California Data Breach Report

2012-2015

Kamala D. Harris, Attorney General
California Department of Justice

February 2016

California Data Breach Report

2012-2015

Kamala D. Harris, Attorney General
California Department of Justice

February 2016

This document is for informational purposes and should not be construed as legal advice or as policy of the State of California. The document may be copied, provided that (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

Contents

Message from the Attorney General i

Executive Summary iii

Introduction 1

Findings 9

Recommendations 27

Appendix A 39

Appendix B 41

Appendix C 51

Notes 61

Message from the Attorney General

The California Constitution guarantees every Californian the "inalienable right" to privacy. To ensure that protection, California has been on the cutting edge, adopting the strongest and most sophisticated consumer privacy laws in the United States. But California's fast-changing economy requires our constant vigilance to ensure that privacy and security protections keep pace with innovation and new threats. Each day, millions of Californians log on to the internet to conduct business, do homework, purchase goods and services, control devices in their homes, play games, and connect with loved ones. Technology such as smartphones, the "internet of things," wearable devices, and big data are transforming our lives at a rapid pace, while exponentially increasing the amount of personal information that is collected, used, and shared. At the same time, with data becoming more ubiquitous and valuable, the black market for stolen information also continues to expand, increasing the likelihood of hacking by cyber criminals.

With more of our personal information online, it is imperative that organizations employ strong privacy practices. To protect privacy, businesses must have privacy policies that are easy to read and access, inform consumers about material changes to their data handling practices, and carefully select their default settings which often determine how data is collected, used, and shared. Foundational to those privacy practices is information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access.

Data breaches, particularly when they involve sensitive information such as Social Security numbers and health records, threaten not only the privacy but also the security and economic wellbeing of consumers. Breaches also impact a wide range of industries, from the health care and financial services sectors to retail and small businesses, and pose a threat to critical infrastructure and national security. Now that organizations rely increasingly on the collection and use of personal information and criminals take advantage of security weaknesses to obtain and profit from that same information, it is more important than ever that all of us redouble our efforts to ensure that this data does not end up in the wrong hands.

The report that follows provides a comprehensive analysis of the data breaches reported to my office from 2012 to 2015. In the last four years, nearly 50 million records of Californians have been breached and the majority of these breaches resulted from security failures.

Furthermore, nearly all of the exploited vulnerabilities, which enabled these breaches, were compromised more than a year after the solution to patch the vulnerability was publicly available. It is clear that many organizations need to sharpen their security skills, trainings, practices, and procedures to properly protect consumers.

Securing data is no doubt challenging, with sophisticated cyber criminals – including some nation states – waging an escalating battle. But many of the breaches reported to us could have been prevented by taking reasonable security measures, and an organization that voluntarily chooses to collect and retain personal information takes on a legal obligation to adopt appropriate security controls.

As we become further immersed in the online world, our lives and our livelihoods depend more and more on our ability to use technology securely. The potential of a digitally connected society is immense, so it is critical that we put the appropriate safeguards in place before individuals feel that they must either abandon their right to privacy or go offline to protect it. This report is a starting point, and a call to action, for all of us—organizations, individuals, and regulators—to work toward a safer and more secure online future.

Sincerely,

Attorney General Kamala D. Harris

Executive Summary

Since 2012, businesses and government agencies have been required to notify the Attorney General on breaches affecting more than 500 Californians. In our latest report, we analyze all such breaches from 2012 through 2015. In it we present our findings on the nature of the breaches that are occurring, what can be learned from them about threats and vulnerabilities, and we make recommendations aimed at reducing the risk of data breaches and mitigating the harms that result from them.

In the past four years, the Attorney General has received reports on 657 data breaches, affecting a total of over 49 million records of Californians. In 2012, there were 131 breaches, involving 2.6 million records of Californians; in 2015, 178 breaches put over 24 million records at risk. This means that nearly three in five Californians were victims of a data breach in 2015 alone.

These breaches occurred in all parts of our economy: retailers and banks, doctors, dentists and hospitals, gaming companies, spas, hotels, restaurants, government agencies, schools, and universities. The majority of the reported breaches were the result of cyber attacks by determined data thieves, many of whom took advantage of security weaknesses. Breaches also resulted from stolen and lost equipment containing unencrypted data, and from both unintentional and intentional actions by insiders (employees and service providers).

Types of Breach

- *Malware and hacking* presents the greatest threat, both in the number of breaches (365, 54 percent) and the number of records breached (44.6 million, 90 percent). This is a growing problem compared to other types of breach, increasing by 22 percent in the past four years, from 45 percent of breaches in 2012 to 58 percent in 2015. The six breaches of more than one million records are all of this type. The retail sector in particular struggles with malware and hacking, which comprises 90 percent of all retailer breaches.
- *Physical breaches*, resulting from theft or loss of unencrypted data on electronic devices, came in a distant second. The relative share of this type of breach declined, from 27 percent of all breaches in 2012 to 17 percent in 2015. The health care sector had the greatest problem with breaches of this type (more than half of all its breaches), and small businesses were more than 50 percent more likely to report a physical breach than were larger businesses.
- *Breaches caused by errors*, predominantly misdelivery (of email, for example) and inadvertent exposure on the public Internet, were a close third, and have held steady at around 17 percent. Half of government breaches were of this type.

Types of Data Breached

- More of the most sensitive personal information – Social Security numbers and medical information – was breached than other data types.

- Social Security numbers were the data type most often breached, involved in just under half of all breaches, for a total of 24 million records containing Social Security numbers. That is nearly half of the 49.6 million records of Californians breached in the four-year period.

- Medical information was included in 19 percent of breaches and 18 million records, and payment card data in 39 percent of breaches and 16 million records.

- As retailers continue their transition to EMV (chip-enabled payment cards), the attractiveness of trying to steal payment card data from in-store systems will decline and the focus of criminals on Social Security numbers will likely increase.

Industry Sectors

- The retail sector had the largest share of breaches, accounting for 25 percent of breaches and 42 percent of records breached in the past four years. Most retail breaches were caused by malware and hacking, and the type of data most commonly breached was payment card data.

- The financial sector accounted for the second largest share of breaches, 18 percent, and for 26 percent of records breached. The sector showed the greatest susceptibility to breaches caused by insiders (employees, service providers), both through unintentional errors and intentional misuse of privileges. The most common type of data breached in this sector was Social Security numbers.

- Health care, with 16 percent of breaches, continued to be particularly vulnerable to physical breaches, although malware and hacking breaches are starting to increase as the sector's transition to electronic medical records progresses. The most vulnerable information in health care was medical information, such as patient records, and Social Security numbers.

- Despite generally having less data than larger businesses, small businesses were still a significant breach risk and represented 15 percent of all breaches reported. They were most susceptible to hacking and malware attacks, but also experienced physical breaches at a greater rate than larger businesses.

Reasonable Security

Securing data is challenging, with technology evolving rapidly, business practices relying increasingly on the collection and use of personal information, and sophisticated cyber criminals waging an escalating battle. Yet securing information is the ethical and legal responsibility of the organizations with which individuals entrust their personal information. The legal obligations to secure personal information include an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes. California's information security statute requires businesses to use "reasonable security procedures and practices…to protect personal information from unauthorized, access, destruction, use, modification, or disclosure." Federal laws, including the Gramm Leach Bliley Act (GLBA) and the Health Insurance Portability and Access Act (HIPPA), contain general security requirements for the financial services and health care industries. Authoritative security standards describe the measures that organizations should take to achieve an appropriate standard of care for personal information.

State Breach Laws

As the number of state data breach laws has grown in recent years, there has been an effort to pass a federal law that would preempt state laws. The rationale offered has been a reduction of the burden of complying with the different state laws. The proposals under consideration in Congress, however, have tended to set the bar far below California's current level of protection. They would also in many cases preempt not only state laws on data breach but also longstanding information security and consumer protection statutes.

Recommendations

1) The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.

2) Organizations should make multi-factor authentication available on consumer-facing online accounts that contain sensitive personal information. This stronger procedure would provide greater protection than just the username-and-password combination for personal accounts such as online shopping accounts, health care websites and patient portals, and web-based email accounts.

3) Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers. This is a particular imperative for health care, which appears to be lagging behind other sectors in this regard.

4) Organizations should encourage individuals affected by a breach of Social Security numbers or driver's license numbers to place a fraud alert on their credit files and make this option very prominent in their breach notices. This measure is free, fast, and effective in preventing identity thieves from opening new credit accounts.

5) State policy makers should collaborate to harmonize state breach laws on some key dimensions. Such an effort could reduce the compliance burden for companies, while preserving innovation, maintaining consumer protections, and retaining jurisdictional expertise.

Introduction

Data breaches are growing in scope, affecting more organizations and more people. Much is at stake: data breaches impose financial, reputational, and lost opportunity costs on individuals and organizations. Data breaches also threaten critical infrastructure and imperil national security.

There are real costs to individuals. Victims of a data breach are more likely to experience fraud than the general public, according to Javelin Strategy & Research.[1] In 2014, 67 percent of breach victims in the U.S. were also victims of fraud, compared to just 25 percent of all consumers.

In recognition of this growing threat, starting in 2003, California has required businesses and government agencies to notify California residents when they experience a breach of the residents' personal information. Since 2012, businesses and government agencies have also been required to notify the Attorney General on breaches affecting more than 500 Californians.

In furtherance of the breach notice law's transparency goals, we post the notices on the Attorney General's website as they are submitted. We also review the breaches, sometimes taking legal action,[2] and always seeking to learn from them. This report is the result of our review and analysis of the 657 data breaches reported to the Attorney General from 2012 through 2015.[3]

In the report we present our findings on the nature of the breaches that are occurring and what can be learned from them about threats and vulnerabilities. We also make recommendations aimed at reducing the risk of data breaches and mitigating the harms that result from them.

California's Breach Notice Law

California was the first to enact a data breach notification law, which took effect in 2003. In the twelve years since then, 46 other states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, as well as foreign jurisdictions around the world, have enacted similar laws.[4]

The California law's original intent was to give early warning to consumers that they were at risk of identity theft so that they could act to protect themselves.[5] The law's impact, however, has been more far-reaching. The law's transparency requirement has motivated organizations to devote greater attention and additional resources to their data privacy

and security practices and has highlighted data insecurity as a matter of concern for policy makers and the general public.

The law requires any person or business that conducts business in California, and any state or local agency, that owns or licenses "computerized data" that includes personal information to notify any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a breach of security. Entities that maintain such data are required to notify the owner or licensee of the information in the event of a breach of the data. The complete text of the California law can be found in Appendix C.

Scope of Information Covered

When California's law first took effect, it focused on the type of information used to commit financial identity theft: Social Security number, driver's license number, and financial account number. The type of information covered by the law has been updated multiple times since then, in response to emerging threats and rapidly changing technology. In 2008, with awareness of burgeoning medical identity theft and its life-threatening impact for California residents, medical and health insurance information were added to the law's purview. In 2013, with evidence that criminal organizations were targeting online account credentials, the law was amended to also include a user name or email address, in combination with a password or security question and answer that permits access to an online account. In 2015, in recognition of the growing sensitivity of the location information included in the data, data from automated license plate reader systems was added to the definition in the breach law.

Notification Trigger and Timing

The requirement to notify is triggered by the acquisition, or reasonable belief of acquisition, of personal information by an unauthorized person.

Organizations that own or license the data must notify individuals "in the most expedient time possible and without unreasonable delay." The law conveys the need for urgency, and by providing a flexible standard, rather than a bright-line rule, it accommodates realities in particular breach situations. It allows for the time needed to determine the scope of a breach and to secure the system, and provides an option for a delay if law enforcement determines that notifying would impede a criminal investigation. An organization that maintains data on behalf of the data owner or licensee is required to immediately notify the owner or licensee of a suspected breach.

Notification Format and Delivery Method

The law's provisions are aimed at making notices helpful to recipients. As the notices were seen to be difficult to read and understand and were often lacking key information, the law was amended to require plain language and specific pieces of information that provide what individuals need to know to be able to take appropriate defensive actions:

1) the name and contact information of the notifying organization;
2) the types of personal information involved;
3) contact information for the credit reporting agencies in cases involving a breach of Social Security or driver's license numbers; and
4) the date of the breach, and a general description of the incident (if known at the time of the notification).

Additional information that may be provided in the notice includes what the organization has done to protect individuals and advice on what individuals can do to protect themselves.

Most recently, in 2015, the law was amended to require the use of a format that improves the readability of the notices.

The law has a preference for notification to take the form of a written notice mailed to individuals, but it is flexible in allowing notification by other means in certain situations. When a breach (i) requires notifying more than 500,000 people, or (ii) providing written notice would cost more than $250,000, or (iii) an organization lacks sufficient contact information, the "substitute notice" method may be used. This method requires posting a notice on the organization's website, notifying statewide media, and sending a notice to available email addresses. In a breach of online account credentials, online notification may be used instead of a written or substitute notice, since that is the normal mode of communication between the breached organization and those affected.

Breach Victim Protection

In an effort to help breach victims, an amendment was passed in 2014 that requires organizations to offer identity theft prevention and mitigation services in breaches of Social Security or driver's license numbers. Breaches of these are the types of data put individuals at risk of new credit accounts being opened in their names, among other things, and the required services are intended to address such risks.

Other State Breach Notice Laws

The breach notification laws in the 46 other states are similar in many ways, because most are modeled on the original California law. All of them require notifying individuals when their personal information has been breached, prefer written notification but allow using the "substitute method" in certain situations, allow for a law enforcement delay, and provide an exemption from the requirement to notify when data is encrypted.

There are some differences, primarily in three areas: (i) the notification trigger, (ii) the timing for notification, and (iii) the definition of covered information.

Of the 47 states with breach laws, 36 states (77 percent) use the "harm" trigger for notification, generally allowing an organization to be relieved of its obligation to notify if the organization makes a determination that there is no reasonable risk of harm or misuse of the data. California and 10 other states (23 percent) have a standard of acquisition, or a reasonable belief of acquisition, by an unauthorized person, which can be understood as putting the data at risk of harm.

Most state breach laws (85 percent) have essentially the same notification timing provision as California—in the most expedient time possible, without unreasonable delay. Seven states have an outer boundary time limit for notification of individuals, ranging from 30 to 90 days.

There is a range of definitions of personal information. All state laws include the basic types in the original California law (Social Security number, driver's license number, financial account number). Eight states (17 percent), including California, add medical information, and five (11 percent), including California, add online account credentials. Thirteen states (28 percent), including California, add other types of information, with health insurance information, biometric information, and taxpayer ID being the most common.

In addition, 19 states (40 percent), including California, have specific content requirements for notices. Most require what would logically be included in such a notice: a general description of the breach, the types of personal information involved, what the organization is doing in response, and contact information for the organization and for credit reporting agencies. A few have additional, unique content requirements. For example, the Massachusetts law prohibits disclosing the nature of the breach or the number of residents affected in the notice, and the Wisconsin law requires the notice to tell the recipient to make a written request to learn the personal information involved.

Twenty-five states (53 percent) require a breached organization to notify the state Attorney General and/or another government agency.

Federal Data Breach Proposals

As the number of state laws has grown in recent years, there has been an effort to pass a federal breach notice law that would preempt state laws and set a national uniform standard. The rationale offered has been regulatory simplification and reduction of the burden of complying with the different state laws. The proposals under consideration in Congress, however, have tended to set the consumer protection bar very low. And in many cases they would preempt not only state laws on data breach, but also longstanding information security and consumer protection statutes.

In addition to the overly broad preemptive scope, the federal breach law proposals would infringe on state-based innovation. Over the years, states have proven nimble in responding to rapidly changing circumstances that affect their residents. As discussed earlier, California has made several amendments to the law. Preempting the right of states to make such adjustments in the law would deprive their residents and other jurisdictions of valuable insight and information that can inform timely innovation and adaptation to evolving technology.

Not only would most of the federal proposals lower the level of protection provided below that in states with stronger laws, but residents of other states would lose the benefit they now enjoy from the highest-common-denominator approach many organizations take in multi-state breach responses, in effect affording California-level protections to residents of all states.

The federal proposals tend to use very narrow definitions of harm and of personal information and to set overly rigid timelines for notification. The vast majority of state breach laws have a flexible timing provision, which allows for achieving an appropriate balance. While a specific deadline may be intended to prevent major delay, the outer bound may become the de facto standard for notification. The time needed from discovery to notification is alsovery fact specific. A deadline of 30 or 45 days would be too long in many cases, and might be too short in others. Furthermore, what constitutes a reasonable time for notification today might be unreasonable tomorrow, as technological improvements allow for faster forensic analysis, cheaper and more effectively targeted notice, and an improved ability by companies to quickly provide consumers with remedies.

Many of the federal proposals would also encroach on enforcement by State Attorneys General. Even when allowing enforcement by State Attorneys General, they would do so with restrictions, such as requiring prior notice to federal agencies and enforcement only in federal court. The states have been leaders in privacy protection and have protected their residents from irreparable harm by enforcing state breach laws. Placing such restrictions on State Attorneys General would unnecessarily hamper their ability to protect consumers.

Update on Previous Breach Reports

EMV Developments

In our 2014 data breach report, in the wake of the series of large retailer breaches of payment card data that occurred in 2013, we encouraged the prompt adoption of the improved security offered by chip-enabled payment cards, also known as EMV (named for the three companies that originated the standard: Europay, MasterCard, and Visa). EMV is a replacement for magnetic stripe cards, offering greater security because stolen mag-stripe data can be used to create counterfeit credit cards. EMV creates a one-time code for each transaction, rendering it impossible to use stolen card data to make counterfeit cards for use at the point of sale. The use of counterfeit cards is the most common type of card fraud, responsible for $3 billion, for 45 percent of U.S. card fraud losses in 2014.[6]

In our report, we recommended that retailers move promptly to update their point-of-sale terminals to be able to read chip-enabled cards, particularly in light of the October 2015 "liability shift." Prior to the shift, liability for card fraud among the parties was determined by the card brands (Visa, MasterCard, Discover, and American Express). This shift changed the apportionment of liability to make the party with the lower level of security, that is, the one that has not enabled EMV (retailer or card issuer), liable for the cost of fraud resulting from counterfeit card transactions. Card-issuing banks have upgraded their cards, with 98 percent of total payment cards in the U.S. now bearing chips.[7] Retailers have more work to do in upgrading their terminals to accept cards bearing chips, and the full transition to EMV is not expected to be complete until the end of 2017. In the meantime, until all retailer terminals have been upgraded, the new chip cards still also retain the vulnerable magnetic stripe, so we can continue to expect breaches of payment card data at the point of sale for a few more years, until all retail terminals are chip-enabled and the magnetic stripe can be eliminated from cards.

As EMV migration advances, we also anticipate seeing a shift in breach targets from "brick-and-mortar" stores sale to online merchants, where stolen card data retains value because the full account number is used for purchases. Data other than payment card data will also increasingly be targeted. For example, Javelin Strategy & Research predicts that businesses that store or transmit Social Security numbers will become high-value targets.[8]

Health Care Sector Encryption

In both our previous breach reports, we recommended that the health care sector adopt stronger encryption practices to protect medical information on portable devices and consider it for desktop computers as well. We made this recommendation because we saw

that health care was experiencing a much higher rate of breaches of stolen equipment containing unencrypted data than other sectors. The trend in health care breaches in the past two years suggests some improvement in encryption practices. In 2012, 68 percent of health care breaches were the result of stolen or lost equipment, compared to 21 percent of breaches in all other sectors. In 2015, 39 percent of health care breaches were of this type, while in other sectors it accounted for just 13 percent. There is still a long way to go in addressing this preventable type of breach.

Breach Notices

We also recommended making breach notices easier to understand and strengthening the substitute notice procedure. As previously described, the new addition to California's breach notification law requires breach notices to use a format that will make them easier to understand by prescribing one of two options: (i) use the title "Notice of Data Breach" and the headers "What Happened," "What Information Was Involved," "What We Are Doing," What You Can Do," and "For More Information;" or (ii) use the form provided in the statute. In addition, the law requires organizations to maintain substitute notices posted on their websites for a minimum of 30 days, and it defines conspicuous posting as being linked on the home page, with the link distinguished from the rest of the page by color, size of type, or by symbols that draw attention to it.

Resources for Consumers

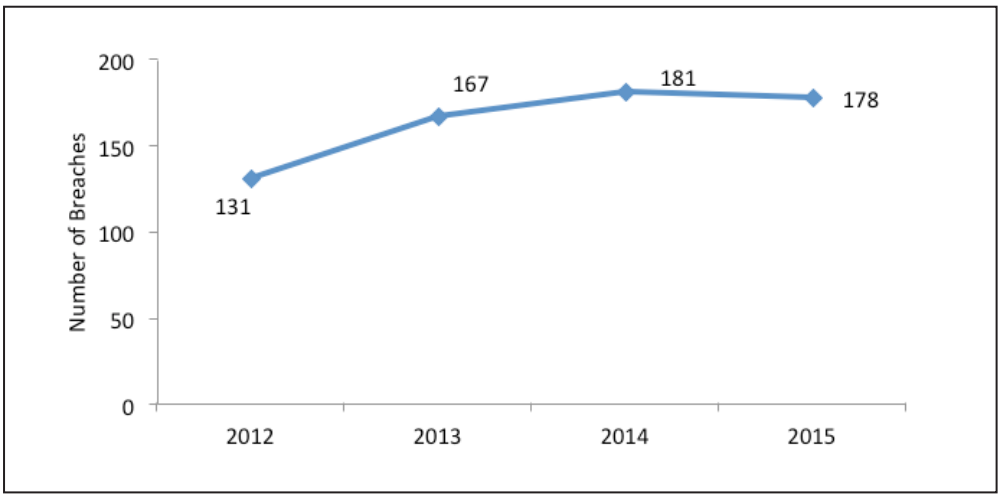
In last year's report, we also commented on the particular risk that debit cardholders face in payment data breaches and the inadequacy of the usual advice given in breach notices to protect against this risk. To address this and to provide appropriate guidance for consumers on breaches of all types of data, we published Breach Help: Consumer Tips from the California Attorney General. This information sheet provides specific advice for different types of data breached. Regarding debit card data, the advice is to monitor the account online, promptly report any unauthorized transaction, and consider cancelling the card as the best way to protect the linked bank account. Breach Help is just one of a broad range of privacy resources for consumers, in English and Spanish, available on the Attorney General's website. For more helpful information, visit *www.oag.ca.gov/privacy.*

Advice on what to do in response to a breach notice is available in Breach Help: Consumer Tips from the California Attorney General, at www.oag.ca.gov/privacy.

Findings

As noted earlier, from 2012 through 2015, the Attorney General received reports of 657 data breaches that involved the personal information of more than 500 California residents. After increasing for the previous two years, the number of breaches remained essentially flat in 2015.

Figure 1: Number oF Breaches, 2012-2015



While the total number of breaches did not increase in the past year, the total number of Californians affected rose dramatically from 4.3 million in 2014 to over 24 million in 2015.

Figure 2: Number oF Records Breached, 2012-2015

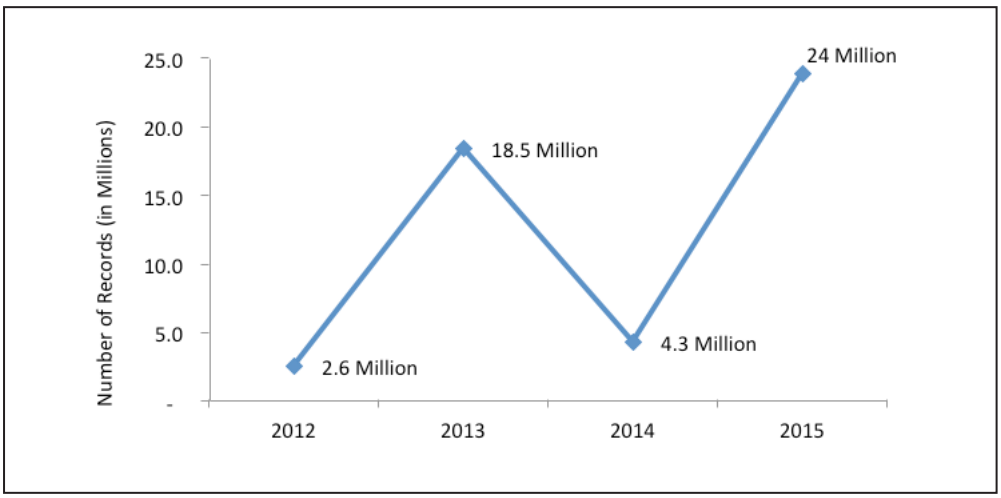
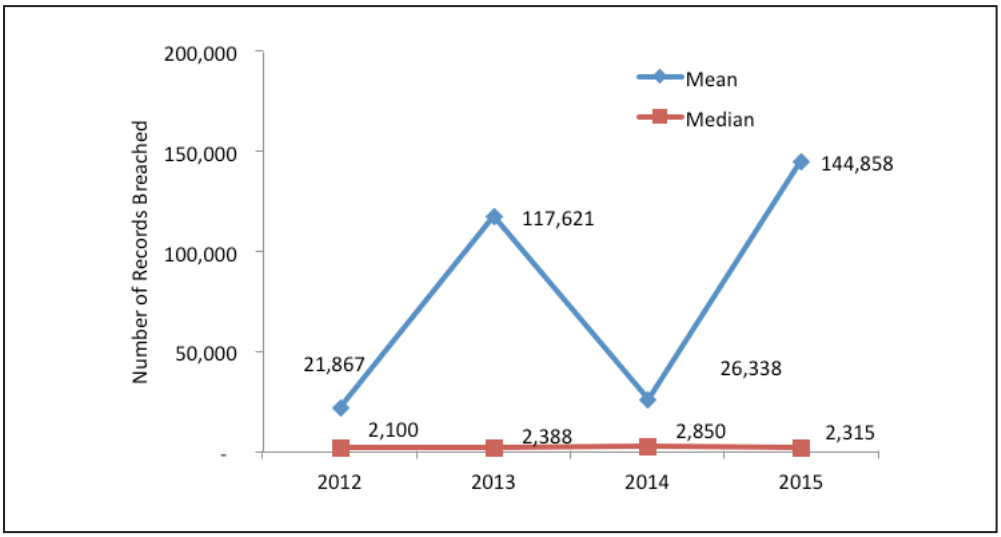


Figure 3 shows the mean and median breach size by year. While the median breach size has been fairly steady at between 2,000 and 3,000 records, the mean was much higher in 2013 and 2015, due to a few larger breaches.

Figure 3: Mean and Median Breach Size, 2012-2015



The jump in size from 2012 to 2013, as discussed in our last breach report, is attributable to two very large breaches at two retailers, LivingSocial and Target, each involving the information of approximately 7.5 million Californians. This explains the considerable difference between the mean (average) breach size in 2013 of 117,621 and the median of 2,388. If the two outliers were omitted, the total number affected for 2013 would have been 3.5 million instead of 18.5 million with a mean of 21,000. In 2014, the largest reported breach, at Shutterfly, affected just under one million Californians.

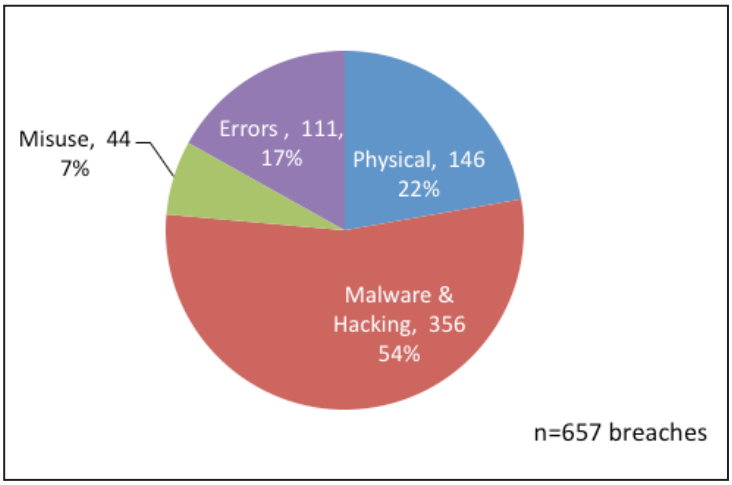
Breaches reported in 2015 account for half of the over 49 million Californians affected in the past four years. In 2015, there were four incidents that each breached the information of over two million Californians: Anthem at 10.4 million was the largest, followed by UCLA Health at 4.5 million, next was PNI Digital Media with 2.7 million Californian customers of online photo centers (Costco, RiteAid, and CVS) that it services, and finally, T-Mobile/Experian at 2.1 million.

Breach Types

As in previous reports, we categorize breaches by type, as seen in Figure 4 below.[9]

- *Malware and hacking breaches* are caused by intentional intrusions into computer systems by unauthorized outsiders.
- *Physical breaches* result from the theft or loss of unencrypted data stored on laptops, desktop computers, hard drives, USB drives, data tapes or paper documents.
- *Error breaches* stem from anything insiders (employees or service providers) unintentionally do or leave undone that exposes personal information to unauthorized individuals.
- *Misuse breaches* are the result of trusted insiders intentionally using privileges in unauthorized ways.

Figure 4: Breaches by Type, 2012-2015



Malware and Hacking

More than half of the reported breaches in the past four years are categorized as malware and hacking. This type has accounted for the largest share of breaches every year. This type of breach affected over 44 million records, 90 percent of all records breached. The six biggest breaches are all of this type and together comprise over 70 percent of all records breached. See Figure 5.

Figure 5: Mean and Median Breach Size, 2012-2015

Anthem, Inc.	10.4 million	2015
Target	7.5 million	2013
Living Social	7.5 million	2013
UCLA Health	4.5 million	2015
PNI Digital Media (Costco/RiteAid/CVS)	2.8 million	2015
T-Mobile USA, Inc. (Experian)	2.1 million	2015

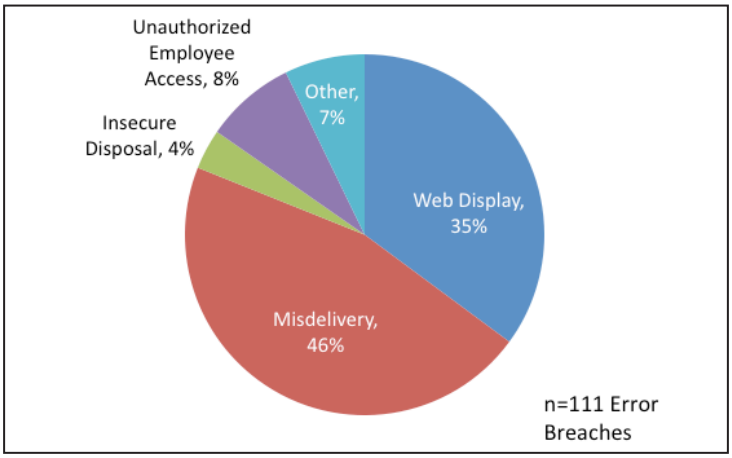
Physical Theft and Loss

Breaches resulting from physical theft and loss are the next largest segment, accounting for 22 percent of all breaches from 2012 to 2015. Physical breaches accounted for 2.8 million records, or six percent of all records of Californians breached.

Miscellaneous Errors

Breaches resulting from errors by insiders (employees, service providers) made up 17 percent of total breaches and four percent (two million) of total records breached. As shown in Figure 6, misdelivery of personal information to an unintended recipient, whether by email, postal mail, fax, or other means, was the most common type of error. It comprised 46 percent of the error breaches and eight percent of all breaches, was. The next most common type of error breach is the unintentional posting of information on a public website,

Figure 6: Error Breaches by Type of Error, 2012-2015



making up 35 percent of error breaches and six percent of all breaches. Other errors that account for the remaining breaches of this type include failing to shred documents or "wipe" digital data from devices when discarding them, and allowing unauthorized employees to have access to data.

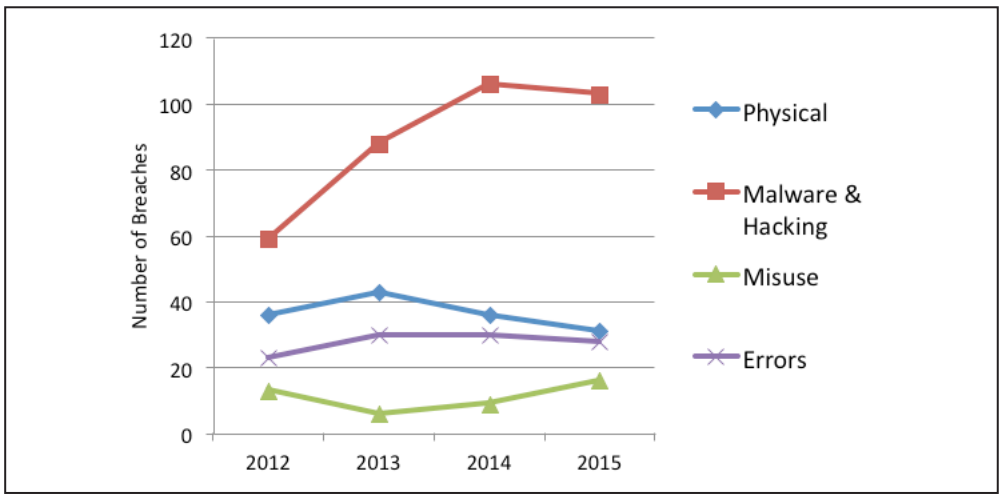
Misuse

Misuse of access privileges by insiders accounted for the smallest share of breaches, at seven percent. This type of breach put over 206,000 records of Californians at risk, representing less than one percent of total records breached.

Key Trends in Breach Types

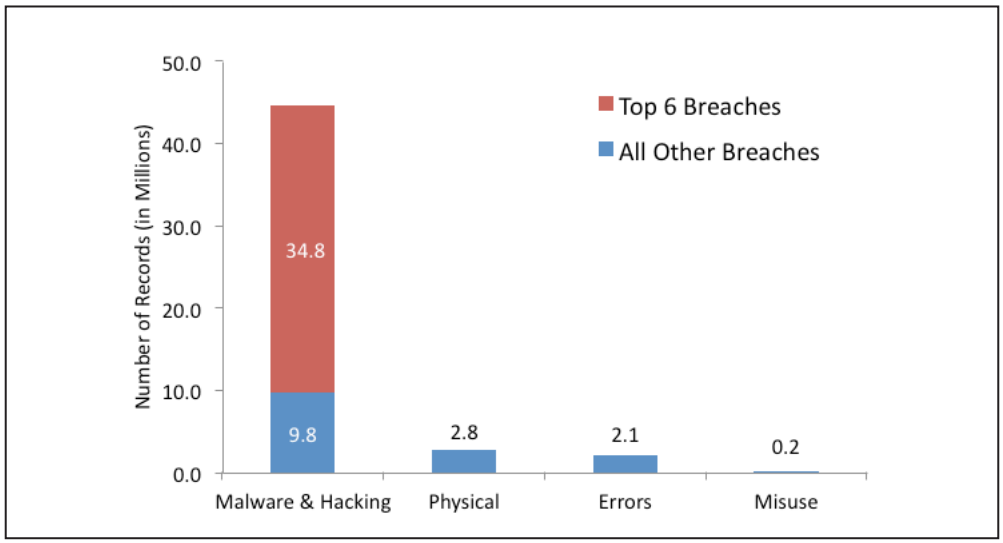
As seen in Figure 7, the incidence of malware and hacking breaches has trended generally up, almost doubling from 2012 to 2015. At the same time, the share of breaches resulting from physical loss and theft has gone down, from 27 percent of breaches in 2012 to 17 percent in 2015. This may reflect a more widespread and effective use of encryption to protect data in transit.

Figure 7: Type of Breach by Year, 2012-2015



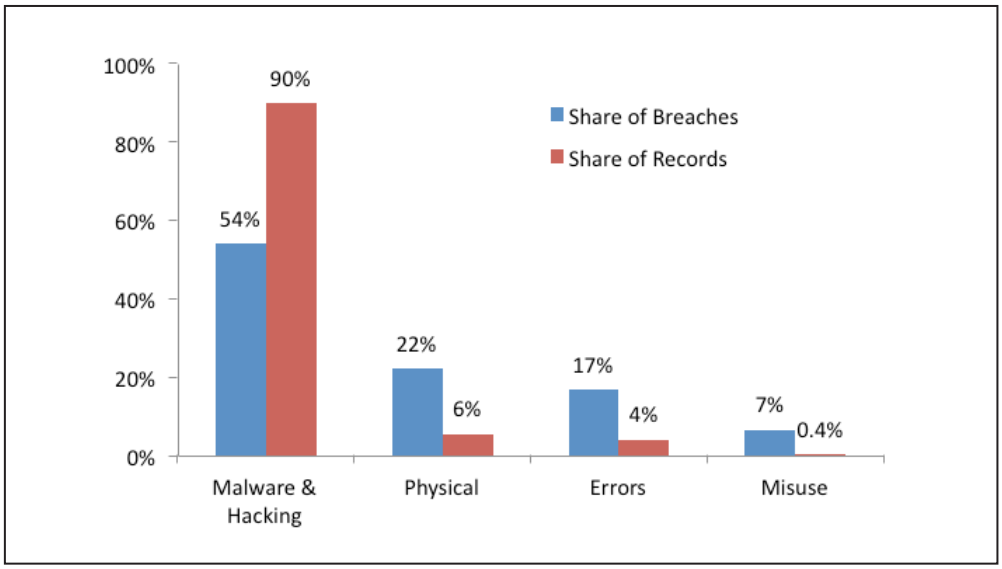
As Figure 8 shows, the biggest breaches by far were the result of malware and hacking. Physical breaches came in a distant second, accounting for six percent of records, followed by error breaches at four percent, and breaches resulting from intentional misuse by insiders at under one percent.

Figure 8: Type of Breach by Number of Records Breached, 2012-2015



Malware and hacking were the major threat in both share of breaches (54 percent) and share of records breached (90 percent), as shown in Figure 9. While physical breaches were the next most common type, at 22 percent, they tend to be smaller than malware and hacking breaches, accounting for just six percent of total records breached. Breaches caused by insiders, whether from unintentional errors or intentional misuse, are also smaller.

Figure 9: Type of Breach by Share of Breaches and Records, 2012-2015



Data Types

The types of data covered by California's breach law are (i) name, plus Social Security number, driver's license number, financial account number (such as bank account numbers and payment card numbers), medical information, or health insurance information; and (ii) credentials for online accounts (user ID or email address, plus password or security question and answer).[10]

Social Security numbers are among the most sensitive data types, because their abuse is the most difficult type of fraud for consumers to detect, protect against, and recover from. When a single credit or debit card account number is stolen, the victim can discover it in the next bill (if not earlier) and can stop the fraud by closing the account. It is a different story for stolen Social Security numbers. In the hands of identity thieves, Social Security numbers, and to a lesser extent driver's license numbers, can be used for a variety of purposes. They enable thieves to open new credit accounts, take out loans, apply for and receive government benefits, among other things – all in the victim's name. They can also be used for other fraudulent purposes, including taking over existing bank accounts and getting health care or government benefits. Criminals have provided stolen Social Security numbers when arrested, resulting in the creation of fraudulent criminal records in the victim's name. Such uses can take months or sometimes years to detect. Even when detected, undoing the damage can be very challenging because it is almost never possible to change

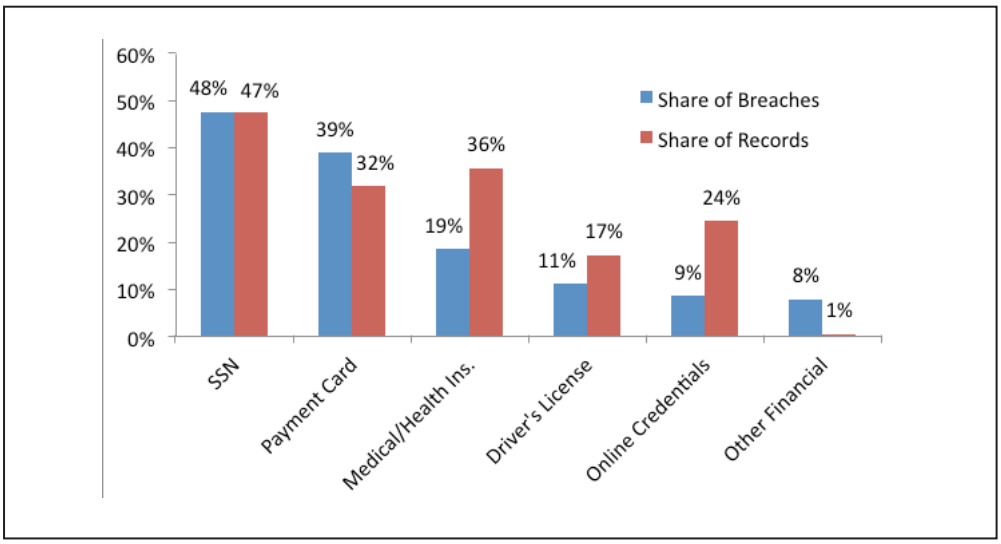
your Social Security number. So while the identified fraud may be repaired, the stolen number remains useful to criminals, who can re-victimize individuals repeatedly for years.

Social Security numbers continue to figure significantly in data breaches, and were involved in nearly half (48 percent) of all breaches and in 47 percent of records breached, as shown in Figure 10. Over 18 million Social Security numbers were breached in 2015, primarily in the large incidents at Anthem, UCLA Health, and T-Mobile/Experian. There has been a slow decline in the incidence of Social Security number breaches in the past four years. In 2012, 56 percent of breaches involved Social Security numbers and in each subsequent year this percentage decreased, comprising 43 percent of all breaches in 2015. As noted in the discussion of EMV developments, however, this may rise again in the coming years.

Payment card data was the next mostly likely data type to be breached, and was involved in 39 percent of all breaches. Medical or health insurance information, which most individuals regard as very sensitive, comprised a larger share of records breached, 36 percent compared to 32 percent for payment data.

Driver's license numbers figured in 11 percent of breaches and 17 percent of records breached. Online account credentials, a data type that was added to the breach law in 2014, were involved in nine percent of breaches. The higher incidence of this data type in records breached, 24 percent, is largely attributable to the big LivingSocial breach in 2013 and the PNI Digital (Costco, RiteAid, CVS) breach in 2015.

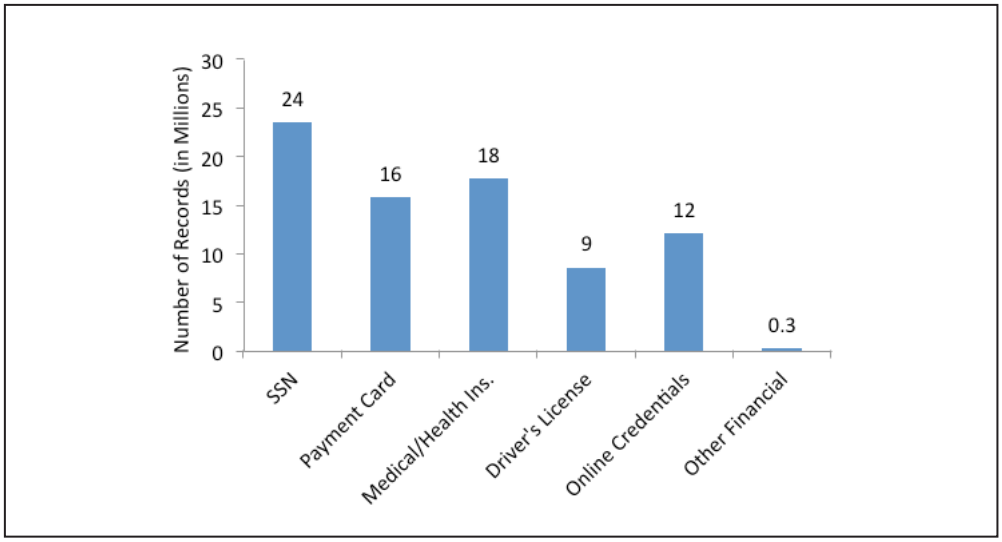
Figure 10: Type of Data by Share of Breaches and Records, 2012-2015



Note: Total is greater than 100% because some breaches involved more than one data type.

Looking at the raw numbers, we see that records containing the most sensitive information were breached in larger quantities: 24 million records containing Social Security numbers and nearly 18 million containing medical or health insurance information, as shown in Figure 11. Payment card data is next, in nearly 16 million breached records. More than 12 million breached records included online account credentials.

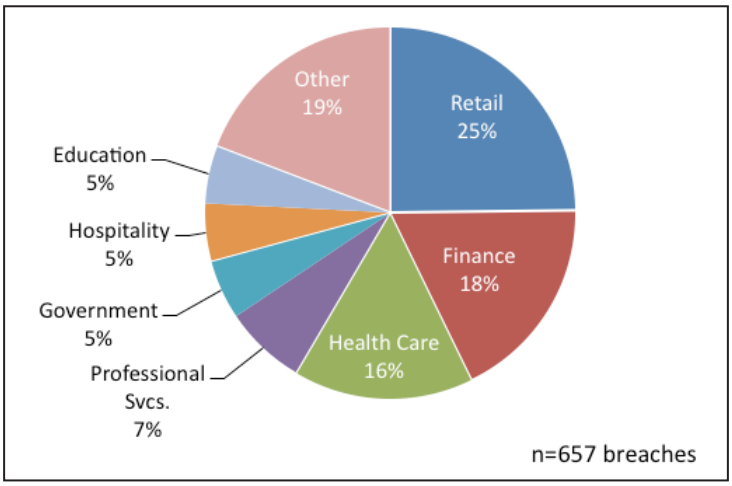
Figure 11: Number of Records Breached by Data Type, 2012-2015



Industry Sectors

We classify the organizations that report breaches to the Attorney General according to the U.S. Census Bureau's North American Industry Classification System.[11] As shown in Figure 12, the retail industry has seen the largest share of breaches throughout the four-year period, averaging 25 percent of all the breaches in our dataset. The finance sector, which includes insurance, represented 18 percent of the breaches and health care a similar 16 percent. Professional services accounted for seven percent, and government, hospitality, and education five percent each. All other sectors made up 19 percent of total breaches, although none of them accounted for more than 4 percent.

Figure 12: Breaches by Industry Sector, 2012-2015



The large size of many of the retail breaches from 2012 to 2015 is evident in Figure 13 as the sector's share of breaches is only 25 percent but its share of records breached is 42 percent (21 million records). The financial sector, which includes insurance, also had disproportionately larger breaches, with 18 percent of total breaches but 26 percent of all records. The large Anthem breach in 2015 is a major driver here; without that breach, finance's total share of all records would drop to six percent. The health care sector's share of records breached (14 percent) is slightly less than its share of breaches (16 percent).

Figure 13: Breaches and Records Breached Industry Sector, 2012-2015

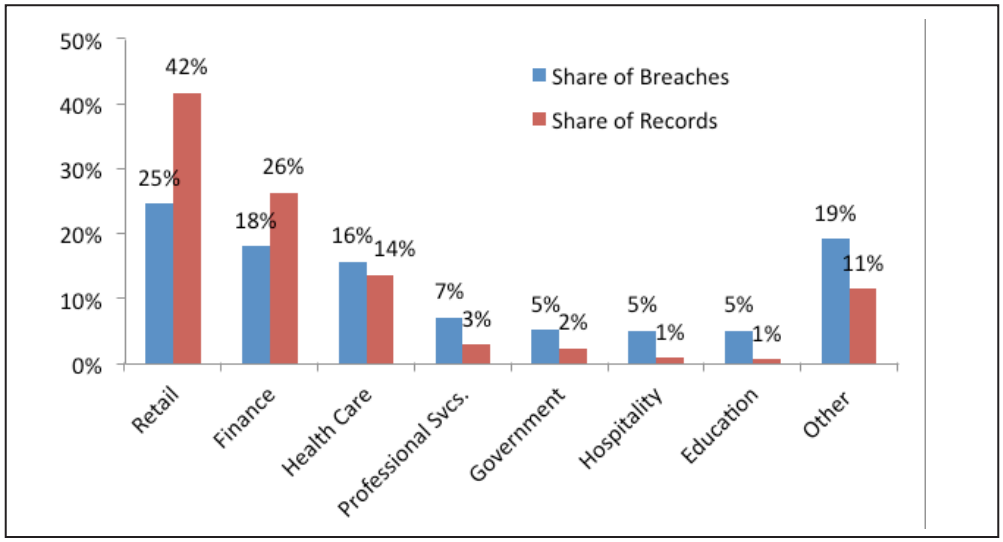


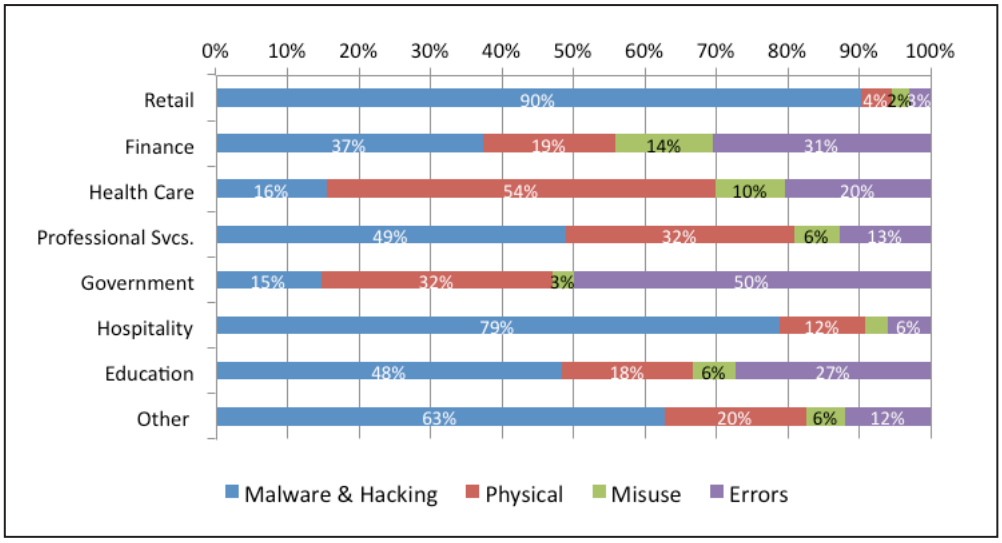
Figure 14 shows the types of breach that occurred within each industry sector. While malware and hacking was the dominant type of breach (54 percent), it did not dominate all sectors. This type accounted for nearly all breaches in the retail sector (90 percent) and for a significant share of breaches in most other sectors. The exceptions are health care and government, where only 16 percent of breaches were of this type.

The incidence of physical breaches also differed across sectors. Over the four years, these incidents of stolen or lost documents or digital devices containing unencrypted data accounted for 22 percent of all breaches, but make up 54 percent of the breaches in health care. Professional services and government also experienced a significant rate of this type of breach, at 32 percent each.

Error breaches were most common in the government and finance sectors, at 50 and 31 percent, respectively.

Breaches resulting from intentional misuse by insiders were a small share in every sector, with only finance and health care seeing a double digit incidence, at 14 and 10 percent, respectively.

Figure 14: Industry Sectors by Breach Type, 2012-2015

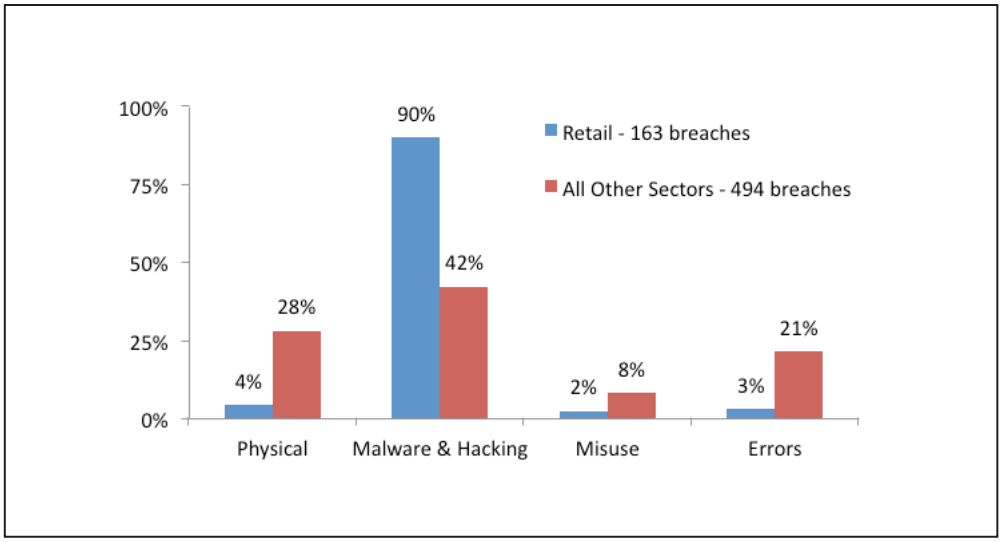


We took a closer look at the three largest industry sectors: retail, finance, and health care because together they represented just under 60 percent of all breaches and over 80 percent of records breached. The three sectors have notably different profiles, differing both by type of breach and by type of data involved.

Retail Sector Breaches

There were 163 retail breaches in the four-year period, constituting 25 percent of all breaches, and 90 percent of them were caused by malware and hacking. This is more than twice the rate of other sectors for this type of breach, as shown in Figure 15.

Figure 15: Retail Sector vs. all Others by Type of Breach, 2012-2015



The retail sector breaches were also the largest – involving 21 million records of Californians, 42 percent of the total of over 49 million. Two of the largest breaches were at retailers, Target and LivingSocial, together accounting for 15 million of the records breached.

Most of the retail breaches (83 percent) involved payment card data, with 10 percent (including the LivingSocial breach) involving online account credentials, and 7 percent Social Security numbers.

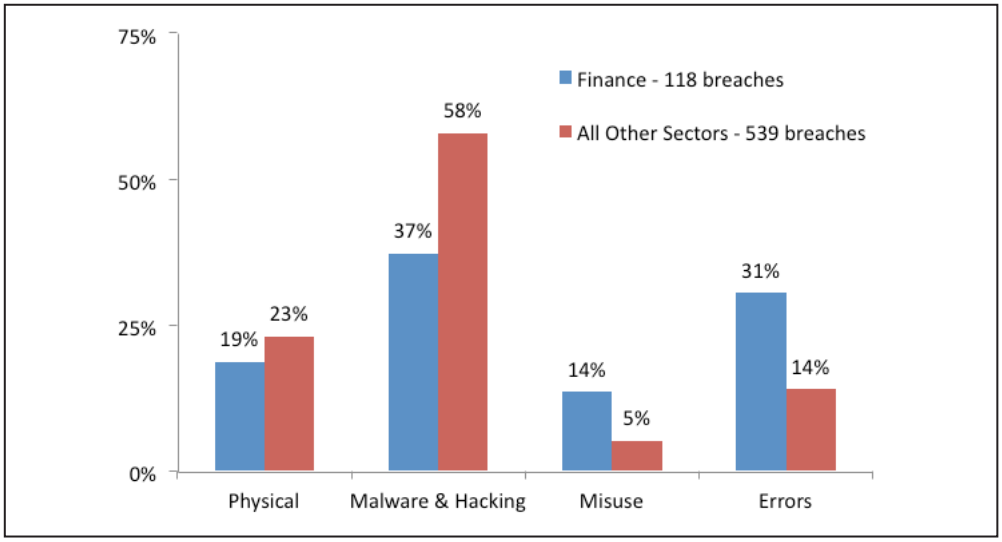
Financial Sector Breaches

The financial sector, which also includes insurance, accounted for 18 percent (118) of the breaches and 26 percent of the records breached (13 million records). It has a notably different breach profile than retail. As shown in Figure 16, the sector had a significantly lower incidence of hacking and malware – the dominant type of breach – compared to all other sectors (37 percent of its total compared to 58 percent), and just over one third

the incidence of hacking and malware breaches as retail. Breaches resulting from errors by insiders, however, were more than twice as common as in other sectors (31 percent versus 14 percent). The financial sector also experienced nearly three times the share of breaches caused by insiders abusing their access privileges: 14 percent compared to five percent in all others.

The type of data most commonly involved was Social Security numbers, which figured in 75 percent of financial sector breaches.

Figure 16: Financial Sector vs. all Others by Type of Breach, 2012-2015

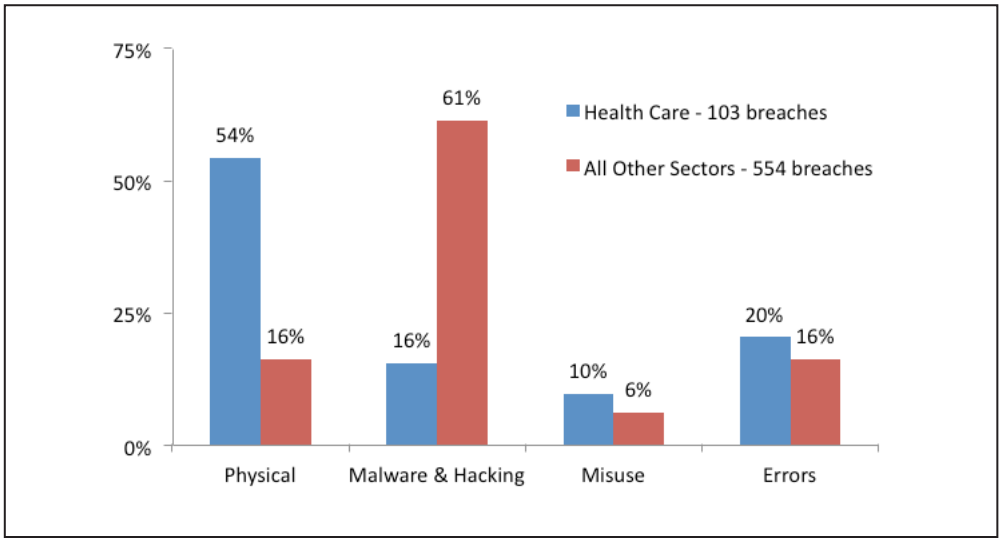


Health Care Sector Breaches

The health care sector accounted for 16 percent of breaches (103) and 14 percent (6.8 million) of Californians' records breached over the four years.

As we have noted in previous reports, the health care sector differs from the others in having a significantly higher incidence of breaches resulting from physical theft and loss: 54 percent compared to just 16 percent in all other sectors. See Figure 17.

Figure 17: Health Care Sector vs. all Others by Type of Breach, 2012-2015



Physical breaches have declined in health care in the past two years, from a high in 2013 of 72 percent of all health care breaches compared to 18 percent in all other sectors, to 39 percent in 2015, compared to 13 percent in other sectors. The industry appears to be improving in its use of encryption to protect data on laptops and other portable devices, but there is still a long way to go in addressing this preventable type of breach.

At the same time, the incidence of malware and hacking breaches in health care has been rising, from five percent in 2012 to 21 percent in 2015. As the transition to electronic medical records continues, the health care sector will increasingly face the same challenges in securing digital data that other sectors have been grappling with for several years. Given the extreme sensitivity of the data involved in health care breaches, this is a challenge that the industry must meet.

Health care breaches tend to involve the most sensitive types of personal information. Social Security numbers figure in 50 percent of health care breaches, and medical information in 69 percent.

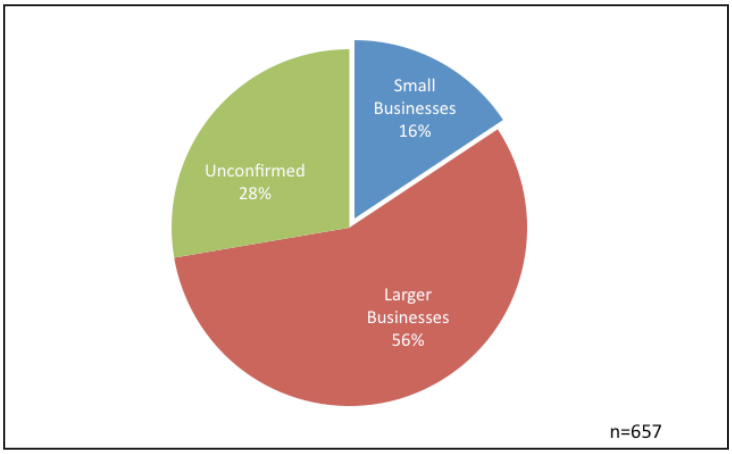
Small Businesses

In order to see whether the experience of small businesses with data breach is different from that of larger businesses, we used the Small Business Administration's size standards to identify the small businesses in our dataset.[12] While there are differences for different

industry sectors and revenues are also a factor, small businesses are generally those with fewer than 500 employees. Government agencies and non-profit organizations are not covered by the SBA standards, and we were not able to confirm the status of some businesses. We distinguished three groups by size: (i) known small businesses; (ii) known larger businesses; and (iii) government agencies, non-profits, and businesses of unconfirmed size.

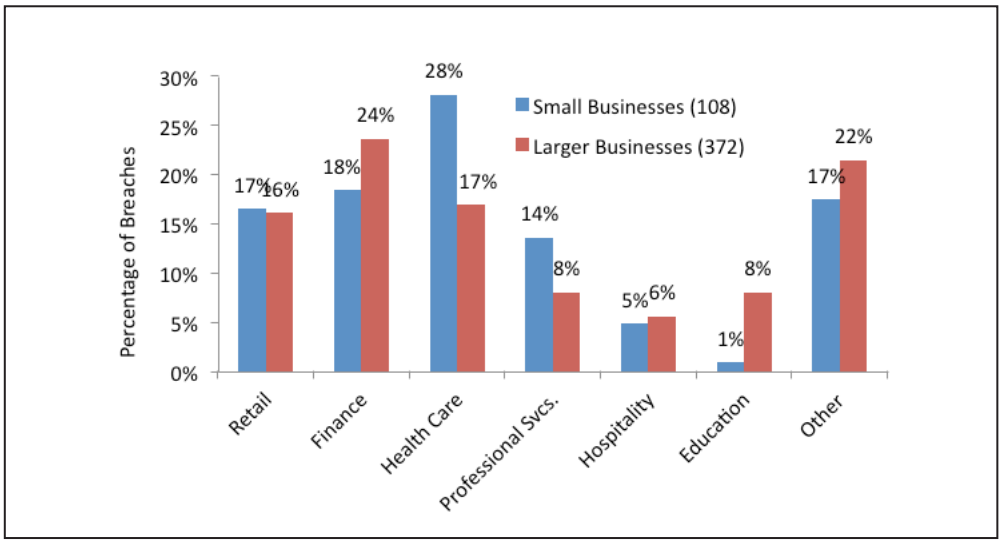
As shown in Figure 18, 16 percent of the organizations in our dataset are confirmed as small businesses and 56 percent as larger, or non-small, businesses. The share of small businesses increased over the four years, from 12 percent in 2012 to 17 percent in 2015. This may indicate that hackers are increasingly also targeting more vulnerable small businesses, given they often have fewer resources to dedicate to security, and/or it may reflect a growing awareness among small businesses of the requirement to notify the Attorney General of data breaches, which became law in 2012.

Figure 18: Breaches by Size of Business, 2012-2015



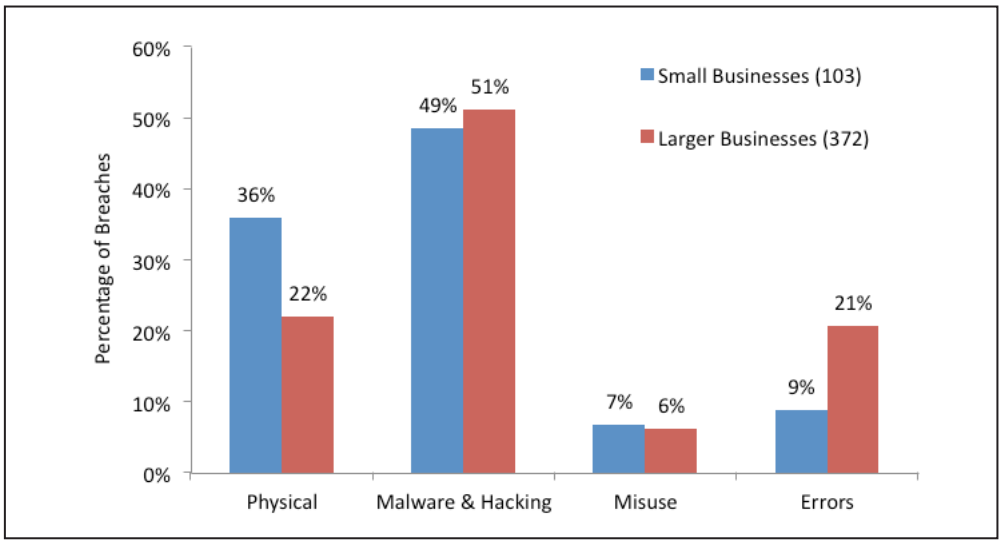
Small businesses differed from larger businesses in having a smaller share of financial sector entities and larger shares of health care and professional services. As shown in Figure 19, 18 percent of the small businesses in our dataset were financial, compared to 24 percent of larger businesses. On the other hand, 28 percent of small businesses were in health care, compared to 17 percent of larger businesses, and 14 percent were in professional services, compared to eight percent for larger entities.

Figure 19: Industry Sector by Size of Business, 2012-2015



We found that small businesses were more likely to have breaches resulting from physical theft and loss, as shown in Figure 20. This may be attributable to some extent to the industry makeup of the group. Small businesses show a larger representation of health care and professional services, both sectors that experience physical breaches at a higher rate than other sectors.

Figure 20: Type of Breach by Size of Business, 2012-2015



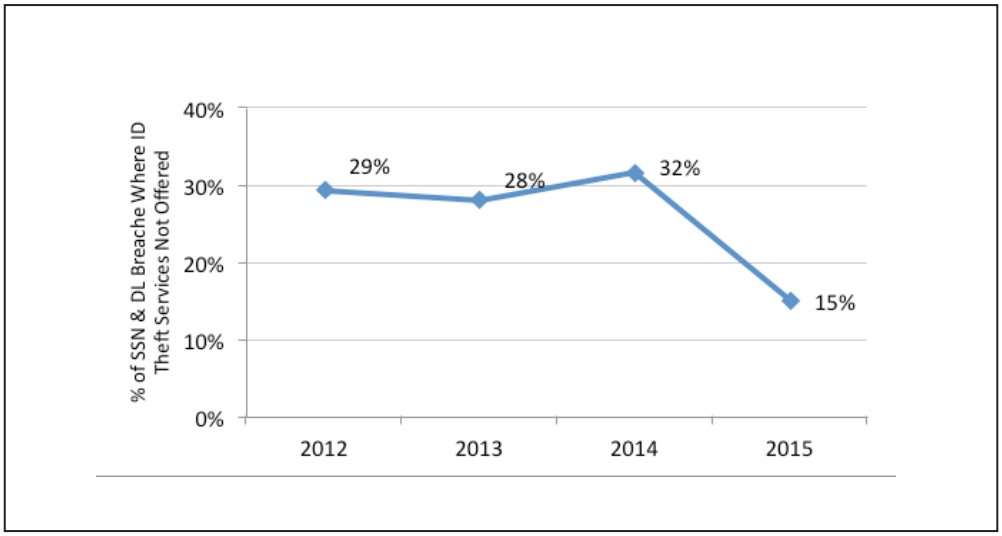
Not surprisingly, small businesses had smaller breaches, involving a total of just over one million records, compared to 46 million for larger businesses. The mean (average) small business breach involved 9,850 records, compared to 123,704 for larger businesses.

Additional Findings

Identity Theft Prevention and Mitigation Services

The new breach law requirement that companies must offer identity theft services to victims in certain breaches appears to be having an impact. From 2012 through 2014, organizations did not provide such services in 30 percent of breaches of Social Security or driver's license numbers. As shown in Figure 21, when the law took effect in 2015, the failure rate dropped to half that, 15 percent.

Figure 21: Social Security & Driver's License Number Breaches Where Identitiy Theft Prevention Services Not Offered, 2012-2015



Timing of Notification

The law requires notifying individuals of a breach "in the most expedient time possible and without unreasonable delay." The average (mean) time from discovery of a breach to notification of those affected was 40 days, and the median was 30 days. In 25 percent of the breaches consumers were notified in 16 days or less, and in 75 percent of them notification was made in 50 days or less. The time from discovery to notifying the Attorney General was similar, 44 days on average, with a median time of 31 days. These figures are for the 73 percent of breaches for which we have the date of discovery.

Substitute Notice

Organizations in nearly all of the 657 breaches reported provided notice by mail directly to individuals; the substitute notice method was used in 33 breaches (five percent). In those instances, organizations delivered the notice via websites, the news media, and sometimes also email. Retailers accounted for 12 of the substitute notices, restaurants and hotels for 12, with the others from a variety of sectors. All but three of the substitute notices were for breaches of payment card data, where the method was likely used because of insufficient contact information to permit direct written notices. The other three involved online account credentials.

Notification of Law Enforcement

Organizations report having notified law enforcement in 62 percent of breaches (340), and filing a police report in 26 percent (172). All state laws allow for a delay in notification if law enforcement says notifying would impede an investigation. The use of such a delay was reported in just seven percent (44) of the breaches in our dataset. The average time to notify those affected in such cases was 60 days, compared to 40 days when there was no law enforcement delay.

Repeaters

Over the four years, 24 organizations reported two data breaches. There were five organizations that reported three (California Correctional Health Care Services, California Department of Public Health, HSBC Bank, St. Joseph Health System, Yolo Federal Credit Union), one that reported four (California Department of Corrections and Rehabilitation), and two that reported five (Kaiser and Massachusetts Mutual Life Insurance Company). This does not include card-issuing financial institutions such as American Express and Discover that notified their cardholders of payment data breaches that occurred at merchants.

Recommendations

In reviewing four years of data breaches, we have seen certain patterns that suggest lessons to be learned. We offer these recommendations to organizations as part of the collective effort to improve privacy and security practices and reduce the number, size, and impact of data breaches. The first recommendation concerns a *minimum* standard of care for personal information. The next three recommendations encourage organizations to adopt specific practices that can help consumers, by reducing the risk of a breach and/or mitigating the impact when breaches do occur. The final recommendation addresses the proliferation of state breach laws and proposed federal legislation.

Limiting the personal information collected and retained can provide the strongest protection.

(1) Reasonable Security: The Standard of Care for Personal Information

As data breaches continue and the stakes increase, organizations must be vigilant and proactive to ensure more effective protection for personal information and other critical data. This starts with basic privacy practices. Limiting the personal information collected and retained can provide the strongest protection; if an organization does not have data, the data cannot be breached. But good privacy practices are also reliant on a foundation of good security: an organization cannot protect people's privacy without being able to secure their information from unauthorized access.

Security is challenging.

Securing information in the online world is very challenging. The adversaries are sophisticated. Large criminal enterprises, including transnational organizations and even nation-states, are engaged in attacking our information assets and stealing data. Their motivations are varied, running the gamut from financial gain, to corporate espionage, business disruption, and even cyber warfare. Cyber threats are constantly evolving, and the fight is asymmetrical, with organizations having to protect their systems against everything all the time, while an attacker only has to be successful once.

There are also internal challenges, both technological and human. Organizational information assets and data have become widely distributed in multiple locations, including outside the organization's physical control (e.g., in the cloud and on the hand-held devices of employees and vendors). This exposure is exacerbated by an emerging data-driven business model, where organizations are amassing huge quantities of information and retaining it for possible future use, sometimes indefinitely. In addition, employees and vendors can be careless in their handling of personal information or are able to intentionally steal information by taking advantage of security holes.

Furthermore, security solutions are complex, requiring integrating technology with processes to ensure that the technology is properly deployed and used. For example, some breaches of retail point-of-sale systems have resulted from installation errors by equipment installers, even though the technology itself was not faulty.

Security is a responsibility.

While there is no perfect security, organizations have a responsibility to protect personal information. External adversaries cause most data breaches, but this does not mean that organizations are solely victims; they are also stewards of the data they collect and maintain. People entrust businesses and other organizations with their data on the understanding that the organizations have a both an ethical and a legal obligation to protect it from unauthorized access.

Neglecting to secure systems and data opens a gateway for attackers, who take advantage of uncontrolled vulnerabilities. In its annual *Data Breach Investigations Reports,* Verizon has regularly pointed out that 99.9 percent of exploited vulnerabilities were compromised more than a year after the controls for the vulnerability had been publicly available.[13] If organizations choose to amass data, and then fail to uphold their responsibilities as data stewards, they are also culpable.

The legal obligation to secure information is contained in an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes.[14] California has an information security statute (California Civil Code § 1798.81.5) that requires all businesses that collect personal information on California residents to use "reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction use, modification, or disclosure."[15]

There are major federal information security laws and related regulations, including the Gramm Leach Bliley Act (GLBA) for the financial services industry, the Health Insurance Portability and Accountability Act (HIPAA) for health care entities and their business associates, and the Federal Information Security Management Act (FISMA) for federal agencies.[16]

Just like California law, the federal legal regimes invoke a concept of providing "reasonable" and/or "appropriate" information security in order to fulfill an organization's responsibilities.

Regulators have also offered security guidance. The Federal Trade Commission has drawn lessons from more than 50 of its security enforcement actions to develop a best practices guide entitled *Start with Security: A Guide for Business.* The Federal Communications Commission developed tips for smaller organizations which it published in *Cybersecurity*

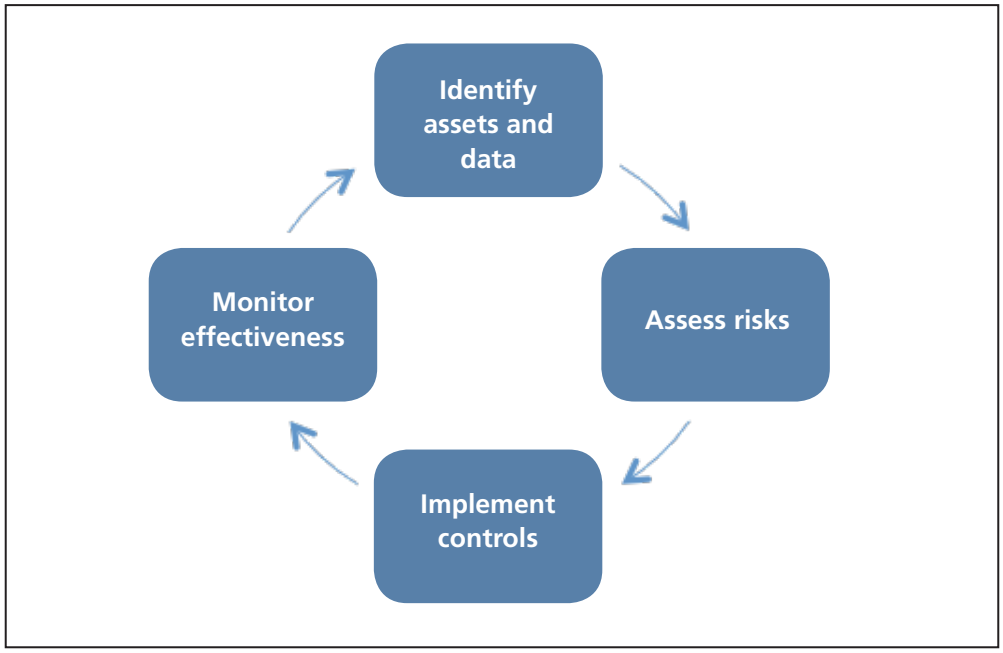
for Small Business. The California Attorney General has provided recommendations on how smaller businesses can reduce their risk of cyber security incidents in *Cybersecurity in the Golden State.*

Security is a process.

Information security laws and regulations generally require a risk management approach. In essence, this means organizations must develop, implement, monitor, and regularly update a comprehensive information security program. The required security risk management process generally includes the same basic steps, starting with assigning responsibility for information security within the organization, and continuing as follows:

1) **Identify** information assets and data to be secured.
2) **Assess** risks to the assets and data.
3) **Implement** technical, administrative, and physical controls to address identified risks.
4) **Monitor effectiveness** of controls and update as risks, business practices, and controls evolve.

Figure 22: Security Risk Management Process



Security is based on standards.
The risk management process will only achieve reasonable security if the risks to information assets and data are identified and effective security controls are implemented. That's where standards come in. Security standards define the scope of security controls, the criteria for evaluating their effectiveness, the techniques for ongoing assessment and monitoring, and the procedures for dealing with security failures.[17]

There are a number of authoritative information security standards that organizations can and do use to develop their programs. These standards are updated periodically and are aligned on the basic security process and the defensive controls to be implemented. Among the best known standards are those published by the National Institute of Standards and Technology (NIST), in particular *Special Publication 800-53* and the *Framework for Improving Critical Infrastructure Cybersecurity*.[18] The International Organization for Standardization's *ISO/IEC 27002:2013* is also foundational.[19] In addition to the comprehensive technical standards, there are catalogs and lists of known security vulnerabilities.[20]

While there is no dearth of information on the security risk management process and standards for security controls, synthesizing all of this information and prioritizing the actions to take can be a challenge. The Center for Internet Security's *Critical Security Controls for Effective Cyber Defense* (the Controls) is designed to address this challenge.[21]

Recommendation 1:
The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.

Formerly known as the SANS Top 20, the Controls are now managed by the Center for Internet Security (CIS), a non-profit organization that promotes cybersecurity readiness and response by identifying, developing, and validating best practices.[22] The Controls were originally developed by federal agencies in 2008 and since then have been the product of a public-private partnership that includes cyber security experts from government and the private sector in the U.S., as well as around the world.

Informed by lessons learned from actual attacks and breaches, the Controls are a consensus list of the best defensive controls to detect, prevent, respond to, and mitigate damage from cyber attacks. They are updated periodically to keep up with technological advances

and changing threats, and are aligned with the most authoritative comprehensive security standards and legal requirements. (See Appendix B.)[23]

Overview of the CIS Critical Security Controls

The Controls are a recommended set of 20 security measures with a high payoff; they are the priority actions that should be taken as the starting point of a comprehensive program to provide reasonable security. In a SANS report on adoption and implementation of the Controls, they are described as providing "the prioritized guidance that cost-conscious executives are looking for when determining where best to invest their limited technology budgets." Adopters also reported valuing the Controls for providing a clear way to present and manage progress on security and risk posture.[24]

Implementing the Controls will not prevent every attack, but it will significantly reduce the risk and impact of the commonly occurring breaches we have seen in the past several years. The set of 20 Controls constitutes a minimum level of security – a floor – that any organization that collects or maintains personal information should meet.

The Controls are listed in priority order, and they act in concert. For example, in order to be able to protect data on laptops and other portable devices (the twelfth Control, called CSC 12), an organization must first know what devices it has and where they are (CSC 1).

The Center for Internet Security provides specific guidance and resources for implementing the Controls. Each Control is presented with an explanation of why it is critical, followed by specific actions (sub-controls), and by procedures and tools for implementing it. A set of tools for implementing the first five controls, which are the first steps to take, has been developed specifically for small organizations.[25]

The controls are intended to apply to organizations of all sizes and are designed to be implementable and scalable. The depth and complexity of the specific actions (called sub-controls) are greater for larger entities and for entities that maintain highly sensitive personal information. Organizations can implement the controls by adopting the sub-controls that fit the size, complexity, and criticality of their systems, as well as the nature of their data. For example, while a small business might take an inventory of its computers and other devices with a manual count, a larger organization could use an automated process to identify the equipment connected to its network.

The following table summarizes the Controls, grouped by the type of action they feature. The complete list of Controls is found in Appendix A.

Count Connections	Know the hardware and software connected to your network. (CSC 1, CSC 2)
Configure Securely	Implement key security settings. (CSC 3, CSC 11)
Control Users	Limit user and administrator privileges. (CSC 5, CSC 14)
Update Continuously	Continuously assess vulnerabilities and patch holes to stay current. (CSC 4)
Protect Key Assets	Secure critical assets and attack vectors. (CSC 7, CSC 10, CSC 13)
Implement Defenses	Defend against malware and boundary intrusions. (CSC 8, CSC 12)
Block Access	Block vulnerable access points. (CSC 9, CSC 15, CSC 18)
Train Staff	Provide security training to employees and vendors with access. (CSC 17)
Monitor Activity	Monitor accounts and network audit logs. (CSC 6, CSC 16)
Test and Plan Response	Conduct tests of your defenses and be prepared to respond promptly and effectively to security incidents. (CSC 19, CSC 20)

Our review of the 657 data breaches reported to the Attorney General in the past four years suggests that many could have been prevented or at least detected and corrected more rapidly had the basic security measures in the Controls been implemented.

Malware and Hacking Breaches

More than half the breaches in our dataset were the result of malware and hacking, the intentional unauthorized intrusion into computer systems by outsiders. As previously noted, breaches of this type were responsible for 90 percent of the records put at risk, affecting nearly 45 million California residents.

There are multiple vulnerabilities that can enable this type of breach. One is the role of insiders in responding to social engineering. One such exploit, phishing, has been recognized as a key delivery vector for malware for several years. Employees are tricked into clicking on a link in a phishing email that downloads malicious software. Verizon reports that 23 percent of recipients now open phishing emails and 11 percent click on the attachments.[26] Phishing is also used to trick employees into giving up their credentials, allowing attackers to steal data from their computers. Thieves use personal information gleaned from social media and other sources to identify insiders with administrative access privileges, targeting them for spear-phishing to get their credentials or posing as them to get access to critical systems.

There are security controls that address this vulnerability. Training employees to recognize phishing attacks is, of course, vital (CSC 17). Limiting administrative privileges to a strict job-required basis reduces the number of "super-user" employees who can be spear-phished (CSC 5).

In addition, strong authentication is a control that protects against the use of stolen credentials (CSC 5, CSC 7). Multi-factor or multi-channel authentication for administrators

and for employees or vendors with remote access to internal systems requires adding an out-of-channel mechanism, such as a text message sent to a cellphone to get a one-time-use code. An attacker would not only have to phish for user ID and password, but would also have to physically steal the employee's cellphone.

Other preventive measures include creating a software inventory, "whitelisting" the authorized programs and then preventing unauthorized software from being installed or executed on the system (CSC 2) and securely configuring equipment to prevent the exploitation of open ports or default passwords (CSC 3).

Unsupported and unpatched software is a serious vulnerability. Keeping up-to-date in patching newly discovered security vulnerabilities is critical (CSC 4). This includes upgrading to new versions of browsers and other critical software when earlier versions are no longer supported and patched. Applications exposed to the public Internet present a significant threat vector, and it is critical that organizations use up-to-date, patched and supported browsers. When an older browser version is no longer supported by a developer, security gaps go unaddressed and users are left exposed to data leaks and breaches.

Applications exposed to the public Internet present a significant threat vector and it is critical that organizations use up-to-date, patched, and supported browsers.

Other basic measures also contribute to a strong defense, including boundary defenses (CSC 12) and controlling ports and other vulnerable access points (CSC 9). Maintaining and analyzing audit logs also allows for early detection of the use of stolen credentials, brute-force attacks on passwords, and other anomalous activity on the network (CSC 6).

Physical Theft and Loss Breaches

Breaches resulting from unencrypted data on stolen or lost devices are particularly prevalent in the health care sector and they tend to involve the most sensitive types of information, Social Security numbers and medical information. As we have noted in previous data breach reports, breaches of this time are preventable. Applicable controls include inventorying devices, and using encryption to protect the data, particularly on mobile devices (CSC 1) (CSC 13). Implementing these controls could have protected more than 2.7 million California residents whose personal information was put at risk by these avoidable breaches.

Error Breaches

Many breaches resulting from errors can be prevented or their impact mitigated by several controls. Errors by insiders that resulted in breaches included sending information by email

to unintended persons, disposing of digital devices without first "wiping" the data, and unintentionally making information available to unauthorized persons by posting it on a website. Errors like these led to 111 breaches, affecting more than two million Californians in the past four years. Security controls that would be particularly effective in addressing these vulnerabilities include training and awareness directed to staff and vendors who handle sensitive information (CSC 17), and using strong encryption and data loss prevention software (CSC 13). Monitoring the flow of data (CSC 13) can flag and even prevent the unintentional (or intentional, for that matter) emailing of unencrypted Social Security numbers and other personal information outside the network.

Encrypting data on portable devices could have prevented breaches that affected more than 2.7 million Californians.

Misuse Breaches

Breaches caused by employees or service providers who intentionally make unauthorized use of privileges or resources are also addressed by the Controls. Limiting access privileges on a "least privilege" basis (i.e., the minimal level of access that allows users to do their specific jobs), along with monitoring with a particular focus on the limited number of privileged "super users," are critical (CSC 4, CSC 5). Also relevant are the strategic use of encryption to protect sensitive data and the deployment of automated tools at perimeters to monitor for sensitive data leaving the network and block unauthorized attempts to exfiltrate it (CSC 13). These and others of the Controls would reduce the risk of internal misuse of access, a type of breach that affected over 200,000 California residents.

While the analysis above is certainly not exhaustive, it is offered to show that a significant portion of the breaches that put the personal information in over 49 million records at risk in the past four years were the result of the exploitation of known vulnerabilities for which there are known controls.

(2) Multi-Factor Authentication

Recommendation 2:
Organizations should not only use multi-factor authentication to protect critical systems and data, but should also make it available on consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care websites and patient portals, and web-based email accounts.

The combination of username and password is currently the most basic way to authenticate individuals in the online world, to verify that they are who they say they are. Its effectiveness as a security measure relies on the user's ability to devise passwords unique to each account, ensure that the passwords are sufficiently complex, change them periodically, keep them secret, and remember all of the user's username/password combinations. It also requires the organizations that rely on password authentication to secure those usernames and passwords.

This authentication system is failing. We don't use unique passwords for each of our accounts because it would simply be too hard to remember them all. This makes successfully hacked online account credentials very valuable to data thieves, because stolen credentials for one account often allow access to many others.

Making matters worse, many individuals do not use strong passwords that are difficult to guess. For several years, the most common passwords have been "123456," "password," "12345678," "qwerty," and "12345."[27] Nor do individuals change their passwords as often as they should. And organizations do not always take appropriate measures to protect passwords. Accordingly, we have seen many breaches over the past few years in which hackers targeted huge repositories of online account credentials that were not adequately secured.

A stronger form of online authentication uses multiple factors, from independent categories of credentials. Multi-factor authentication pairs "something you know," such as a password or PIN, with "something you have," such as your cellphone or a physical one-time-password token, or "something you are," such as a biometric like a fingerprint. For example, after inputting a password, the user receives a text on his or her cellphone, providing a one-time-use code to enter to log into the account. This means that for hackers or thieves to be successful, they would not only have to acquire the password but would also have to steal the victim's phone. Financial institutions have used multi-factor authentication for access to online bank accounts for nearly a decade, sometimes supplementing username and password with biometrics such as "keystroke dynamics" that recognizes a user's unique typing pattern or with other factors, such as a one-time-password generator.

This form of authentication should be used by all organizations to help protect access to critical systems and sensitive data, such as medical information, financial information, Social Security numbers, as well as company confidential information like intellectual property and trade secrets. Multi-factor authentication is included in the CIS Critical Security Controls for administrative access (CSC 5.6), organizational email accounts (CSC 7), remote login access to company systems (CSC 12.6), and user accounts on the company network (CSC 16.11).

Multi-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care web sites and patient portals, and web-based email accounts.

We want to draw particular attention to the importance of protecting individuals' email accounts. Our email accounts serve as our online calling card, as we shop, bank, and use social networks. Someone who takes over another person's email account can move around the Internet masquerading as that person. Access to an email account also provides a treasure trove of information to use in phishing and other social engineering exploits, as well as information on financial accounts that can be used to take them over. Many, but not all, of the major consumer email providers offer multi-factor authentication. We recommend that the others do so as well, promptly.

(3) Encryption of Data in Transit

Recommendation 3:
Organizations, particularly health care, should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers.

We made the recommendation to encrypt data in transit in our previous breach reports, and although improvement appears to have been made, there are still some sectors lagging behind. As discussed above, encryption is a key Control for protecting data on portable devices (CSC 13).

Government and professional services experience breaches resulting from stolen or lost equipment containing unencrypted data at a higher rate than the average for breaches in all sectors.

But the most striking, and most disturbing, example is health care. More than half (55 percent) of the breaches in this sector are the result of a failure to encrypt, compared to just 16 percent of breaches in all other sectors. Moreover, this sector's breaches involve the most sensitive types of personal information: medical information and Social Security numbers.

As we have said in the past, breaches of this type are preventable. Affordable solutions are widely available: strong full-disk encryption on portable devices and desktop computers when not in use.[28] Even small businesses that lack full time information security and IT staff can do this. They owe it to their patients, customers, and employees to do it now.

(4) Fraud Alerts

Recommendation 4:
Organizations should encourage those affected to place a fraud alert on their credit files when Social Security numbers or driver's license numbers are breached.

As discussed earlier in the report, the transition to the use of more secure EMV payment cards will increase the criminal demand for Social Security numbers, and the abuse of Social Security numbers is the most difficult type of fraud for consumers to detect, protect against, and recover from.

There are services for consumers that offer early detection of new account fraud, and we are seeing that Californians are now more likely to receive the benefit of such services. As discussed earlier, in 2015 a new law took effect that requires an organization that is the source of a breach of Social Security numbers or driver's license numbers to offer identity theft prevention and mitigation services at no cost to the affected individuals for no less than 12 months. Since then, we have seen over a 20 percent increase in these services being offered in such breaches.

These identity theft prevention and mitigation services generally include credit monitoring, which alerts consumers to new account activity in their credit records, and remediation assistance in the event of actual identity theft. A credit freeze is the strongest protection against new account fraud, but for some individuals the freeze can be cumbersome, as it must be lifted (for a fee) whenever an individual wants to apply for new credit, insurance, or employment.

There is an additional measure, which is free, fast, and effective in preventing new account fraud: a fraud alert. A fraud alert provides protection against the use of a stolen Social Security number to apply for and open new accounts. Consumers can place a fraud alert on their credit files with a single phone call or online. When a merchant checks the credit history of someone applying for credit the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. Providing additional identification is generally difficult for an identity thief, which is why the fraud alert is effective. An alert lasts for 90 days and can be renewed.

Many of the notices on Social Security or driver's license number breaches sent in 2015 do mention the availability of a fraud alert, but the information is most often buried in the

details about ordering credit reports and enrolling in the identity theft prevention and mitigation service offered. We recommend that all organizations encourage notice recipients to place a fraud alert in this type of breach, and make the information on how to do it more prominent in their notices.

(5) Harmonizing State Breach Laws

Recommendation 5:
State policy makers should collaborate in seeking to harmonize state breach laws on some key dimensions. Such an effort could preserve innovation, maintain consumer protections, and retain jurisdictional expertise.

The proliferation of state data breach notification laws has led to calls for regulatory simplification. Proposals in Congress would set a uniform standard by preempting state laws on data breach and often on data security as well. The standards proposed, however, would lower the bar, thereby providing less consumer protection for Californians, and because in multi-state breaches the highest standard tends to prevail, less protection for residents of other states as well.

An alternative approach to achieving the goal of easing the compliance burden is to harmonize state breach laws on some key dimensions. While the state laws have often been characterized as a "patchwork," there is a clear pattern to that patchwork as we discussed in our analysis of all the state data breach notification laws. Furthermore, compliance with the highest standard typically meets the obligations of a number of lower standards, thus minimizing the number of patches in the quilt. We recommend that state-level policy makers including state legislators and Attorney Generals' offices collaborate in identifying opportunities to highlight the common pattern and reduce some of the differences. Such an effort could result in simplifying compliance, while preserving consumer protections, flexibility in adapting to changing threats, and the benefits of jurisdictional expertise.

Appendix A

The CIS Critical Security Controls for Effective Cyber Defense

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

The CIS Critical Security Controls for Effective Cyber Defense, Version 6.0, October 15, 2015, is available from the Center for Internet Security at *www.cisecurity.org/*. The document is licensed under a Creative Commons Attribution-- Non Commercial-- No Derivatives 4.0 International Public License. The link to the license terms can be found at *https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode*.

Appendix B

The Critical Security Controls Master Mapping (Excerpt)

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 1: Inventory of Authorized and Unauthorized Devices	CA-7: Continuous Monitoring CM-8: Information System Component Inventory IA-3: Device Identification and Authentication SA-4: Acquisition Process SC-17: Public Key Infrastructure Certificates SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-1 ID.AM-3 PR.DS-3	A.8.1.1 A.9.1.2 A.13.1.1	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	2.4
CSC 2: Inventory of Authorized and Unauthorized Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-8: Information System Component Inventory CM-10: Software Usage Restrictions CM-11: User-Installed Software SA-4: Acquisition Process SC-18: Mobile Code SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-2 PR.DS-6	A.12.5.1 A.12.6.2	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	
CSC 3: Secure Configurations for Hardware and Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan	PR.IP-1	A.14.2.4 A.14.2.8 A.18.2.3	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	2.2 2.3 6.2 11.5

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 3 *continued*	CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation SI-4: Information System Monitoring					
CSC 4: Continuous Vulnerability Assessment and Remediation	CA-2: Security Assessments CA-7: Continuous Monitoring RA-5: Vulnerability Scanning SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring SI-7: Software, Firmware, and Information Integrity	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	A.12.6.1 A.14.2.8	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Work-station, Laptop, Handheld)	6.1 6.2 11.2
CSC 5: Controlled Use of Administrative Privileges	AC-2: Account Management AC-6: Least Privilege AC-17: Remote Access AC-19: Access Control for Mobile Devices CA-7: Continuous Monitoring IA-2: Identification and Authentication (Organiza-tional Users) IA-4: Identifier Management IA-5: Authenticator Management SI-4: Information System Monitoring	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Authentication and Access Controls	2.1 7.1-7.3 8.1-8.3 8.7
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs	AC-23: Data Mining Protection AU-2: Audit Events AU-3: Content of Audit Records AU-4: Audit Storage Capacity AU-5: Response to Audit Processing Failures	PR.PT-1 DE.AE-3 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4	A.12.4.1-A.12.4.4 A.12.7.1	164.308(a)(1): Security Management Process-Informa tion System Activity	Security Monitoring	10.1-10.7

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 6 *continued*	AU-6: Audit Review, Analysis, and Reporting AU-7: Audit Reduction and Report Generation AU-8: Time Stamps AU-9: Protection of Audit Information AU-10: Non-repudiation AU-11: Audit Record Retention AU-12: Audit Generation AU-13: Monitoring for Information Disclosure AU-14: Session Audit CA-7: Continuous Monitoring IA-10: Adaptive Identification and Authentication SI-4: Information System Monitoring	DE.DP-5		Review - R 164.308(a)(5): Security Awareness and Training-Log-in Monitoring-A		
CSC 7: Email and Web Browser Protections	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation SI-4: Information System Monitoring	PR.IP-1	A.14.2.4 A.14.2.8 A.18.2.3	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	2.2 2.3 6.2 11.5

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 8: Malware Defenses	CA-7: Continuous Monitoring SC-39: Process Isolation SC-44: Detonation Chambers SI-3: Malicious Code Protection SI-4: Information System Monitoring SI-8: Spam Protection	PR.PT-2 DE.CM-4 DE.CM-5	A.8.3.1 A.12.2.1 A.13.2.3	164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A 164.310(d)(1): Device and Media Controls-Accountability A 164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Work-station, Laptop, Handheld)	5.1-5.4
CSC 9: Limitation and Control of Network Ports	AC-4: Information Flow Enforcement CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-6: Configuration Settings CM-8: Information System Component Inventory SC-20: Secure Name /Address Resolution Service (Authoritative Source) SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver) SC-22: Architecture and Provisioning for Name/ Address Resolution Service SC-41: Port and I/O Device Access SI-4: Information System Monitoring	PR.AC-5 DE.AE-1	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Network Security	1.4

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 10: Data Recovery Capability	CP-9: Information System Backup CP-10: Information System Recovery and Reconstitution MP-4: Media Storage	PR.IP-4	A.10.1.1 A.12.3.1	164.308(a)(7): Contingency Plan - Data Backup Plan R 164.308(e)(7): Contingency Plan - Disaster Recovery Plan R 164.308(a)(7): Contingency Plan - Testing and Revision Procedure A 164.310(d)(1): Device and Media Controls - Data Backup and Storage A	Encryption	4.3 9.5-9.7
CSC 11: Secure Configurations for Network Devices	AC-4: Information Flow Enforcement CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-8: Information System Component Inventory MA-4: Nonlocal Maintenance SC-24: Fail in Known State SI-4: Information System Monitoring	PR.AC-5 PR.IP-1 PR.PT-4	A.9.1.2 A.13.1.1 A.13.1.3		Network Security	1.1-1.2 2.2 6.2

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 12: Boundary Defense	AC-4: Information Flow Enforcement AC-17: Remote Access AC-20: Use of External Information Systems CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration SA-9: External Information System Services SC-7: Boundary Protection SC-8: Transmission Confidentiality and Integrity SI-4: Information System Monitoring	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	A.9.1.2 A.12.4.1 A.12.7.1 A.13.1.1 A.13.1.3 A.13.2.3		Network Security Security Monitoring	1.1-1.3 8.3 10.8 11.4
CSC 13: Data Protection I	AC-3: Access Enforcement AC-4: Information Flow Enforcement AC-23: Data Mining Protection CA-7: Continuous Monitoring CA-9: Internal System Connections R-9: Information Spillage Response MP-5: Media Transport SA-18: Tamper Resistance and Detection SC-8: Transmission Confidentiality and Integrity SC-28: Protection of Information at Rest SC-31: Covert Channel Analysis SC-41: Port and I/O Device Access SI-4: Information System Monitoring	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2	A.8.3.1 A.10.1.1- A.10.1.2 A.13.2.3 A.18.1.5	164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R 164.310(d)(1): Device and Media Controls-Accountability A 164.312(a)(1): Access Control-Encryption and Decryption A 164.312(e)(1): Transmission Security - Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	Encryption Data Security	3.6 4.1-4.3

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 14: Controlled Access Based on the Need to Know	AC-1: Access Control Policy and Procedures AC-2: Account Management AC-3: Access Enforcement AC-6: Least Privilege AC-24: Access Control Decisions CA-7: Continuous Monitoring MP-3: Media Marking RA-2: Security Categorization SC-16: Transmission of Security Attributes SI-4: Information System Monitoring	PR.AC-4 PR.AC-5 PR.DS-1 PR.DS-2 PR.PT-2 PR.PT-3	A.8.3.1 A.9.1.1 A.10.1.1	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R 164.308(a)(4): Information Access Management - Access Authorization A 164.312(a)(1): Access Control -Encryption and Decryption A 164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A 164.312(a)(1): Access Control - Automatic Logoff A 164.312(d): Person or Entity Authentication - R 164.312(e)(1): Transmission Security-Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	Authentication and Access Controls Encryption Data Security	1.3-1.4 4.3 7.1-7.3 8.7

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 15: Wireless Access Control	AC-18: Wireless Access AC-19: Access Control for Mobile Devices CA-3: System Interconnections CA-7: Continuous Monitoring CM-2: Baseline Configuration IA-3: Device Identification and Authentication SC-8: Transmission Confidentiality and Integrity SC-17: Public Key Infrastructure Certificates SC-40: Wireless Link Protection SI-4: Information System Monitoring		A.10.1.1 A.12.4.1 A.12.7.1		Network Security Encryption Security Monitoring	4.3 11.1
CSC 16: Account Monitoring and Control	AC-2: Account Management AC-3: Access Enforcement AC-7: Unsuccessful Logon Attempts AC-11: Session Lock AC-12: Session Termination CA-7: Continuous Monitoring IA-5: Authenticator Management IA-10: Adaptive Identification and Authentication SC-17: Public Key Infrastructure Certificates SC-23: Session Authenticity SI-4: Information System Monitoring	PR.AC-1 PR.AC-4 PR.PT-3	A.9.1.1 A.9.2.1-A.9.2.6 A.9.3.1 A.9.4.1-A.9.4.3 A.11.2.8	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(4): Information Access Management - Access Authorization A 164.308(a)(4): Information Access Management-Access Establishment and Modification A 164.308(a)(5): Security Awareness & Training-Password Management A 164.312(a)(1): Access Control - Unique User Identification R 164.312(a)(1): Access Control - Automatic Logoff A 164.312(d): Person or Entity Authentication - R 164.312(e)(1): Transmission Security - Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	Authentication and Access Controls	7.1-7.3 8.7-8.8

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1: Security Awareness and Training Policy and Procedures AT-2: Security Awareness Training AT-3: Role-Based Security Training AT-4: Security Training Records SA-11: Developer Security Testing and Evaluation SA-16: Developer-Provided Training PM-13: Information Security Workforce PM-14: Testing, Training, & Monitoring PM-16: Threat Awareness Program	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	A.7.2.2	164.308(a)(5): Security Awareness and Training - Security Reminders A 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A 164.308(a)(5): Security Awareness and Training-Log-in Monitoring A 164.308(a)(5): Security Awareness and Training - Password Management A	Personnel Security	12.6
CSC 18: Application Software Security	SA-13: Trustworthiness SA-15: Development Process, Standards, and Tools SA-16: Developer-Provided Training SA-17: Developer Security Architecture and Design SA-20: Customized Development of Critical Components SA-21: Developer Screening SC-39: Process Isolation SI-10: Information Input Validation SI-11: Error Handling SI-15: Information Output Filtering SI-16: Memory Protection	PR.DS-7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6-A.14.2.8		Application Security Software Development & Acquisition	6.3 6.5-6.7

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 19: Incident Response and Management	IR-1: Incident Response Policy and Procedures IR-2: Incident Response Training IR-3: Incident Response Testing IR-4: Incident Handling IR-5: Incident Monitoring IR-6: Incident Reporting IR-7: Incident Response Assistance IR-8: Incident Response Plan IR-10: Integrated Information Security Analysis Team	PR.IP-10 DE.AE-2 DE.AE-4 DE.AE-5 DE.CM-1-7 RS.RP-1 RS.CO-1-5 RS.AN-1-4 RS.MI-1-2 RS.IM-1-2 RC.RP-1 RC.IM-1-2 RC.CO-1-3	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4- A.16.1.7	164.308(a)(6): Security Incident Procedures - Response and Reporting R	12.10	
CSC 20: Penetration Tests and Red Team Exercises	CA-2: Security Assessments CA-5: Plan of Action and Milestones CA-6: Security Authorization CA-8: Penetration Testing RA-6: Technical Surveillance Countermeasures Survey SI-6: Security Function Verification PM-6: Information Security Measures of Performance PM-14: Testing, Training, & Monitoring		A.14.2.8 A.18.2.1 A.18.2.3		11.3	

This table is excerpted from the Critical Security Controls Master Mappings Tool, available at *http://www.cisecurity.org/critical-controls/tools/AuditScripts_CISControlv6_Mappings.xlsx*. It is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Appendix C

California Data Breach Notification Statutes

Civil Code Section 1709.29

a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[FORM OMITTED]

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and 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:

(A) Social security number.

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

(C) 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.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

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

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information.

Substitute notice shall consist of all of thefollowing:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

California Civil Code Section 1798.82

(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[FORM OMITTED]

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and 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:

(A) Social Security number.

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

(C) 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.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

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

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Notes

[1] Javelin Strategy & Research, *2015 Data Breach Fraud Impact Report* (June 2015), pp.12-13, available at *www.javelinstrategy.com*.

[2] Privacy enforcement actions are posted on the Attorney General's website when they are final, at *https://oag.ca.gov/privacy/privacy-enforcement-actions*.

[3] In some breaches, more than one organization notified those affected. For example, in the 2015 Anthem breach, in addition to Anthem's notice, seven employers for which Anthem was a service provider submitted notices that they'd sent to their employees, resulting in eight sample notices for the single Anthem breach submitted to the Attorney General. Also in 2015, a breach at a service provider to a number of California wineries resulted in 23 notices being submitted from different wineries. Similarly, a breach in a service provider to major drug stores resulted in three notices submitted by the different stores. In some payment data breaches at retailers or restaurants, card-issuing banks also notified their cardholders, resulting in multiple sample notices for the same breach being submitted to the Attorney General. In such cases of multiple notifications of a single breach, all the notices submitted are published on the website at www.oag.ca.gov/ecrime/databreach/list .For analytical purposes, however, each breach was counted only once. Thus the total number of breaches reported to the Attorney General from 2012 through 2015 is 657, while the number of sample notices published on the website for the same period is 699.

[4] The three U.S. states without breach notice laws as of the end of 2015 are Alabama, Mew Mexico, and South Dakota.

[5] See legislative committee analyses of SB 1386 (Peace) and AB 700 (Simitian) of 2002, at *www.leginfo.legislature.ca.gov*.

[6] Lost and stolen cards used at the point of sale made up 12 percent of card fraud losses, and card-not-present fraud (online, phone) 43 percent, see *http://tsys.com/ngenuity-journal/chip-and-pin-vs-chip-and-signature-a-rivalry-nears-historic-proportions.cfm*.

[7] Business Insider, *The U.S. EMV Migration Report* (November 19, 2015), quoted at *www.businessinsider.com/the-us-emv-migration-report-what-new-chip-cards-mean-for-consumers-issuers-and-merchants-2015-11*.

[8] Javelin Strategy & Research, *op.cit*., p. 6.

[9] The categories of breaches are based generally on Verizon's Vocabulary for Event Recording and Incident Sharing (VERIS) Framework, a taxonomy designed to provide a common language for describing security incidents. Because of limitations in our knowledge of the details of some breaches, we did not use the full spectrum of VERIS categories. For more on VERIS, see *http://veriscommunity.net/*.

[10] As of January 1, 2016, the definition of personal information in the breach law also includes data from automated license plate reader systems, along with a name.

[11] The North American Industry Classification System (NAICS) sectors used in the breach report are Retail, Finance and Insurance, Health Care, Professional Services, Government (Public Administration), Hospitality (Accommodation and Food Service), Education, and Other. The Other category includes agriculture, utilities, information, manufacturing, wholesale trade, transportation, real estate and waste management, no one of which accounted from more than 5 percent of the breaches in our dataset. The most recent version of the NAICS is available at *www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012*.

[12] The Small Business Administration has established size standards for for-profit industries, based on annual receipts and number of employees. The standards are set according to the North American Industry Classification System (NAICS) code for a business. The size standards are used to determine eligibility for the SBA programs; see more at *www.sba.gov/category/navigation-structure/contracting/contracting-officials/small-business-size-standards*.

[13] Verizon, 2015 Data Breach Investigations Report, pp. 15-16.

[14] Thomas J. Smedinghoff, "An Overview of Data Security Legal Requirements for All Business Sectors," October 2015, available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323*. The article includes a list of information security law references.

[15] On the other hand, the Massachusetts data security regulations require businesses to follow a process to develop a comprehensive written information security program, but also include some specific measures to be included in the program. See Massachusetts General Law Chapter 93H and implementing regulations 201 CMR 17.00 et seq.

[16] Gramm-Leach-Bliley Act (GLB), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC). Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR Part 164, Standards for the Protection of Electronic Protected Health Information. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq. See also Federal Communications Commission, Open Internet Order (Mar. 12, 2015), Section 201 and Section 222; Se

[17] William Stallings, "Standards for Information Security Management," Internet Protocol Journal, Volume 10, No. 4 (December 2007), p. 10, available at *http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/ipj_10-4.pdf*.

[18] NIST, *Special Publication 800-53: Security and Privacy Controls for Federal information Systems and Organizations, Revision 4, and Framework for Improving Critical Infrastructure Cybersecurity*, both available at *www.nist.gov*.

[19] International Organization for Standardization, *ISO/IEC 27002:2013 Information technology, Security techniques, Code of practice for information security controls*, available at *www.iso.org*.

[20] Center for Internet Security, at *https://benchmarks.cisecurity.org*, NIST National Checklist Program, at *http://csrc.nist.gov/fdcc/faq-common_security_configurations.html*, and the Defense Information Systems Agency's Security Technical Implementation Guides, at *http://iase.disa.mil/stigs/Pages/index.aspx*. Also MITRE Corporation, Systems Engineering Guide on Configuration Management Tools, at *www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/configuration-management/configuration-management-tools*.

[21] The CIS Critical Security Controls for Effective Cyber Defense, Version 6, October 15, 2015, available from the Center for Internet Security at *www.cisecurity.org/.*

[22] In addition to the CIS Critical Security Controls, the Center for Internet Security manages the Multi-State Information Sharing and Analysis Center (MS-ISAC) used by state governments, and the CIS Security Benchmarks. More at *www.cisecurity.org/*.

[23] A mapping of the CIS Critical Security Controls to NIST SP 800-53, the NIST Framework, ISO 27002, HIPAA, the Federal Financial Institutions Examination Council Examiners Handbook, and several other security standards is available at *www.cisecurity.org/critical-controls/tools/AuditScripts_CISControlv6_Mappings.xlsx*.

[24] SANS, *Critical Security Controls: From Adoption to Implementation*, Sponsored by McAfee/Intel Security, September 2014, available at *https://www.qualys.com/forms/whitepapers/sans-critical-security-controls/*.

[25] In an effort to assist smaller organizations, the Center and the National Governors Association have launched a National Cyber Hygiene Campaign, a plain-language, low-cost approach to basic cyber security that focuses on the first five controls. The Campaign is developing Tool Kits, which are works in progress, including instructions, technical guidance, links to additional resources, and tips on measuring the implementation and effectiveness of the controls. Information on the National Campaign for Cyber Hygiene is available at *www.cisecurity.org/cyber-pledge/*.

[26] Verizon, *2015 Data Breach investigations Report*, pp. 12-13.

[27] prweb, "SplashData's fifth annual 'Worst Passwords List' shows people continue putting themselves at risk," January 19, 2016, at *www.prweb.com/releases/worst/passwords/prweb13170789.htm*.

[28] In a recent case, the FTC settled with a provider of dental office management software, alleging that Henry Schein Practice Solutions, Inc., falsely advertised the level of encryption used to protect patient data. The complaint referenced NIST's Advanced Encryption

Standard as the industry standard for strong encryption. See *www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled*.

California Department of Justice
Privacy Enforcement and Protection Unit

www.oag.ca.gov/privacy