An Empirical Analysis of California Data Breaches

Richard Chen
Stanford University

Zakir Durumeric
Stanford University

Abstract

Data breaches have steadily become more frequent over the last several years. Under California's data breach notification law, all companies serving California residents who had their data stolen in a breach are required to disclose a breach report detailing the incident. We empirically analyze the public dataset of California data breach notifications, which contains 1,437 breach incidents between January 2012 and September 2018, to find patterns in the types of companies breached, attack vectors, and information stolen. We find that the financial services industry and large companies with over 10,000 employees are most likely to be breached. Software vulnerability is the most common descriptive attack vector. Social security numbers and payment cards are by far the two most common personal information stolen. We also show how attack vectors and information stolen tend to be predictable based on the company's profile.

1 Introduction

The number of data breaches continues to get worse over time. According to Risk Based Security, 2017 was the "worst year on record" for data breach activity, with over 1,200 data breaches and over 3.4 billion records exposed nationwide. [1] We know the exact number of data breaches that occur thanks to data breach notification laws, which require companies that have been breached to report breach incidents to state governments. Yet to our knowledge, there has been no study that analyzes such publicly available dataset.

In this study, we analyzed all data breaches reported to the California Department of Justice website. From a dataset of 1,437 data breaches between January 20, 2012 and September 21, 2018, we gathered data about the company's profile, the attack vector, and information stolen for each data breach. Over this time period, there was an average of 18 data breaches per month with a maximum of 60 data breaches in February 2017. The number of data breaches has been steadily increasing at a rate of 0.18 more data breaches each month compared to the previous month. We found patterns in company profiles, attack vectors, and personal information stolen across data breaches.

For company profiles, we found that the eight industries most frequently affected by data breaches accounted for over half of all data breaches, and the 25 most-affected industries accounted for over 80% of all data breaches. Large businesses (1,000+ employees) accounted for over half of all data breaches.

For attack vectors, other than unauthorized access, the most common attack vectors were software vulnerability, stolen computer or data, and data found publicly. Ransomware and phishing email were two fairly recent attack vectors that commonly occur since 2016. When comparing attack vectors to industries, there was often a single attack vector that accounted for most data breaches in a given industry.

For personal information stolen, the two most common were social security numbers and payment cards (credit/debit cards). This generally was true across all industries except for the industries that dealt with medical records.

2 Background

Data breach notification laws can be thought of as a laissez-faire accountability model that forces organizations to understand their security risks. Organizations can make security decisions on their own but must disclose data breaches if their decisions result in a security failure. Disclosure creates accountability inside an organization not only by raising awareness but also by defining costs for organizations to avoid in the form of notification expenses and adverse publicity. These laws haven't eliminated data breaches but have helped mitigate their impact.

The California Security Breach and Information Act (S.B. 1386) of July 2003 established the first-ever data breach notification law. The law requires any business or state agency to notify any California resident whose personal information was acquired or reasonably believed to have been acquired

by an unauthorized person. The law only applies to information that is either (a) not encrypted or (b) encrypted if an encryption key is also compromised. [2]

"Personal information" is defined as either of the following: [3]

(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

  (i) Social security number.

  (ii) Driver's license number or California identification card number.

  (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

  (iv) Medical information.

  (v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

The law also requires that a sample copy of any breach notice sent to more than 500 California residents be provided to the California Attorney General. [2] (In some cases, the organization that sent the notice is not the one that experienced the breach. For example, a bank may notify of a credit card number breach that occurred at a merchant, not the bank.)

The law has had an enormous impact on providing transparency around security failures. In 2004, there were only three publicized data breaches for publicly traded companies. In 2005, when the California law went into effect, there were 51. [4] California's law also prompted every other state to pass similar legislation in the absence of a single federal data breach notification law, with Alabama being the last state to pass a data breach notification law in March 2018. [5] Such notification to consumers and state authorities gave law enforcement, researchers, and others better data for understanding the nature and scope of the data breach problem instead of relying on reports from media outlets, which don't cover every breach that occurs.

Finally, these laws have sparked entire new industries to help organizations prevent data breaches and respond appropriately if they occur. As an example, cyber insurance is a fairly recent industry that protects businesses from risks relating to data breaches and cyber attacks. The market for cyber insurance premiums totaled $5 billion in 2018 and is expected to double in the next five years. [6]

3 Related Work

Prior studies have mainly focused on the cost of data breaches to companies.

The *2018 Cost of a Data Breach Study: Global Overview*, conducted by IBM Security and Ponemon Institute, surveyed more than 2,200 IT, data protection, and compliance professionals from 477 companies that experienced a data breach in the past 12 months. According to the report, data breaches continue to be costlier and result in more consumer records being lost or stolen cumulatively every year. The key findings were: [7]

- The average total cost of a data breach in 2018 rose from $3.62 million to $3.86 million, an increase of 6.4% from 2017.
- The average cost for each lost record in 2018 rose from $141 to $148, an increase of 4.8% from 2017.
- The average size of data breaches increased by 2.2%.

In addition to presenting trends in the cost of data breaches, the study also determined a 27.9% likelihood that an organization breached today will be breached again in the next two years. [7]

Lastly, the study reported on the relationship between how quickly an organization identifies and contains a data breach and its financial consequences. The average time to identify a breach was 197 days and the average time to contain a breach was 69 days. Companies that contained a breach in under 30 days saved over $1 million compared to those that took more than 30 days to resolve the breach. The study revealed a reduction in cost when companies participate in threat sharing activities and deploy data loss prevention technologies. [7]

Data breaches are now a consistent cost of doing business. The biggest financial consequence to organizations that experience a data breach is lost business. Industries such as healthcare and financial services have the costliest data breaches because of fines and loss of business. [7] The costs beyond settlement with banks include legal support, forensic investigation, data and network restoration, compliance with breach notification laws, business interruption, and post-breach marketing to restore reputation. [8]

4 Methodology

Since companies are forced to disclose data breaches, the California state government has a comprehensive dataset of all companies serving California residents that have been breached. In this study, we looked at all California data breach notifications that are publicly available on the California Department of Justice website. The website lists detailed breach notification reports for all data breaches that have been reported since January 20, 2012. [9]

We collected a dataset of 1,437 breach incidents that were reported between January 20, 2012 and September 21, 2018.

4.1 Company Data

We labeled each company that was breached with its "industry," "company type," and "company size" using LinkedIn's dataset on companies. "Industry" is based on LinkedIn's Industry Codes. [10] "Company type" is one of the following: educational institution, government, nonprofit, partnership, privately held, public company, self-employed, or sole proprietorship. "Company size" is one of the following: 1-10, 11-50, 51-200, 201-500, 501-1,000, 1,001-5,000, 5,001-10,000, or 10,000+.

While we were able to label every company with its industry, LinkedIn's dataset did not have the company type or size for every company. Only 75.5% of companies were labeled with "company type" and 83.4% of companies were labeled with "company size."

4.2 Data Breach Reports

California law requires that data breach reports follow a standardized form. The "What Happened?" section must include "a general description of the breach incident, if that information is possible to determine at the time the notice is provided," and the "What Information Was Involved?" section must include "a list of the types of personal information that were or are reasonably believed to have been the subject of a breach." [11]

For the "What Happened?" section, we classified each breach incident into one of the following attack vectors:

- **Compromised Email:** A compromised email account allows the attacker to gain access to every website that uses the email as a login.
- **Compromised Machine:** Physical machines (e.g. point-of-sale credit/debit card terminals, ATM machines) are hacked using methods such as card skimmers.
- **Data Found Publicly:** Personal information is found online by third-parties or in the physical garbage bin without being shredded.
- **Exposed Data:** (1) Misconfigured privileges causes a database or files to be exposed publicly online and possibly searchable by Google or enables an employee without proper authorization to access the files. (2) A software bug causes a user's personal information to be displayed to other users.
- **Insider Theft:** A current or former employee exfiltrates personal information such as by sending files to a non-work email, taking physical records or hard drives, or saving files to a non-work cloud storage. Some purposes are for committing fraud, identity theft, or theft of trade secrets.
- **Lost Computer or Data:** An employee loses his/her unencrypted computer, physical records of personal information are found missing, or mail containing personal information is lost in transit.
- **Phishing Email:** An employee is mislead into entering his/her credentials into a spoofed login page.
- **Ransomware:** Malware encrypts a company network's files and demands ransom for the files to be decrypted.
- **Social Engineering:** A spoofed email impersonates the CEO or a high-level company executive to mislead an employee into sending personal information, or an attacker misleads customer support into giving access to a user's account.
- **Software Vulnerability:** Vulnerabilities include web vulnerabilities (e.g. SQL injection, XSS attack) and unpatched third-party software or libraries (e.g. Apache Struts vulnerability).
- **Stolen Computer or Data:** An employee's unencrypted computer or physical records containing personal information is stolen.
- **Stolen Credentials:** An account's password is the same one used on another compromised website, or the password is weak and easily brute-forced.
- **Unauthorized Access:** A catch-all term for vague data breach reports that follow the general form: "We detected unauthorized access to our network where some personal information may have been exposed."
- **Wrong Data Sent:** An employee accidentally sends personal information or the wrong personal information to an external third-party.

For the "What Information Was Involved?" section, we compiled a list of "personal information" (defined earlier in Section 2) that was affected by each breach incident. Other affected information, such as date of birth and address, could be voluntarily disclosed in the breach report but is not required by law, so we did not consider other affected information in our study due to voluntary response bias.

5 Results

5.1 Company Profiles

The companies breached most often were American Express (5.9%) and Discover Financial Services (1.8%), two major

credit card companies. This is not surprising given that both companies are required to notify their customers every time a dataset of credit card information is found publicly online (see "Data Found Publicly" in Section 4.2). 5.4% of companies were breached more than once during the time period between January 20, 2012 and September 21, 2018.

The top eight industries accounted for over 50% of all data breaches across 98 different industries: financial services (17.6%), hospital & health care (9.5%), retail (5.4%), hospitality (4.6%), higher education (4.5%), insurance (3.5%), medical practice (3.4%), and accounting or government administration (tied 4.1%). The top 25 industries accounted for over 80% of all data breaches. [Figure 1]

An overwhelming majority of breached companies were either privately held (37.0%) or public company (34.8%). The remaining company types were nonprofit (11.5%), educational institution (6.9%), government agency (6.0%), partnership (1.9%), sole proprietorship (1.6%), and self-employed (0.3%).

The majority of data breaches came from large companies with 10,000+ employees (30.3%). Including the 5,001-10,000 range (5.3%) and 1,001-5,000 range (16.7%), large businesses altogether accounted for 52.3% of all data breaches. [Figure 2] This is contrary to prior claims that two-thirds of all data breaches come from small to medium-size businesses (SMBs). [12] However, there may be some response bias in the data since SMBs are less likely to report data breaches, even if required by law, in scenarios such as when an employee loses a laptop containing personal information.

Prior work found that companies that contain a data breach in under 30 days save over $1 million compared to those that take more than 30 days to resolve. [7] According to our findings, only 21.5% of data breaches were reported within 30 days. While the median report time was 78 days, the distribution of report times was heavily skewed right such that the average report time was 175 days. The longest time it took to report a data breach was 7 years, 6 months, and 9 days (2,747 days).

18.6% of companies that reported breaches were unable to ascertain the exact date(s) when the data breach occurred. For those that were able to, there was an average of 18 data breaches per month with a maximum of 60 data breaches in February 2017. (June through September 2018 may be underreported since it takes on average 175 days to report a data breach that occurred.) The number of data breaches has been steadily increasing at a rate of 0.18 more data breaches each month compared to the previous month. There was also a slight seasonal pattern in data breaches with a small increase in the number of data breaches during February through April. [Figure 3]

Accounting was the only industry with a significant change in frequency of data breaches over time. 94.2% of all data breaches that affected accounting firms happened after January 2016. Prior to January 2016, there were only 4 reported instances of accounting firms being breached.

5.2 Attack Vectors

The most common attack vector is the generic catch-all term "unauthorized access" (27.0%) because many data breach reports did not explain the specific attack vector. For the data breach reports that did explain how the company was breached, software vulnerability (13.1%), stolen computer or data (11.4%), data found publicly (11.1%), wrong data sent (7.3%), and exposed data (7.2%) accounted for over half of all attack vectors. [Figure 4]

Some attack vectors were concentrated within a small time frame. For compromised machine attacks, there was a spike of 39 incidents in February 2017; excluding that month, compromised machine attacks only averaged 1.35 incidents per month. This spike was the result of an attacker installing credit card skimmers on the point-of-sale payment terminals for several Acme Car Wash and Clearwater Express stations. Similarly, in October 2016, there were 13 incidents of wrong data sent, compared to the normal average of 1.41 incidents per month. This was the result of insurance company EmblemHealth inadvertently printing customers' SSNs on the external mailing labels of packages, which happened repeatedly for multiple days throughout October before the company finally discovered the error.

Some attack vectors were fairly recent phenomenons. Ransomware attacks started happening in July 2016 with hospitals and medical practices being the primary targets. Before then, there was only a single reported incident of ransomware, which affected the law firm Ziprick & Cramer, LLP in January 2015. Likewise, phishing email attacks started happening consistently every month since February 2016, averaging 2.03 incidents per month. Before then, there were only scattered incidents of phishing email attacks, averaging just 0.16 incidents per month. [Figure 5]

There is usually a single attack vector that accounts for a large number of data breaches in each industry. Data found publicly was by far the largest cause of data breaches for financial services companies (63.8%). Others include: software vulnerability for apparel & fashion (62.5%), consumer goods (60.0%), and retail (52.5%); compromised machine for hospitality (57.9%) and restaurants (57.1%), stolen computer or data for medical practice (52.6%); and exposed data for computer software (50.0%). [Figure 6] The data also corroborated prior work that showed internal negligence was to blame for most data breaches involving personal health information. [13]

Similarly, there is usually a single industry that accounts for a large number of data breaches for each attack vector. Financial services was by far the largest industry for the data found publicly attack vector (90.3%). Others include: hospital & health care for lost computer or data (35.7%); hos-

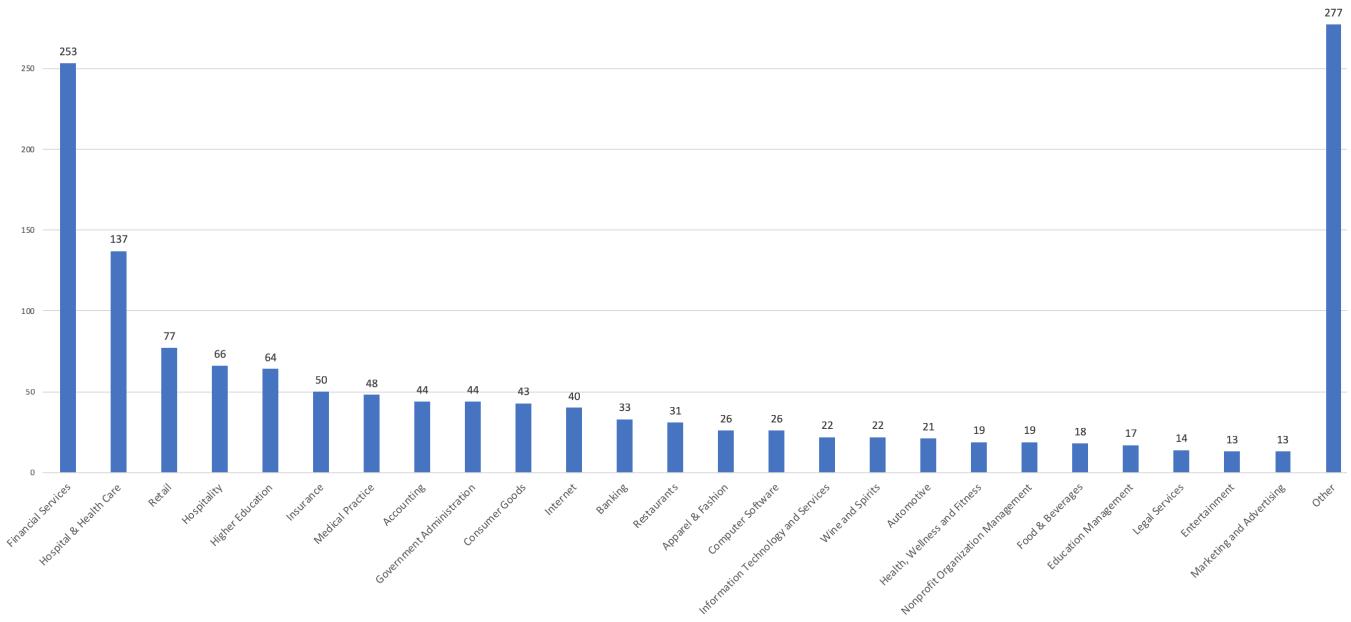

Figure 1: Frequency of data breaches for the top 25 industries out of 98 different industries. The top 8 industries accounted for over half of all data breaches, and the top 25 industries accounted for over 80% of all data breaches.

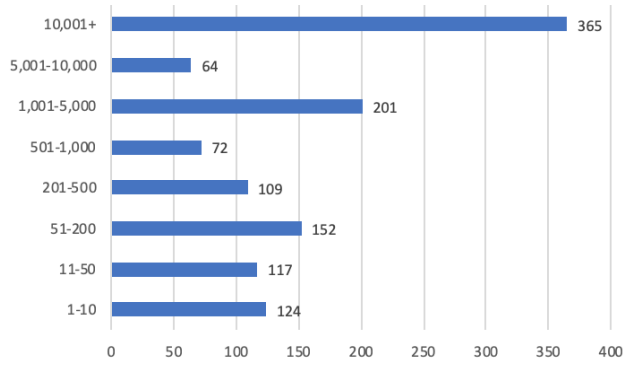

Figure 2: Frequency of data breaches per company size. Large businesses (1,000+ employees) accounted for over half of all data breaches.

pitality for compromised machine (34.4%); medical practice for ransomware (33.3%); and internet for stolen credentials (32.4%). [Figure 6]

Most attack vectors most commonly occurred in large companies with 10,000+ employees. This supports the notion that a large attack surface increases the likelihood of an attack happening regardless of the specific attack vector. For instance, it becomes more likely that an employee inadvertently sends personal information to the wrong person the more employees an organization has.

The main exceptions were software vulnerability and ransomware. 24.7% of software vulnerability attacks affected businesses with 51-200 employees. 40.0% of ransomware attacks affected small businesses with 1-10 employees; these were doctor offices that relied on a handful of insecure software systems to store their medical records. This data runs contrary to the narrative that large organizations are primarily the targets of ransomware attacks, such as when the NotPetya ransomware crippled the network of the multinational shipping giant Maersk and cost $250-$300 million in damages. [14]

5.3 Personal Information Stolen

The two most common personal information stolen by far were social security numbers (42.4%) and payment cards including credit/debit cards (41.1%). Other information stolen included medical records (14.8%), passwords of other users in addition to the compromised account (11.6%), bank routing and account numbers (10.0%), health insurance informa-

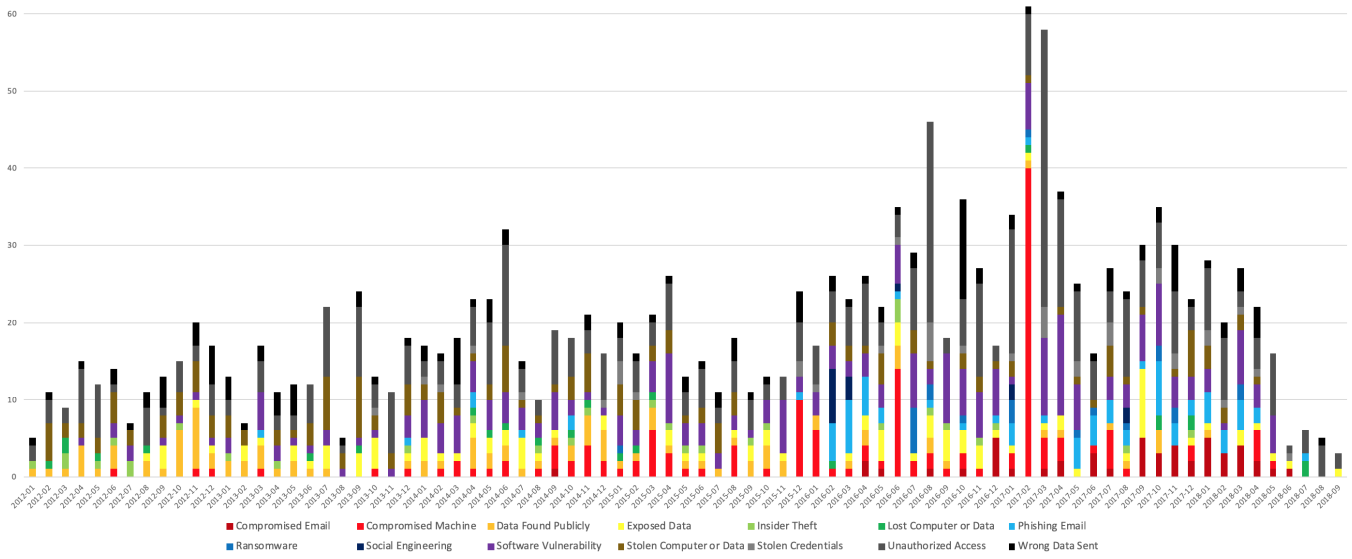

Figure 3: Number of data breaches per month since January 2012, broken down by each attack vector. There was an average of 18 data breaches per month with a maximum of 60 data breaches in February 2017. The number of data breaches has been steadily increasing at a rate of 0.18 more data breaches each month compared to the previous month.

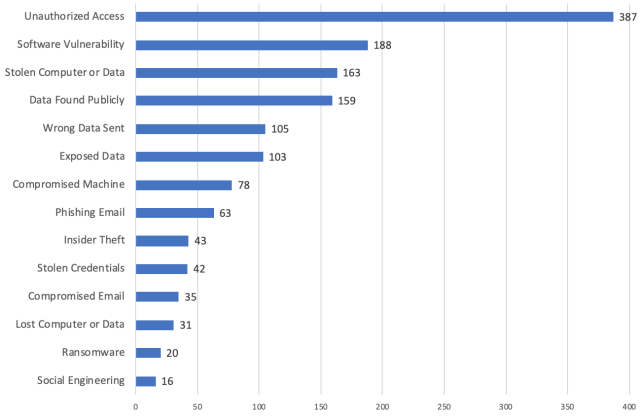

Figure 4: Frequency of data breaches per attack vector. The most common attack vector is the generic catch-all term "unauthorized access" because many data breach reports did not explain the specific attack vector.

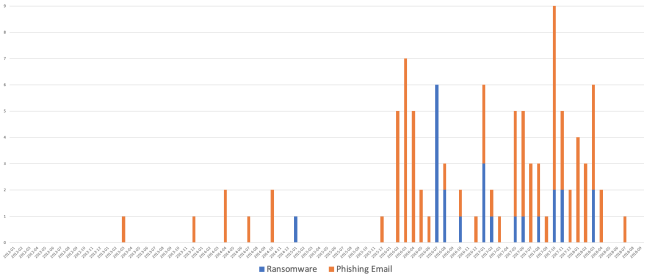

Figure 5: Frequency of ransomware and phishing email over time. Both have occurred much more commonly recently, with ransomware starting in July 2016 and phishing email starting in February 2016.

tion (8.7%), and driver's license numbers (7.9%). [Figure 7]

There were three spikes in theft of payment card information in April 2015, February 2017, and March 2017. 14% of all payment card thefts happened within those three months. These concentrated data breaches occurred because many companies within the same industry were using the same payment card processor – whether a point-of-sale payment terminal or a software that stores payment card information – that got compromised.

In April 2015, 23 wineries were using the Missing Link direct sales software system to store payment card information, which was accessed by an unauthorized third-party. In February 2017, several Acme Car Wash and Clearwater Express stations were using the same point-of-sale payment terminals that were compromised with card skimmers. In

	Compromised Email	Compromised Machine	Data Found Publicly	Exposed Data	Insider Theft	Lost Computer or Data	Phishing Email	Ransomware	Social Engineering	Software Vulnerability	Stolen Computer or Data	Stolen Credentials	Wrong Data Sent	Total
Financial Services	5	0	139	12	8	4	10	0	2	6	5	6	21	218
Hospital & Health Care	5	0	2	15	8	10	8	4	1	4	32	0	25	114
Retail	0	8	0	3	1	0	2	1	2	31	3	6	2	59
Hospitality	2	22	0	1	0	0	2	0	0	5	2	4	0	38
Higher Education	1	1	0	11	2	1	4	1	1	4	13	1	6	46
Insurance	0	0	0	6	6	0	5	0	1	3	8	0	11	40
Medical Practice	2	0	1	2	3	1	0	6	0	3	20	0	0	38
Government Administration	0	0	2	9	3	4	1	0	0	2	3	0	15	39
Accounting	4	1	1	2	0	0	1	2	0	3	10	0	0	24
Consumer Goods	1	0	1	1	0	0	1	0	1	18	3	4	0	30
Internet	0	0	2	4	0	0	0	0	0	6	1	12	0	25
Banking	1	3	3	4	2	3	2	0	0	0	1	0	2	21
Restaurants	0	16	0	0	1	1	0	1	0	4	4	0	1	28
Computer Software	1	0	0	8	0	0	3	0	0	0	1	1	2	16
Apparel & Fashion	2	2	0	1	0	0	0	0	0	10	0	1	0	16
Information Technology and Services	1	2	0	2	1	1	2	0	0	6	0	1	0	16
Wine and Spirits	0	0	0	0	1	0	0	1	0	1	0	0	0	3
Automotive	0	4	1	1	1	0	0	0	0	3	5	0	0	15
Health, Wellness and Fitness	0	0	0	4	3	0	1	0	0	6	2	0	0	16
Nonprofit Organization Management	0	0	1	2	0	1	0	1	1	2	3	0	1	12
Food & Beverages	0	5	0	0	0	1	1	0	0	4	2	0	1	14
Education Management	0	0	0	2	1	0	1	0	0	4	1	0	3	12
Legal Services	0	0	1	2	0	0	1	1	0	1	5	0	0	11
Entertainment	0	0	0	0	0	1	0	0	0	3	1	1	0	6
Marketing and Advertising	1	0	0	0	0	0	2	0	0	3	1	0	0	7
Total	26	64	154	92	41	28	47	18	9	132	126	37	90	**864**

Figure 6: Frequency of each attack vector for the top 25 industries. The scattered green squares suggest that there is a single attack vector that accounts for most data breaches for each industry and likewise a single industry that accounts for most data breaches for each attack vector. (Unauthorized access is omitted since it is a non-descriptive attack vector.)

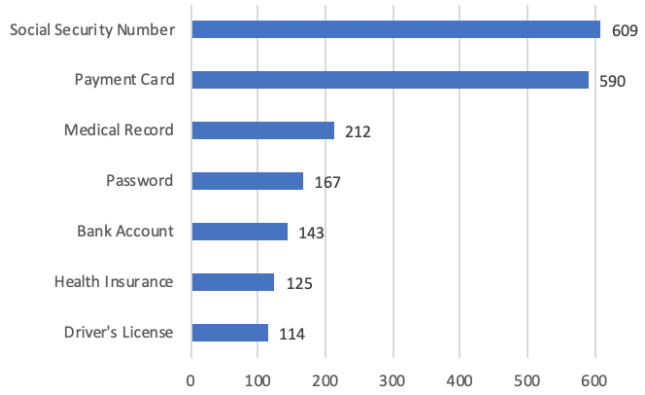

Figure 7: Frequency of each personal information stolen. The two most common personal information stolen by far were social security numbers and payment cards.

	SSN	Payment	Medical	Password	Bank	Insurance	DL	Total
Financial Services	93	154	4	7	43	3	26	330
Hospital & Health Care	62	3	94	1	2	32	8	202
Retail	10	62	0	12	0	0	4	88
Hospitality	6	61	0	3	1	0	2	73
Higher Education	51	8	7	6	9	4	7	92
Insurance	38	3	10	1	3	13	5	73
Medical Practice	28	1	34	0	3	24	5	95
Government Administration	32	6	4	0	4	5	9	60
Accounting	41	3	0	0	23	2	1	70
Consumer Goods	6	32	2	10	4	2	2	58
Internet	4	11	1	25	1	1	3	46
Banking	18	13	0	2	9	0	2	44
Restaurants	9	22	0	0	1	0	0	32
Computer Software	13	4	4	7	1	2	1	32
Apparel & Fashion	1	22	0	5	0	1	0	29
Information Technology and Services	9	8	2	1	1	4	2	27
Wine and Spirits	3	19	0	18	1	0	0	41
Automotive	7	10	1	3	2	3	5	31
Health, Wellness and Fitness	7	8	7	1	0	1	1	25
Nonprofit Organization Management	8	4	5	5	1	1	3	27
Food & Beverages	4	13	1	3	1	2	1	25
Education Management	5	5	1	1	1	0	0	13
Legal Services	13	1	2	0	2	1	5	24
Entertainment	5	5	1	4	3	2	1	21
Marketing and Advertising	5	7	1	3	1	1	3	21
Total	478	485	181	118	117	104	96	**1579**

Figure 8: Frequency of each information stolen for the top 25 industries. In general, social security numbers and payment cards were the two most common personal information stolen regardless of the industry, except for the industries that dealt with medical records.

March 2017, 24 hotels were using the Sabre SynXis Central Reservations system to facilitate the booking of hotel reservations, in which stolen credentials enabled an attacker to steal payment card information. These incidents show that relying on a single vendor to process personal information, such as payment cards, creates a single point of failure risk.

Bank account numbers have also become more frequently stolen in recent years. There were three times as many reported incidents after November 2015 compared to before November 2015.

Social security numbers and payment cards were the two most common personal information stolen across the top 25 industries. The few exceptions were medical records for hospital & health care (46.5%) and medical practice (36.8%), as well as passwords for Internet companies (54.3%). The financial services industry was the industry most commonly affected by stolen social security numbers (19.5%), payment cards (31.8%), bank account numbers (36.8%), and driver's license numbers (27.1%). The hospital & health care industry was the industry most commonly affected by stolen medical records (51.9%) and health insurance information (30.8%). The Internet industry was the industry most commonly affected by stolen passwords (21.2%). [Figure 8]

Social security numbers and payment cards were also the two most common personal information stolen across all company sizes with the exception of health insurance information, which was most common for small businesses with 1-10 employees.

6 Conclusion and Future Work

The attack vectors and information stolen in data breaches tend to follow a predictable pattern depending on the company's profile. For instance, we found that for many industries, the types of attack vectors and information stolen are concentrated in only a few categories. Based on our findings, we can better predict how a company is going to be breached and what information is at risk of getting stolen. This is very useful for not only high-risk organizations but also cyber insurance underwriters that have to create cyber risk models to determine premiums based on the company's profile.

There are many possible areas for future work. This study only focused on California data breaches, but we could extend this study to compare California data breaches to those from other states, since all states have a data breach notification law. There may be notable differences because many tech companies are located in California.

Furthermore, we could assess the financial damage of data breaches. Some data breaches do not materially affect the company's bottom line, while others, such as the Equifax data breach, greatly impact the company's financials. With this information, we can ascertain what types of data breaches cause more financial damage than others, and whether the severeness of financial damage correlates with the company's profile.

Lastly, for data breaches that were able to attribute who was responsible, we could figure out if and/or how such data was used maliciously.

7 References

[1] "Data Breach Activity Reaches All-Time High." *Help Net Security*, Help Net Security, 23 May 2017.

[2] "Data Breach Charts." *BakerHostetler*, July 2018.

[3] California Civil Code. Title 1.81, Section 1798.81.5.

[4] Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, 2014.

[5] Heck, Zachary. "Alabama Rolls with Tide as Last State to Adopt Breach Notification Law." *Lexology*, Lexology, 30 Apr. 2018.

[6] Betterley, Richard S. "Cyber/Privacy Insurance Market Survey—2018." *The Betterley Report*, June 2018.

[7] "2018 Cost of a Data Breach Study: Global Overview." *Ponemon Institute*, July 2018.

[8] Williams, Gareth, Robert E. Schulz, David C. Tesher, and Laurence P. Hazell. "Cyber Risk and Corporate Credit." *RatingsDirect*. 9 June 2015.

[9] "Search Data Security Breaches." *State of California Department of Justice*, DOJ, oag.ca.gov/privacy/databreach/list.

[10] "Industry Codes." *LinkedIn Developers*, LinkedIn Corporation.

[11] California Civil Code. Title 1.81, Section 1798.82.

[12] Boneh, Dan. "Why Is Computer Security Difficult?" Cybersecurity: A Legal and Technical Perspective. 3 Apr. 2018, Stanford, California.

[13] "Internal Negligence to Blame for Most Data Breaches Involving Personal Health Information." *Help Net Security*, Help Net Security, 25 Nov. 2018.

[14] Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, Conde Nast, 24 Oct. 2018.