Abstract**—This paper develops a framework for evaluating the effectiveness of cyber security breach reporting laws across states. In doing so, trends and correlations in state reporting along with other relevant factors are identified using readily available data. This paper addresses two critical questions in the assessment of breach reporting legislation: 1) How does the rate of reporting security breaches across states compare with the rate of reporting of security threats to computer operating systems?, and 2) What factors other than the implementation of breach reporting legislation effect the rate of reporting security breaches across states? The framework developed in this paper can be applied in future analyses to evaluate the effectiveness of breach reporting legislation and can assist in pinpointing legislative weaknesses across states.

Limitations in the availability of data inspired the generation of a number of recommendations for the improvement of breach reporting law evaluation. First, more time is needed to collect data, as most laws have been in place for two or fewer years. Second, each state should have a central database that records all reported cyber security breaches. This will allow for greater visibility to the public and would make for greater accessibility of data for both consumers and researchers. Finally, further research efforts should be conducted on the topic of OS security vulnerability patch rates and their relevance to the actual, realized cyber threat level of operating systems.

## I. INTRODUCTION

WITH the growth of the e-commerce sector and companies' growing utilization of the Internet and digitized data over the past twenty years, cyber security has garnered much attention in today's economy. While new technologies have led to a more interconnected global economy and a number of positive advancements, such as faster communication, greater competition, and lower prices, they also pose an entirely new form of risk to companies and consumers. A wide variety of cyber-based

crime opportunities over the past two decades have resulted in an evolution of various types of cyber attacks that are being used to disrupt businesses, corrupt data, steal personal information, and cause other kinds of business problems that ultimately result in economic losses to individual business and the national economies as a whole [2]. Among those attacks are denial of service attacks, viruses, and worms, which typically cause short-lived disruptions with short-lived consequences; and attacks that could result in longer lasting consequences, such as loss of reputation, loss of intellectual property, legal liability, or long, substantial Internet infrastructure outages [2].

Even with the introduction of these new forms of risk, efficient cyber security budgeting within companies and government agencies is not assured. The inefficient allocation of cyber security dollars can be attributed to three facts: 1) Regulatory legislation on cyber security is relatively new, vague, and yet to be proven effective, 2) There is yet to be a large-scale catalytic event that has demanded greater attention and concern for cyber security, and 3) There still exists a knowledge gap between executive business decision makers and IT decision makers in corporations. Because the probability of a large-scale cyber event is unpredictable, and the closure of the knowledge gap requires a gradual, long-term analysis, this paper focuses on the range of short-term effects of regulatory legislation on cyber security trends.

The idea of cyber security regulation is relatively new. Until 2003, there was no federal or state legislation in place that specifically required a company to report a disclosure of private information; however, to date there are 34 states along with the District of Columbia that have some form of cyber breach notification legislation [3]. Prior to the first breach reporting legislation, the federal government had passed laws such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Sarbanes-Oxley Act. These acts do not create specific cyber breach notification requirements, but instead give the authority to create them [5].

The recent trend of state cyber breach notification laws can essentially be attributed to two main events. First, in July of 2003 California became the first state to enact legislation that required companies operating within the state to report any compromise of private information to affected parties [3]. Second, the ChoicePoint incident in February of 2005, showed that the impacts of cyber security

Manuscript received April 9, 2007. This work was supported in part under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this paper are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

Ben Brooker (e-mail: bjb2v@virginia.edu) is a student in the Department of Systems & Information Engineering at the University of Virginia, Charlottesville, VA 22904 USA.

J. Crawford (e-mail: jac2bp@virginia.edu) is a graduate research assistant in Systems & Information Engineering at the University of Virginia, Charlottesville, VA 22904 USA.

B. Horowitz (e-mail: bh8e@virginia.edu) is a Professor of Systems & Information Engineering at the University of Virginia, Charlottesville, VA 22904 USA.

breaches can be large for the company involved. The company announced that it had unwittingly sold the personal information of at least 145,000 Americans to identity thieves in 2004 [6]. Because of this incident, ChoicePoint has incurred significant financial losses from legal and professional fees, victim notification costs, heightened cyber security investments, and damaged reputation [6]. As a result, states began enacting security breach notification legislation, and 34 states, along with the District of Columbia, currently have some form of law in place [3].

The primary purpose of these breach reporting laws is to hold companies and government agencies accountable for improper and inefficient investments in cyber security protection and to help protect and inform the public. The laws impact a company's reputation in a manner it hasn't been before, and the change in breach reporting requirements offers an important byproduct: visibility to the press [7]. Given that the press has interest in reporting on cyber breaches, this will inherently give visibility to the public [7].

Ideally, breach reporting laws will create a bridge between cyber breach incidents and the people that they impact; however, there are two factors that can prevent this connection. First, companies may be more inclined to withhold information on security breaches rather than increase cyber security investment to avoid negative effects on reputation. Second, the media may not be interested in reporting publicized security breaches if the stories do not attract readers. This paper recognizes both factors, but primarily focuses on the media component of cyber security breach reporting laws.

The goal of this paper is to develop a method for evaluating the effectiveness of cyber security breach reporting laws across states. In doing so, trends and correlations in state reporting along with other relevant factors are identified, and two critical questions are made with respect to the assessment of breach reporting legislation: 1) How does the rate reporting security breaches across states compare with the rate of reporting of security threats to computer operating systems?, and 2) What factors other than the implementation of breach reporting legislation affect the rate of reporting security breaches across states? The methodology used in this paper can be applied in future analyses to evaluate the effectiveness of breach reporting legislation and can assist in pinpointing legislative weaknesses across states.

## II. METHODOLOGY

Here we introduce a basic framework that can be used in the assessment of the effectiveness of cyber security breach reporting legislation. The framework consists of two main analyses: 1) A correlation analysis to uncover any factors

that may attribute to the rate of breach reporting across states, and 2) A rate comparison analysis that compares the rates of breach reporting to the rate of software companies developing various operating system security patches (in response to identified exploitation possibilities). The results of the analyses are then given multiple interpretations and conclusions are drawn.

Before going into further detail about the analyses conducted, a number of terms must be defined. First, a breach is defined to be an event in which computerized personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A publicized breach is a breach that is made public by reporting to consumer reporting agencies, law enforcement, the media, or directly to the individuals affected. Personal information is defined as the first name or initial and last name of an individual, with one or more of the following: 1) Social Security Number, 2) driver's license number, 3) credit card or debit card number, or 4) a financial account number with information such as PINs, passwords or authorization codes that could gain access to the account [8]. In the context of this paper, a breach reporting law is defined as a state law that requires handlers of personal information to notify all affected parties in the event of a breach that compromises the parties' personal information. Finally, in the rate comparison analysis, the term threat is used rather than vulnerability when describing security patches. The assumption is made that only critical or high level vulnerabilities are true threats that can lead to a breach of security for companies and government agencies, so they are the only patches included in the counts.

Prior to conducting the analyses, data pertinent to cyber security breach reporting legislation had to be collected and the accessibility and availability of data had to be determined. As there is no central, federal or state-sponsored database of reported security breaches, third-party reporting sites had to be used to gain an estimate of the true rate of breach reporting across states. PrivacyRightsClearinghouse.org and Attrition.org are third-party sites committed to informing consumers of publicized cyber security breaches and offer an extensive list of news reports from the last three years [1],[4]. To conduct the correlation analysis, state statistics and information were taken from the Census Bureau [9]. Then to conduct the rate comparison analysis, the vulnerability patch rates of various operating systems were taken from the National Vulnerability Database [10].

This framework for effectiveness evaluation offers three important views of the current state of cyber security breach reporting. First, a simple state-by-state count of publicized security breaches is made to offer a very general, macro view of breach reporting. Next, the correlation analysis aims to identify any factors that may attribute to different

rates of reporting across states. The number of publicized breaches is compared to factors such as the existence of a law in a state, the population of a state, the number of businesses in a state, and the newspaper distribution in a state. Finally, the rate comparison analysis offers a view of how breach reporting and corporate responsibility compare to the hacking threat posed to the most used operating systems. If there are major disparities in rates, hypotheses can be made about how companies are acting with respect to the actual level of risk in their cyber security systems.

### III. RESULTS

#### A. Breach Count

The analysis begins with a simple count of the number of breaches reported in 2005 and 2006. In 2005 there were a total of 143 reported cyber security breaches in the United States, and 46% of states had some form of cyber security breach reporting legislation. As shown in Table 2 and Figure 1, nearly half of the publicized breaches involved colleges and universities, with financial institutions, state agencies, federal agencies, and medical institutions also having high counts. When a state-by-state view is taken of the breach counts, California dominated other states with approximately 23% of the total breaches reported (see Table 1). Along with California, Ohio, Georgia, New York, Colorado, Texas, North Carolina, Michigan, Iowa, Massachusetts, and Washington D.C. accounted for 70% of the total breaches reported. Out of the 143 reported security breaches, 72% were reported in states that had enacted cyber security breach reporting legislation.

The next year in 2006, there were a total of 319 reported cyber security breaches, an increase of 123% from 2005, and 60% of states had enacted some form of legislation. As shown in Table 4 and Figure 2, colleges and universities still saw the greatest percentage of publicized breaches; however, the growth rate of reported breaches in state agencies, federal agencies, financial institutions, and medical institutions was greater than that of colleges and universities. When a state-by-state view is taken of the breach counts, California breaches accounted for the greatest percentage of any state with 13.5% of the total publicized breaches (see Table 3). The reported breaches were more evenly spread out among states in 2006, with the top 11 states only accounting for 60% of total breaches. North Carolina, Iowa, Michigan, and Massachusetts dropped out of the top ten, and Virginia, Washington, Florida, and Illinois entered with significant increases from the prior year.

Across the fifty states and the District of Columbia, 41 states saw an increase in the number of publicized security breaches from 2005 to 2006, six states saw no change in the number of breaches, and only Georgia, Nevada, Hawaii, and Missouri saw a decrease. There were 23 states that had

legislation in place prior to 2006, and 19 of them saw an increase in the number of reported cyber breaches from 2005 to 2006. Eight states enacted breach reporting legislation in 2006, and the total number of reports among them doubled from 2005 to 2006. Of the eight states, all saw an increase in breach reports with the exception of Idaho, which remained at one breach. The 20 states, including the District of Columbia, which had no breach reporting laws in place prior to 2007, saw the greatest percentage increase. Fifteen of the states saw an increase in reports from 2005 to 2006, and the total number of reports among them increased nearly 300%.

For the purposes of this paper, disclosures of personal information can be divided into two categories: 1) Disclosures involving breaches of data by hackers outside of the organization, and 2) Disclosures involving breaches of data by insiders, lost computers and hardware, and stolen computers and hardware. In 2005, only 34% of reported breaches were of the first category, and of those reported breaches, 80% were reported by colleges and universities (see Table 5). An increase in the number of hacker reports was seen in 2006, but the number of hacker reports as a percentage of the total number of cyber reports decreased to just below 19% (see Table 6). This is potentially a positive finding, as a rise in the effectiveness of cyber security applications could be attributing to the slower rate of increase of reports. However, this could also be discouraging if the slower rate is due to company's withholding information on hacker attacks.

Before any assumptions can be made, an analysis must be conducted to uncover any factors that may contribute to a state's level of cyber security breach reports. For example, one would not want to automatically assume that California has more cyber security breach problems than Iowa because it has eleven times as many reported breaches. There are other factors, such as state population, the number of businesses within a state, and state newspaper distribution that could affect the number of breaches reported. Next, a correlation analysis will be presented in an effort to uncover these factors.

#### B. Correlation Analysis

To conduct the correlation analysis, a number of state statistics were taken from the Census Bureau. Other quantitative and qualitative variables could be used in future analyses, but the variables used in this thesis report are state population, state median income, state newspaper distribution, total number of firms within a state, and the existence of a breach reporting law within a state. Factors were considered strongly correlated when the correlation was greater than or equal to 0.8.

The results of the correlation analyses for 2005 and 2006 are given in Table 7. In 2005, there were strong

correlations between state population and the number of reported breaches (.82), and the number of firms and the number of reported breaches (.83). This is not surprising, as it seems logical that a greater population would lead to a greater number of businesses, which would lead to a more opportunities to experience a cyber breach. The existence of a breach reporting law did not have a significant correlation (.31) with the number of breaches.

In 2006, there was an even greater correlation between state population and the number of reported breaches (.86), and the number of firms within a state and the number of reported breaches (.87). Also, there was a significant correlation between the number of newspapers in circulation and the number of reported breaches (.85). This is a logical finding, as one would assume that state population would be positively correlated to the number of newspapers in distribution. As in 2005, there was no correlation between the existence of a breach reporting law and the number of reported breaches in a state (.21).

To take a closer look at the lack of correlation between the existence of a breach reporting law and the number of reported breaches in a state, the details of individual laws had to be examined. One factor that could be an important disparity between laws is the requirement of a company to notify a consumer reporting agency when a breach of security occurs, rather than just the affected parties. However, when analyzed, no correlation was found between requiring notification to consumer reporting agencies and the number of reported breaches in a state (.21). In fact, only 36% of the total attacks reported were from states that required a consumer reporting agency notification. This does not, however, indicate that the requirement of a company or government agency to report to a central body is of no value. This requirement would at least offer more visibility to the public and more accessibility of data to researchers, specifically if a public database of reported breaches was created.

Thus far, we have shown how simple correlation analyses can be used to make inferences about the effectiveness of breach reporting laws. We have not, however, developed a framework to evaluate the performance of companies with respect to state breach reporting laws. The next section details how cyber security breach reporting rates and operating system vulnerability patch rates can be analyzed to infer how effective companies' cyber security applications are at protecting their information.

### *C. Rate Comparison Analysis*

To conduct this analysis, the overall count of reported cyber security breaches was taken and divided according to industry, as seen in Tables 2 and 4. Then, because we are only analyzing threat patch rates, we are only concerned with reports that involve breaches of security by hackers

outside of the company or government agency. Thus, we offer counts of only these breaches in Tables 5 and 6. We then compare these rates to the rates of security threat patch rates for various operating systems predominantly used by the given industries, which are taken from the National Vulnerability Database. The counts of security threat patches were only of patches of "critical" or "high" severity, as we made the assumption that highly severe threats would be of greatest concern to companies and government agencies.

There were two main limitations faced when collecting data for this analysis. First, because the breach reporting laws are still in their formative years, there is limited data on outside hacker breach reports. This means that the breach reporting rates may be subject to high uncertainty. Second, the rate of security threat patches is not a proven, precise representation of the actual cyber threat posed to companies and government agencies. However, there is no precise way to realize the actual level of cyber threat in a network, and, as explained in our methodology, we believe that the patch data is sufficient for the developmental stages of an evaluation framework. Due to these limitations, we will simply offer an example scenario of how this data could be used. If one were to have access to information on the actual usage of operating systems within an industry, they could apply the data to this framework to gain a better understanding of how industry reporting and actual threat rates compare.

For illustrative purposes, we analyze colleges and universities. From 2005 to 2006, colleges and universities saw outside hacker breach reports drop from 39 to 27, a decrease of 31%. If one were to assume that educational institutions predominantly use a Microsoft operating system, we would see from the National Vulnerability Database data that the OS saw an increase of 32% (71 to 94) in critical patches from 2005 to 2006. Although this is not all-telling, one could make a number of inferences from this information. One possible explanation for the difference in rates is that cyber threats are being patched in a timelier manner across all universities and colleges, translating into better cyber protection for users of their services. Alternatively, however, educational institutions could be withholding breach information or reporting hacker breaches as another category of cyber breach, as reporting one may have more negative repercussions than reporting the other.

A second, similar example can be made of the finance industry. From 2005 to 2006, financial institutions saw a 400% increase of outside hacker breach reports from one to five. One could make the assumption that the UNIX is the predominantly used operating system in the industry, in which case we would see no change in vulnerability patches as the National Vulnerability Database reports one patch for

both 2005 and 2006. Again, this data is not all-telling, but a number of hypotheses could be formed. One possible explanation for the rate disparities is that financial institutions are not patching in a timely manner and multiple institutions are being affected by the same vulnerability. Another possibility is that, because state breach reporting laws have existed for such a short period of time, companies are just beginning to adjust to legislative compliance. Before any conclusions can be made, one must have an understanding of what is at stake and what the rationale is for educational institutions to report or withhold information on cyber security breaches.

#### IV. CONCLUSION

The results presented in this paper are to be interpreted only as a guideline for the further development of a framework for breach reporting law evaluation. Because cyber security breach reporting legislation is still in its formative stages and because the relevant data is disorganized and incomplete, a reliable set of conclusions cannot be reached. Although, after conducting the analyses, we will offer a number of recommendations that will aid future research on the topic and offer more visible, accurate information for consumers and researchers.

The first recommendation for the improvement of this proposed framework is time. Because only 34 states and the District of Columbia have some form of breach reporting legislation, and many of those laws have been in place for less than two years, there is not enough data available to make any reliable conclusions about reporting trends. With time, more states will enact legislation, other states will modify legislation, companies and government agencies will adapt to breach reporting legislation compliance, and trends will be more easily identifiable.

Second, a central database for cyber security breach reports must be created either on the state or national level. This database would serve two main purposes: 1) It would give greater visibility to the entire public, not just the parties directly affected by the breach, and 2) It would make data on breach reports more accessible and more reliable. The creation of a central reporting database would also call for more rigid language in state legislation; states would need to require that businesses and government agencies report to their respective databases and abandon legislation that allows bodies to report at their own discretion and only to the affected parties. While more care would need to be taken in breach reporting compliance, these changes would make for a more accurate depiction of the effectiveness of the laws.

Finally, we recommend that further research be conducted on the topic of cyber threat patch rates and their relevance to the actual cyber risk posed to users. Gauging the actual level of cyber risk of operating systems is difficult because the risk is based on the level of intent of outside hackers and the number of undiscovered vulnerabilities,

which is unknown. It would be of great value to know how a company's level of cyber security compares to the actual level of risk because one would be able to differentiate between a defect in state legislation and a lack of preparedness by a company.

It is important that policy makers understand that with the creation of cyber security breach reporting laws, there is a newly created problem of moral hazard. More specifically, if a company experiences a breach of security, there may be less incentive to report the breach if the actual financial effects of the breach are minimal and the financial reputation-based effects of reporting the breach are extensive. In addition, there may be incentive for a company to falsely report a cyber breach as an alternative disclosure of private information. For example, a business may experience a breach of security where an outside hacker accesses customer information; but to avoid more severe reputation-based consequences, the company may report the incident as a lost or stolen laptop. Policy makers must have a methodology set in place to somehow account for this moral hazard problem.

If these recommendations are adhered to, this framework for the evaluation of cyber security breach reporting laws can be modified and improved such that a fairly accurate picture of the current state of cyber security in the U.S. can be painted. Once the performance of state laws have been effectively evaluated, policy makers can then take appropriate actions, such as conduct interviews with corporate decision-makers or audits of companies and government agencies, to gain a more comprehensive view. Only then can cyber security practices and legislation be accurately evaluated and effective modifications made to give better protection to personal data.

APPENDIX

TABLE I  
2005 CYBER SECURITY BREACH STATISTICS BY STATE

State	Law in Place	Year Enacted	Years Enacted	# Reported Breaches	% Total Reported Breaches
CA	Y	2002	4	32	22.70%
OH	Y	2005	1	12	8.51%
GA	Y	2005	1	9	6.38%
NY	Y	2005	1	8	5.67%
CO	N	2006	0	7	4.96%
TX	Y	2005	1	7	4.96%
NC	Y	2005	1	6	4.26%
MI	N	2006	0	5	3.55%
IA	N	n/a	0	4	2.84%
MA	N	n/a	0	4	2.84%
D.C.	N	2007	0	4	2.84%
FL	Y	2005	1	3	2.13%
HI	N	2007	0	3	2.13%
IL	Y	2005	1	3	2.13%
MN	Y	2005	1	3	2.13%
NJ	Y	2005	1	3	2.13%
PA	Y	2005	1	3	2.13%
WA	Y	2005	1	3	2.13%
IN	Y	2005	1	2	1.42%
MO	N	n/a	0	2	1.42%
NV	Y	2005	1	2	1.42%
TN	Y	2005	1	2	1.42%
VA	N	n/a	0	2	1.42%
AZ	N	2007	0	1	0.71%
AR	Y	2005	1	1	0.71%
CT	Y	2005	1	1	0.71%
DE	Y	2005	1	1	0.71%
ID	N	2006	0	1	0.71%
KY	N	n/a	0	1	0.71%
MT	Y	2005	1	1	0.71%
NE	N	2006	0	1	0.71%
OK	N	2006	0	1	0.71%
OR	N	n/a	0	1	0.71%
RI	Y	2005	1	1	0.71%
UT	N	2006	0	1	0.71%
VT	N	2007	0	1	0.71%
WI	N	2006	0	1	0.71%
AL	N	n/a	0	0	0.00%
AK	N	n/a	0	0	0.00%
KS	N	2006	0	0	0.00%
LA	Y	2005	1	0	0.00%
ME	Y	2005	1	0	0.00%
MD	N	n/a	0	0	0.00%
MS	N	n/a	0	0	0.00%
NH	N	2007	0	0	0.00%
NM	N	n/a	0	0	0.00%
ND	Y	2005	1	0	0.00%
SC	N	n/a	0	0	0.00%
SD	N	n/a	0	0	0.00%
WV	N	n/a	0	0	0.00%
WY	N	n/a	0	0	0.00%

TABLE II  
2005 CYBER SECURITY BREACH COUNT BY INDUSTRY

Industry/Sector	# Reported Breaches
EDUCATION	68
FINANCE	24
STATE	12
FEDERAL	8
MEDICAL	7
TELECOMM	5
BUSINESS/PROF SERV	4
RETAIL	4
GAS/OIL	2
FOOD	2
NONPROFIT	2
AUTO	1
AERO/LOGISTICS	1
SERVICES	1
MANUFACTURING	1
BROADCASTING	1
<b>Total</b>	<b>143</b>

TABLE III  
2006 CYBER SECURITY BREACH STATISTICS BY STATE

State	Law in Place	Year Enacted	Years Enacted	# Reported Breaches	% Total Reported Breaches
CA	Y	2002	5	43	13.48%
NY	Y	2005	2	22	6.90%
OH	Y	2005	2	21	6.58%
VA	N	2007	0	18	5.64%
TX	Y	2005	2	15	4.70%
WA	Y	2005	2	14	4.39%
CO	Y	2006	1	12	3.76%
FL	Y	2005	2	12	3.76%
D.C.	N	2007	0	10	3.13%
IL	Y	2005	2	10	3.13%
GA	Y	2005	2	8	2.51%
IN	Y	2005	2	8	2.51%
KY	N	2007	0	8	2.51%
MI	Y	2006	1	8	2.51%
NJ	Y	2005	2	8	2.51%
NC	Y	2005	2	8	2.51%
PA	Y	2005	2	8	2.51%
CT	Y	2005	2	6	1.88%
MA	N	n/a	0	6	1.88%
MN	Y	2005	2	6	1.88%
SC	N	n/a	0	5	1.57%
WI	Y	2006	1	5	1.57%
IA	N	n/a	0	4	1.25%
MD	N	n/a	0	4	1.25%
MS	N	n/a	0	4	1.25%
NM	N	n/a	0	4	1.25%
OR	N	n/a	0	4	1.25%
AL	N	n/a	0	3	0.94%
KS	Y	2006	1	3	0.94%
NE	Y	2006	1	3	0.94%
OK	Y	2006	1	3	0.94%
RI	Y	2005	2	3	0.94%
TN	Y	2005	2	3	0.94%
UT	Y	2006	1	3	0.94%
AZ	N	2007	0	2	0.63%
DE	Y	2005	2	2	0.63%
MT	Y	2005	2	2	0.63%
VT	N	2007	0	2	0.63%
WV	N	n/a	0	2	0.63%
AK	N	n/a	0	1	0.31%
AR	Y	2005	2	1	0.31%
HI	N	2007	0	1	0.31%
ID	Y	2006	1	1	0.31%
ME	Y	2005	2	1	0.31%
MO	N	n/a	0	1	0.31%
NH	N	2007	0	1	0.31%
LA	Y	2005	2	0	0.00%
NV	Y	2005	2	0	0.00%
ND	Y	2005	2	0	0.00%
SD	N	n/a	0	0	0.00%
WY	N	n/a	0	0	0.00%

TABLE IV  
2006 CYBER SECURITY BREACH COUNT BY INDUSTRY

Industry/Sector	# Reported Breaches
EDUCATION	80
STATE	74
FINANCE	46
MEDICAL	34
FEDERAL	28
AERO/LOGISTICS	8
BUSINESS/PROF	7
RETAIL	7
TELECOMM	7
SERVICES	5
GAS/OIL	3
ENERGY	3
MANUFACTURING	3
AUTO	2
RAILROAD	2
ISP	2
FOOD	2
NONPROFIT	2
PUBLISHING	2
LAW	1
BROADCASTING	1
<b>Total</b>	<b>319</b>

TABLE V  
2005 OUTSIDE HACKER BREACH REPORT COUNT BY INDUSTRY

Industry/Sector	# Outside Hacker Breach Reports
EDUCATION	39
BUSINESS/PROF	3
RETAIL	2
STATE	2
FEDERAL	1
FINANCIAL	1
NONPROFIT	1
<b>Total</b>	<b>49</b>

TABLE VI  
2006 OUTSIDE HACKER BREACH REPORT COUNT BY INDUSTRY

Industry/Sector	# Outside Hacker Breach Reports
EDUCATION	27
STATE	9
FEDERAL	6
RETAIL	5
FINANCIAL	5
BUSINESS/PROFESSIONAL	4
MEDICAL	1
TELECOMMUNICATIONS	1
AUTO	1
GAS/OIL	1
<b>Total</b>	<b>60</b>

TABLE VII  
CORRELATION ANALYSIS RESULTS

	2005	2006
Pop-Attack	0.82196603	0.863475701
Inc-Attack	0.145931173	0.180891921
Firm-Attack	0.825314252	0.866653201
#DNP-Attack	0.622665619	0.673997656
DNPC-Attack	0.691016953	0.851639106
#SNP-Attack	0.627511371	0.679167152
SNPC-Attack	0.755774264	0.84842724
LP-Attack	0.312411727	0.244976799
YP-Attack	0.732743853	0.531645147
RREQ-Attack	-	0.211084975

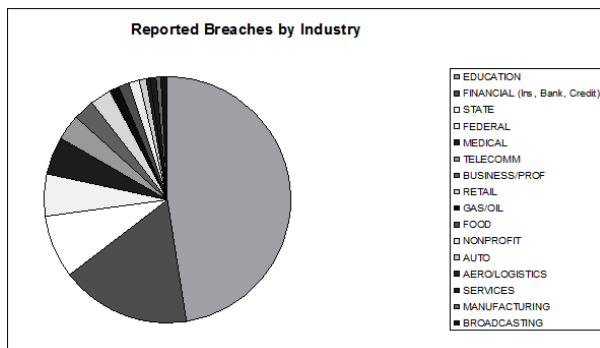


Fig. 1. An industry breakdown of reported cyber security breaches in 2005. In 2005, 16 industries experienced at least one publicized cyber security breach.

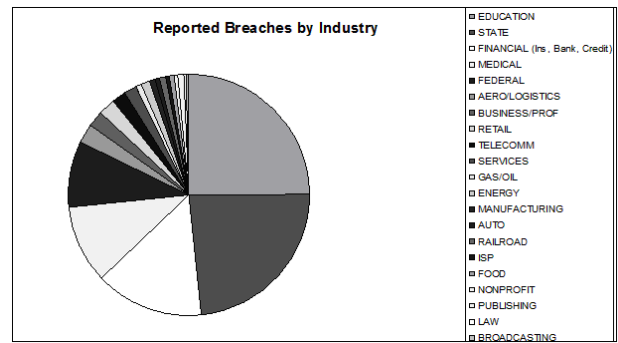


Fig. 2. An industry breakdown of reported cyber security breaches in 2006. In 2006, 21 industries experienced at least one publicized cyber security breach.

## REFERENCES

- [1] *A Chronology of Data Breaches Reported Since the ChoicePoint Incident.* (2006). Privacy Rights Clearinghouse. San Diego, California. Available: <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>.
- [2] Andrijcic, E. and B. Horowitz. (2006). *A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property.* University of Virginia.
- [3] "Security Breach/Notification Legislation." National Conference of State Legislatures. October 8, 2006. Available: <<http://www.ncsl.org/programs/lis/cip/priv/breach.htm>>.
- [4] *Data Loss Archive and Database (DLDOS).* (2006). Attrition.org. Available: <<http://attrition.org/dataloss/>>.
- [5] Wendlandt, Dan. *U.S. Cybersecurity Policy.* (2004). Stanford University. Available: <[http://www.stanford.edu/class/msande91siaut04/slides/cybersecurity\\_policy.ppt](http://www.stanford.edu/class/msande91siaut04/slides/cybersecurity_policy.ppt)>.
- [6] Waldermeir, Patti. *ChoicePoint fined \$15M by FTC.* Ft.com. <<http://www.ft.com/cms/s/b02019f4-8ea2-11d1-b752-0000779e2340.html>>.
- [7] Brooker, B., J. Crawford, and B. Horowitz. (2007). *Linking the Economics of Cyber security and Corporate Reputation.* University of Virginia.
- [8] *Client Alert: January 2007.* Proskauer Rose LLP. 2007. Available: <<http://www.proskauer.com>>.
- [9] U.S. Census Bureau. (2003). Available: <[www.census.gov](http://www.census.gov)>.
- [10] National Vulnerability Database. (2007). Available: <<http://nvd.nist.gov>>.