Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **December 2021**
Sponsored by **ActiveNav**

How to Comply with the CPRA

Executive Summary

With the unprecedented ability of organizations to digitally collect, process, harness and sell personal data on people across the world—much of it without their knowledge or consent—regulators are taking an increasingly activist role to safeguard personal data. Europe has a harmonized data protection framework that applies to all member states—the General Data Protection Regulation (GDPR)—but there is no equivalent federal approach in the United States. Instead, state-level approaches to data privacy and data protection are emerging across the union, with California one of several states at the forefront of this movement.

This report looks at current compliance with the original California Consumer Privacy Act (CCPA) and how organizations are approaching compliance for the California Privacy Rights Act (CPRA), the updated and extended privacy legislation covering data on California residents.

KEY TAKEAWAYS

- **Two thirds of organizations are not yet compliant with the CCPA**
  Only 36% of organizations are currently compliant with the original CCPA, two years after it became operational.
- **Few organizations currently have highly mature data privacy approaches**
  Only 23% of organizations claim their overall approach to data privacy is currently "very mature." This standard is required by the CCPA and CPRA.
- **One third of organizations believe they are already fully CPRA-compliant**
  While the complete set of rules for the CPRA will not be finalized until mid-2022, 33% of organizations believe they are already fully compliant.
- **Critical underlying data disciplines are not widely adopted**
  Many organizations rely on point-in-time data inventories rather than real-time data maps, have insufficient access controls covering personal data, and cannot exclusively identify data related to California residents. Further, organizations lack effective controls for identifying CPRA-covered data across many data sources, such as unsanctioned cloud services, Microsoft Teams, and Slack.
- **Senior leadership understanding of CPRA is lagging**
  Compliance and legal professionals have a higher understanding of the importance of complying with CPRA than senior leadership. This lag threatens prioritization of funding for projects needed to achieve CPRA compliance.
- **Budget for CPRA compliance has not been allocated at 57% of organizations**
  Many organizations have low maturity for data privacy, which means new solutions will be required to achieve CPRA compliance. Three out of five organizations are yet to scope out budget requirements and plan accordingly.
- **Half of organizations cannot validate CRPA compliance for third-party website code**
  Half of organizations lack effective processes for ensuring code supplied by third-party vendors is CPRA-compliant and not compromised. This is alarming since online channels are prominent in the use and collection of personal data.
- **Over half of organizations do not yet have a training program on CPRA**
  Solutions to enable CPRA compliance are affected by organizational processes and people. Employee actions that are ill-advised, careless, or negligent undermine a firm's CPRA compliance posture. Over half of organizations do not have a training program on CPRA responsibilities yet.

The California Privacy Rights Act is one of several state-level initiatives in the United States to address data privacy in the absence of a federal approach.

ABOUT THIS WHITE PAPER

This white paper was sponsored by ActiveNav. Information about ActiveNav is provided at the end of this paper.

This white paper references data from an in-depth survey conducted in October 2021 of 129 professionals involved in developing, approving, enforcing, or reviewing their organization's policies and practices regarding data protection and management. Respondents worked for mid-sized and large organizations (average employees 11,796, median employees 1,250). All respondents are knowledgeable about how their organization is addressing the requirements of the CCPA and will address the new requirements of the CPRA.

What is the CPRA?

The CPRA overlays new and modified privacy rights on the CCPA for residents of California. In this section, we look at the foundation created by the CCPA, and briefly at the changes introduced by the CPRA. This is not intended to be an exhaustive treatment.

BUILDS ON THE FOUNDATION OF THE CCPA

The CCPA created a set of data privacy rights for California residents, with compliance for businesses triggered by holding or using data on California residents rather than physically operating in California. CCPA is focused on "personal information," which is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" and includes a long list of specific data types.[1] Rights for residents over their personal information include:

- **Right to be informed**
  Residents have the right to ask a business to disclose what kinds of personal information has been collected on them—or purchased about them—including why it was collected or purchased.
- **Right of deletion**
  Residents have the right to request deletion of the personal information held on them by a business. In effect, this gives the resident the right to the highest form of opt-out for the use of their personal information.
- **Right to opt out of sale of personal information**
  Residents can request that their personal information is not sold to another business, data broker, or other entity. This right give residents control over who can access and use their personal information. Under CCPA, businesses that collected personal information on consumers had to add a "Do Not Sell my Personal Information" button to their website to streamline usage of this right.
- **Right of transfer**
  A resident can request a business to provide their personal information in a format that enables them to transfer that data to another service.

As in other jurisdictions in the United States and abroad, data privacy and data protection legislation add counteracting checks and balances for consumers against unrestrained data gathering and surreptitious corporate surveillance. The CCPA became law in June 2018 and effective from January 2020.

Data privacy and data protection legislation adds counteracting checks and balances for consumers against unrestrained data gathering and surreptitious corporate surveillance.

THE SIGNIFICANT CHANGES OF THE CPRA

The CPRA revises and extends the CCPA, adding new rights and addressing several shortcomings of the original legislation. The significant changes are:

- **Sensitive personal information is defined as a new category of data**
  The CPRA separately defines "sensitive personal information" as a subset of the general "personal information" category introduced in the CCPA. Data elements covered by this new category include race, ethnicity, sex life, sexuality, financial information, union membership, and geolocation. Sensitive personal information (SPI) imposes additional requirements on businesses.
- **Contractor is introduced as a fourth entity type**
  The CCPA defined three entities: a business, a service provider, and a third party. The CPRA adds "contractor" as a fourth entity, which is essentially a service provider that incurs additional obligations on the lifecycle use of personal data supplied by a business. For example, while both a service provider and contractor have an obligation to use personal information only to perform services on the behalf of a business, a contractor has an additional obligation to not combine personal information supplied by several businesses, such as to create unified mega-profiles on individuals.
- **Creates the California Privacy Protection Agency (CPPA)**
  The CPRA creates a new agency in California to supervise and enforce its requirements. This role was vested with the Attorney General under CCPA, but the CPPA takes over under CPRA.

Other changes extend consent requirements, double the minimum number of residents (or households) required before a business is subject to CPRA, and requires an annual audit of high-risk processing activities.

The CPRA revises and extends the CCPA, adding new rights and addressing several shortcomings of the original legislation.

CPRA ADDS FOUR NEW DATA RIGHTS FOR CALIFORNIA RESIDENTS

The CPRA adds four new rights for California residents and amends five of the original rights introduced by the CCPA. The four new rights are:

- **Right to Correct Inaccurate Personal Information**
  Residents have the right to request that a business corrects any inaccurate personal information held about them, covering both personal and sensitive personal data elements. The exercise of this right would usually follow a Right to Know request, and the CPPA is still working through several practical details related to this right (see the next section for details).
- **Right to Limit Use and Disclosure of Sensitive Personal Information**
  Residents can direct a business to limit the use and disclosure of their SPI. If a business uses SPI to make inferences about an individual—such as for targeted advertising—they must include a link on their website for residents to opt out.
- **Right to Know About Automated Decision-Making**
  If businesses make use of automated decision-making, a resident can request details of how, what, when, where, and why. Residents have the right to know when such decision-making is used, and what the likely outcomes are.
- **Right to Opt-Out of Automated Decision-Making**
  If a resident dislikes how a business is using their personal and sensitive personal information in automated decision-making, they have the right to opt out. Businesses must exclude data covered by opt-out requests.

CPRA RULES ARE STILL BEING DEVELOPED

The CCPA vested rulemaking authority with the Attorney General in California, but that authority was transferred under CPRA to the newly created California Privacy Protection Agency[2] (CPPA) from mid-2021. The new agency is pushing ahead to finalize the rules that apply under CPRA. Areas of particular focus include:[3]

- **Processing that presents a significant risk to consumer privacy or security**
  Businesses are not allowed to process a consumer's personal information when that presents a "significant risk" to their privacy or security. The CPPA is working out what that looks like in practice, including specific restrictions or prohibitions that should apply to such processing.
- **Access and opt-out rights regarding automated decision-making**
  Businesses that use automated decision-making technology are required to disclose this in response to right to access requests and not use it if a consumer exercises their right to opt out of such decision-making. The CPPA is exploring what activities should be covered under the term "automated decision-making" and what the process should look like for exercising the rights of access and opting out.
- **Enacting the new Right to Correct Inaccurate Personal Information**
  The right to request correction is a new right added by the CPRA. The CPPA is looking at what specific rules and procedures will be required to enact this new right, including how frequently a consumer can exercise this right, what a business should do to prevent fraudulent requests, and under what circumstances a business can refuse to meet a right to correct request.
- **Right to limit use and disclosure of sensitive personal information**
  The CPRA enables consumers to request that businesses limit the use and disclosure of their sensitive personal information. The CPPA is considering various specifics about the use of this right.

The CPRA requires that all regulations are finalized by the CPPA by July 1, 2022.

Organizations choosing to ignore their responsibilities under CPRA until mid-2023 are embarking on a risky path.

THE TIMELINE FOR COMPLIANCE IS SHRINKING

The CPRA became law in November 2020 and becomes fully effective in mid-2023. However, the lookback provision in the CPRA means that organizations are required to start tracking the personal and sensitive personal information they collect, use, and share from January 1, 2022. This means businesses will have 12 months of data for any consumer access requests from January 2023. Organizations choosing to ignore their responsibilities under CPRA until mid-2023 are embarking on a risky path. Figure 1 shows the key milestones to full enforcement.

Figure 1
Key Milestones in CPRA Compliance

Source: Osterman Research (2021)

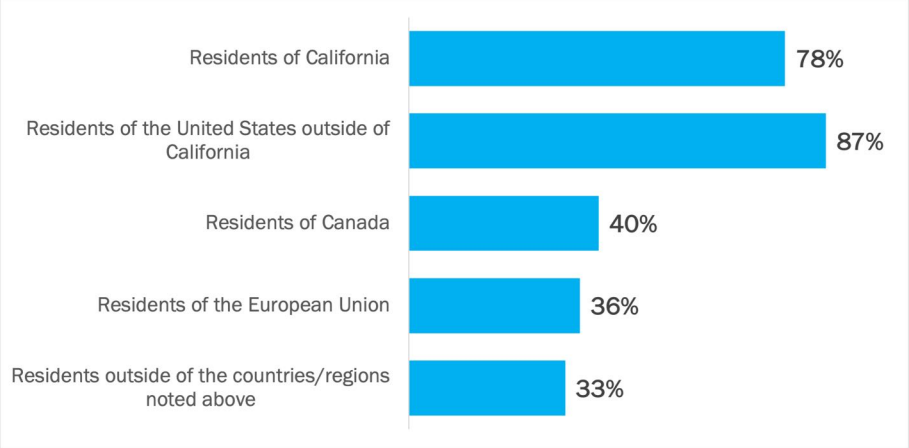
Current Status with Data Privacy Compliance

Compliance with the initial CCPA regulations is already required. In this section, we look at how organizations are currently meeting their compliance responsibilities.

MOST ORGANIZATIONS HAVE DATA ON CALIFORNIA RESIDENTS

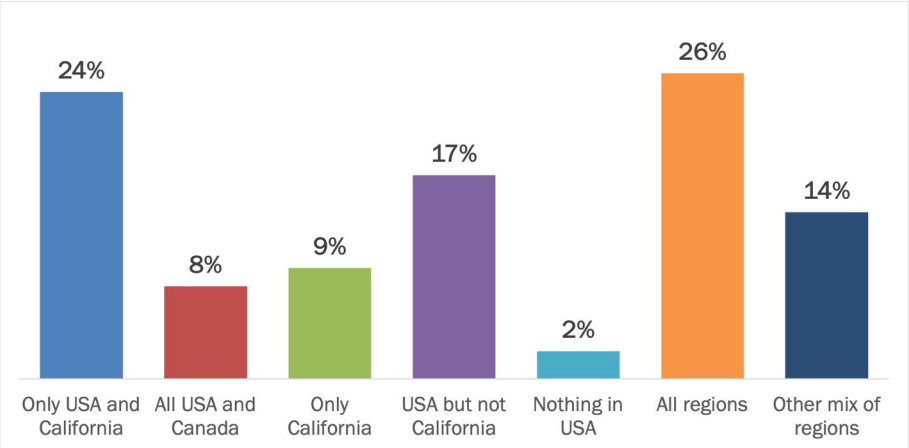
Four out of five organizations possess, process, or control personal data for residents of California (see Figure 2), although organizations fit into different groups for where personal data comes from (see Figure 3). Two thirds of organizations have personal data on residents in California plus a mix of other regions.

Figure 2
Sources of Personal Data
Percentage of respondents



Source: Osterman Research (2021)

Figure 3
Groupings of Sources of Personal Data
Percentage of respondents



Source: Osterman Research (2021)

78%

Organizations possessing, processing, or controlling personal data for residents of California.

SNAPSHOT OF CURRENT MATURITY OF DATA PRIVACY

Maturity of data privacy processes and practices is lacking at many organizations. Only 36% of organizations are currently compliant with the CCPA, only 23% have very mature data privacy approaches, and those not currently compliant with the CCPA expect a higher workload to become compliant with the CPRA. See Figure 4.

Figure 4
Current Status with CCPA Compliance
Percentage of respondents

Source: Osterman Research (2021)

- **Many organizations are not yet compliant with the initial CCPA**
  The initial data privacy law in California—the CCPA—came into effect on January 1, 2020. Almost two years later, only one third of organizations state they are fully compliant with its requirements, and another one quarter expect to be fully compliant by the end of 2021. The CPRA amends and extends the current CCPA requirements, hence current compliance with the CCPA is an indicator for how quickly organizations will be able to comply with the CPRA.
- **Few organizations currently have highly mature data privacy approaches**
  Less than a quarter of organizations claim that their overall organizational and technical approaches to data privacy are currently "very mature." Both the initial CCPA and updates in the CPRA demand elevated maturity in data privacy approaches, a destination that many organizations have not yet reached.
- **CCPA compliance correlated with expected workload for CPRA compliance**
  Organizations that are currently compliant with the CCPA expect a smaller workload for achieving CPRA compliance compared to organizations who are not currently compliant. For organizations that will not be compliant with CCPA until 2022, 51% expect the workload for CPRA compliance to be high or extreme, compared with 71% of already compliant organizations who expect a minor or medium workload.
- **Most of the organizations not planning to be compliant with the CCPA claim not to have personal data on California residents**
  The CCPA applies only to residents of California. While 6% of total respondents to the survey state they have no plans to be compliant with the CCPA, 75% of these respondents claim they do not hold or process data on California residents. If such claims are based on geo-targeted precision rather than relying on people to supply accurate address details, then compliance with the CCPA is not required. This leaves 25% who hold or process data on California residents and yet do not plan to comply.

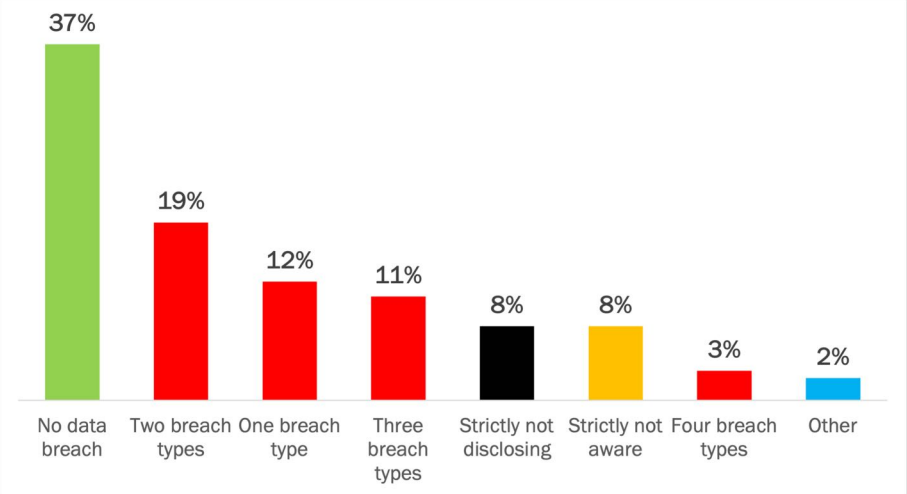
64%

Organizations that are not yet compliant with the initial CCPA.

DATA BREACHES ARE COMMON OCCURRENCES

Three out of five organizations have suffered at least one data breach in the past 12 months covering personal, sensitive, or confidential data or cannot rule out the possibility. Breached data includes personal data on employees, personal data on customers or other parties, corporate intellectual property, and other sensitive or confidential information. Among organizations that have been breached, a breach of two of the above types of data is most common (19% of organizations), followed by one type (12%), and three types (11%). See Figure 5.

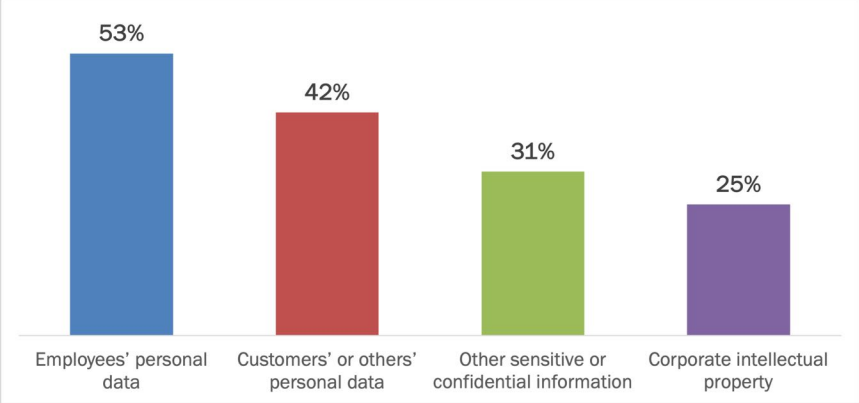
Figure 5
Data Breaches Over the Past 12 Months
Percentage of respondents



Source: Osterman Research (2021)

Among organizations that have been breached, personal data on employees is the most common type of data breach (at 53% of organizations), followed by data on customers or other external parties (42%). These numbers refer to the occurrence of a given type of data breach in the past 12 months, not the number of breaches. See Figure 6.

Figure 6
Data Breaches Over the Past 12 Months
Percentage of respondents



Source: Osterman Research (2021)

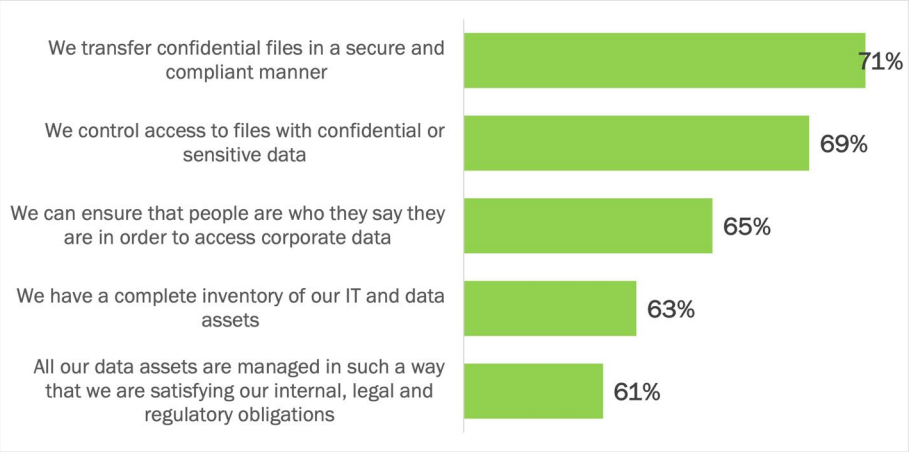
63%

Organizations that have suffered a data breach in the past 12 months or cannot rule out the possibility of a data breach.

SOME DATA PROTECTION PRACTICES ARE WIDELY USED

Organizations that will be subject to the CPRA already use a range of practices to protect data. Practices focused on secure transfer of confidential files, access control, and identity management are commonly used. See Figure 7. While wider adoption of the five practices below is still necessary, at least three out of five organizations claim to have already established effective practices in these areas.

Figure 7
Highest-Rated Practices and Procedures Related to CPRA Compliance
Percentage of respondents indicating "well" or "extremely well"



Source: Osterman Research (2021)

VARIOUS CRITICAL UNDERLYING DATA DISCIPLINES ARE LACKING

A collection of critical underlying data disciplines are not yet widely adopted (see Figure 8). As the enforcement date for the CPRA draws closer, organizations will need to address current weaknesses across a range of data protection disciplines. Organizations need to improve adherence with the following data disciplines, although this is not an exclusive list:

- **Organizations more likely to have a point-in-time inventory of IT and data assets than a real-time data map**
  Data moves fluidly between repositories, cloud workloads, and systems. Having a point-in-time inventory of IT and data assets—in Figure 7, 63% of respondents say this is going "well" or "extremely well"—is important but insufficient. Increasingly, organizations need a real-time assessment of where data subject to CPRA actually resides within the organization as it moves across systems and is stored in places it is not supposed to be stored, as opposed to only a static inventory of systems that are capable of storing data. Over half of respondents—54%—say having a real-time or near real-time data map is currently not going well (see Figure 8).

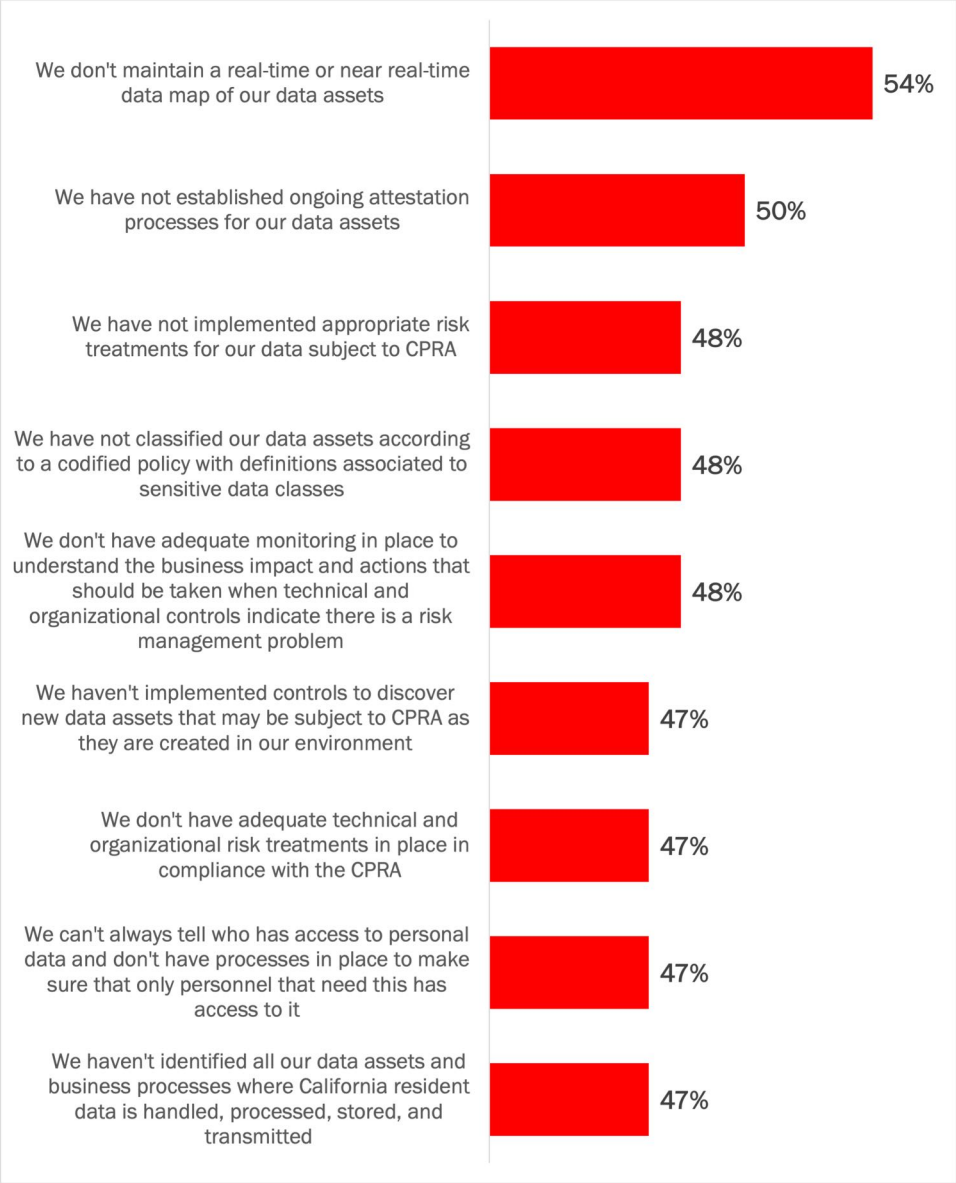
  Without a real-time map of data subject to CPRA, all it takes for a firm to be unable to fully comply with rights requests from California residents is for an employee to store personal or sensitive personal data in an unexpected location. Without a real-time data map, a firm will never be able to offer a high degree of assurance to consumers that its data practices are sufficient to protect their data nor ever fully guarantee compliance to a state regulator. Both carry significant risk.

54%

Organizations lacking a real-time or near real-time map of data subject to CPRA.

- **Controls for verifying identity when accessing corporate data are more effective than when accessing personal data covered by the CPRA**
  Two thirds of organizations currently have strong controls in place for identity verification for access to corporate data (in Figure 7, 65% say they can ensure people are who they say they are in order to access corporate data), but almost half say the same level of controls are lacking for access to personal data (in Figure 8, 47% say current access controls and processes are inadequate for accessing personal data). CPRA focuses on the latter, and while the adoption of stronger controls for both types of data is needed, CPRA elevates the urgency around access to personal data.

Figure 8
Lowest-Rated Practices and Procedures Related to CPRA Compliance
Percentage of respondents indicating inadequate controls in place



Source: Osterman Research (2021)

47%

Organizations with inadequate access controls and processes covering personal data —the focus of the CPRA.

- **About half of organizations cannot identify data related to California residents**
  Unless organizations handling, processing, storing, and transmitting personal data will use the provisions of the CPRA to provide a unified set of data rights to everyone they hold data on, it is vitally important to be able to identify data on California residents exclusively. This is an imperative so that the exercise of rights by a resident are fully met by the organization, rather than just half-heartedly so. About half of respondents say that current practices and processes in this area are inadequate, meaning that they have not identified where California resident data is handled, processed, stored, and transmitted across its data assets and business processes.

- **Current risk treatments and methods for classifying sensitive data for data covered by the CPRA are inadequate**
  Almost half of organizations currently have inadequate risk and classification approaches for data subject to CPRA. In Figure 8, 48% of respondents say risk treatments for data subject to CPRA are inadequate, and 48% also say that sensitive data classification approaches are lacking. Risk treatments include common approaches like identity and access management, plus newer methods such as data masking, pseudonymization, and field-level encryption.

  Data masking, pseudonymization, and field-level encryption provide different ways of protecting the disclosure of personal and sensitive personal information. For example, although a customer's phone number is actually stored in a database, with data masking, employees see a phrase like "[PHONE NUMBER]" on the customer record, rather than the actual number itself. If an employee needs to talk to the customer directly, the system initiates the call while continuing to mask the number from the employee, or if that level of integration is not available, the employee must specifically request access to the phone number for a time-limited period in order to place the call manually. Such risk treatments reduce by design the amount of personal and sensitive personal information that is easily accessible to employees during day-to-day activities. Further, if the customer database is breached, much of the personal and sensitive personal data is masked or encrypted, thereby neutering the extent of the data breach.

- **Organizations do not have the monitoring and controls in place to handle a changing data landscape**
  Almost half of respondents say their firm lacks adequate monitoring to understand what should happen when current controls indicate a risk management problem, and a similar proportion lack controls to discover when new data assets are created in their environment. Both of these weaknesses deal with the ongoing challenge of managing data in light of the CPRA, rather than undertaking a point-in-time assessment about what systems exist that are capable of storing or processing personal data. Both are also related to the indication that many organizations do not have adequate technical and organizational risk treatments in place for CPRA compliance. Technical and organizational risk treatments cover the availability of solutions to assist with CPRA compliance, the design of processes to streamline the exercise of and response to consumer rights, and training of employees to understand their responsibilities under CPRA. Low maturity in these related disciplines indicate a rear-view-mirror approach to CPRA compliance rather than one that assesses where the organization is currently and where it is heading.

48%

Organizations lacking adequate risk treatments and sensitive data classification for data subject to CPRA.

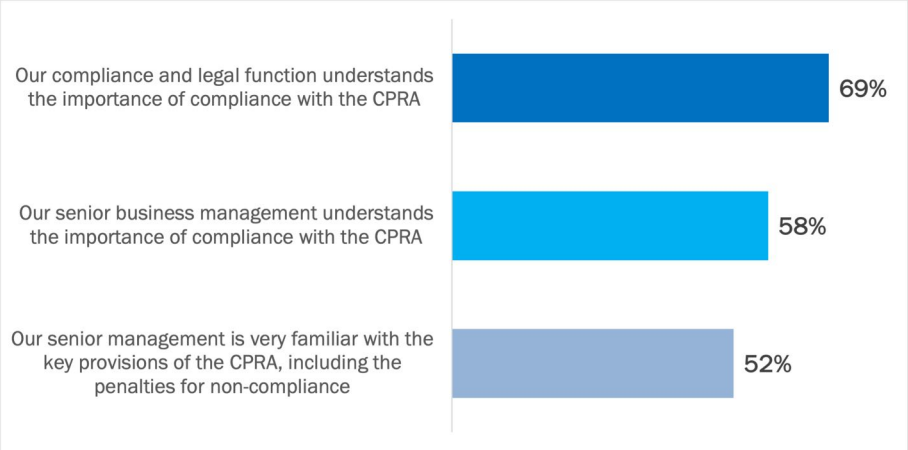
Expectations for CPRA Compliance

In this section, we look at the expectations among organizations for becoming compliant with the data privacy requirements added and expanded on by the CPRA.

LEADERSHIP UNDERSTANDING OF CPRA IS LAGGING

More compliance and legal personnel (69%) understand the importance of complying with the provisions of the CPRA compared with senior business management (58%). Further, among the ranks of senior business management, conceptual understanding of the importance of compliance (58%) ranks ahead of a working knowledge of the requirements and penalty regime (52%). See Figure 9.

Figure 9
Decision-Maker Views on the CPRA
Percentage of respondents indicating "agree" or "strongly agree"



Source: Osterman Research (2021)

Compliance and legal professionals need to understand the importance of compliance with the CPRA—it is part of their job description and the advisory role they play in the organization about compliance responsibilities. While 69% of respondents say this grouping has a strong understanding of the CPRA, 31% of respondents do not. Compliance and legal professionals at organizations subject to the CPRA who are trailing in their understanding need to take urgent action to rectify the imbalance.

The same applies to senior management. Although there is still some time remaining before a higher working knowledge of the CPRA and its penalty regime becomes essential for senior management, that time scope is rapidly shrinking. Once the CPRA goes into enforcement in mid-2023, there is a look-back period to January 2022, which at the date of publishing this report is less than one month away. The risk of insufficient understanding and familiarity with the provisions of the CPRA flows through to insufficient prioritization of funding for the projects needed to achieve timely CPRA compliance.

52%

Organizations where senior management is very familiar with the key provisions and penalty regime of the CPRA.

STRATEGIC PLANS FOR CPRA COMPLIANCE

CPRA imposes a set of strategic demands on organizations. Plans for how to comply with the CPRA are still under development at many organizations. See Figure 10.

Figure 10
Strategic Realities and Beliefs with CPRA Compliance
Percentage of respondents

Source: Osterman Research (2021)

- **Many organizations must comply with the requirements of multiple roles**
  Almost half of organizations have multiple roles to meet under the CPRA, with 41% of organizations being a business and one or more of the other three capacities (i.e., service provider, third party, or contractor). The need to meet the requirements of multiple roles increases the complexity of compliance and drives the need for higher maturity with data privacy approaches. Slightly more than half of organizations must meet only one of the four roles in the CPRA.
- **Budget for CPRA compliance has not been allocated at 57% of organizations**
  With the poor state of data privacy maturity at many organizations, new solutions will be required to achieve CPRA compliance. Almost three out of five organizations are yet to scope out budget requirements and plan accordingly.
- **One third of organizations believe they are already fully CPRA compliant**
  While there are many confirmed requirements for the CPRA, the California Privacy Protection Agency (CPPA) has until mid-2022 to finalize the complete list of rules. One third of organizations believe they are already fully compliant with the CPRA, but this is overconfidence at best and misguided bluster at worst. The rules are not yet finalized; organizations face a changing regulatory framework.
- **Meeting a patchwork of data privacy regulations**
  Just more than half of organizations plan on offering a unified set of data privacy rights to all residents in the United States, irrespective of which state they live in. In effect, this treats the CPRA as the default federal data privacy regulation for the United States. The benevolent extension of data rights in the CPRA to other jurisdictions is commendable, but at the same time, demands a high level of data privacy maturity so that when other state-level requirements are imposed, organizations can meet a patchwork of varying requirements. Organizations that are putting the appropriate data privacy mechanisms in place now will be much better positioned to handle the changing regulatory environment than those who drag their feet. The prospect of varying requirements by state highlights the need for extensible and malleable data privacy controls.

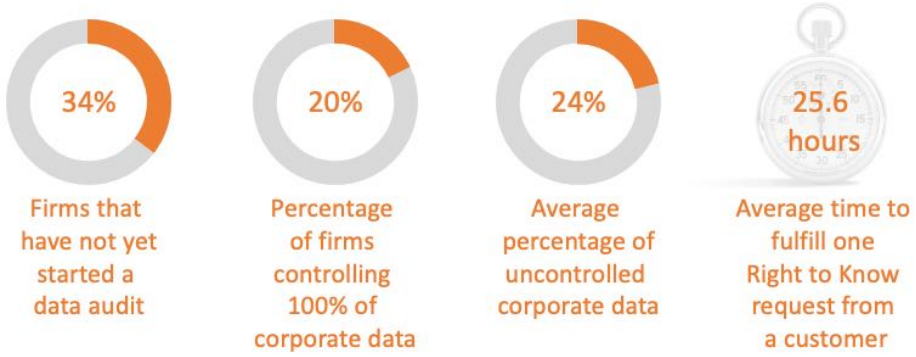
33%

Organizations that believe they are already compliant with the CPRA, even though the rules are not yet finalized.

DATA AND PROCESS PLANS FOR CPRA COMPLIANCE

Complying with the CPRA requires that organizations get a much better handle on the data they collect, process, share, and manage. See Figure 11.

Figure 11
Data Challenges with CPRA Compliance
Percentage of respondents



Source: Osterman Research (2021)

- **One third of organizations do not know where their corporate data is located**
  One third of organizations have not yet even started an audit process to determine where all their corporate data is located, including data classified as personal and sensitive under the CPRA. This is a core discipline to be able to extend the data rights required under the CPRA to residents of California.
- **Four fifths of organizations do not control all corporate data**
  Only one fifth of organizations control all corporate data—that is, where no corporate data is stored on employee-owned laptops or mobile devices that have not been backed up or archived. Four out of five organizations have varying quantities of uncontrolled corporate data to protect.
- **Uncontrolled data creates compliance blind spots**
  Corporate data stored without unified data controls creates opportunities for data breaches as well as blind spots for complying with the exercise of data rights. For example, if a verified California resident exercises their deletion right under the CPRA, leaving copies of covered personal data on employee-owned laptops puts the firm in a posture of non-compliance. If organizations want to continue to utilize bring-your-own-device strategies, enhanced lifecycle protections on corporate data will be required. Across all organizations, 24% of corporate data is not fully under the control of the firm.
- **Meeting a Right to Know request for a customer is expected to take an average of 25.6 hours**
  California residents can request to see the data a firm holds on them, under the right to know provision. Respondents estimated it would take 25.6 hours on average to respond to a single right to know request from a customer—although the median is 6 hours which indicates a wide variation in process maturity across organizations. At 6 hours per request, one full-time employee can process just over six requests per week. At 25.6 hours each, one full-time employee can process only one and a half requests per week. Organizations without effective technical solutions to streamline their response to these requests will face rapidly escalating processing costs. A recent study found that Fortune 500 retailers received an average of 230 requests per year under CCPA.[4]

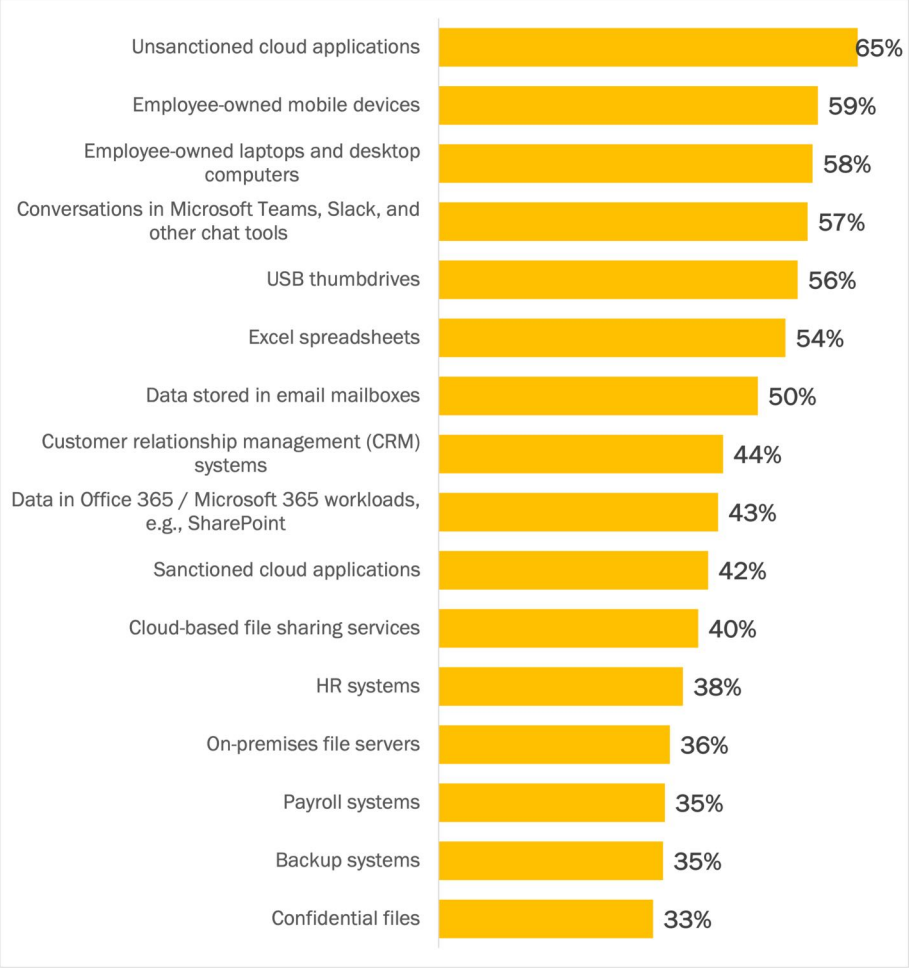
80%

Organizations that do not control 100% of corporate data.

INADEQUATE CONTROLS FOR IDENTIFYING PERSONAL AND SENSITIVE PERSONAL INFORMATION COVERED BY CPRA

Personal and sensitive personal information covered by CPRA requirements is stored across a multitude of data sources. Echoing the earlier finding that less than a quarter of organizations currently have "very mature" data privacy capabilities (Figure 4), many organizations indicate low levels of effectiveness at identifying covered data across common data sources. See Figure 12.

Figure 12
Data Sources with Inadequate Controls for Identifying CPRA-Covered Data
Percentage of respondents indicating low levels of effectiveness



Source: Osterman Research (2021)

Many organizations cannot identify data covered by CPRA across common data sources.

The current lack of effectiveness in identifying covered data across the above data sources is concerning. For instance:

- **Widespread usage of unsanctioned cloud applications**
  One recent study found that 97% of the cloud apps used in the enterprise were unsanctioned, due to business units and employees adopting new services to meet their productivity needs.[5] Unsanctioned services that are not controlled by IT, security, and data protection measures represent a massive risk for organizations.

- **Widespread adoption of Microsoft Teams, Slack, and other chat tools**
  The pandemic of 2020 drove rapid adoption of Microsoft Teams, Slack, and other chat tools.[6] A significant number of employees within organizations are now using these tools to communicate internally and externally, to share access to files containing sensitive and confidential data, and to hold online meetings to collaborate around shared content and ideas. Almost 60% of organizations say they do not have adequate capabilities to identify CPRA-covered data in these tools, which represents a significant shortcoming in the compliance toolset given the changing basis of productivity and collaboration on the front lines. In the case of Microsoft Teams, Microsoft has changed default settings for sharing and guest access multiple times, which further threatens the compliance posture of organizations paying only scant attention to the changing specifics.

- **Data stored in email mailboxes is a key focus for phishing attacks**
  Cybercriminals launch phishing and spear-phishing attacks, deploy malware, and use brute-force methods to guess passwords as inroads to accessing email accounts, both for the data contained inside and the ability to send further attacks using trusted and high-reputation email messages. Email is widely used for responding to customer inquiries, sending documents and files containing personal and sensitive personal information on customers and employees, and distributing spreadsheets of prospects for marketing campaigns. With many cloud-based email services offering mailboxes of 50GB to 100GB in size, even a single compromised email account offers access to a huge volume of data on customers and employees. One half of organizations say they do not have effective means of identifying data covered by the CPRA in email accounts.

- **Email messages are a key source of data leaks**
  Email presents a second critical challenge for CPRA compliance beyond just what is stored in the mailbox: email messages represent a key source of data leaks. Leakage vectors include messages sent to the wrong person due to type-ahead misaddressing, distribution of spreadsheets containing sensitive customer data without appropriate content controls (e.g., encryption), and casual conversations about a customer that include reference to personal and sensitive information that should be better protected.

- **HR systems and payroll systems contain personal and sensitive data on employees**
  HR and payroll systems hold a wide selection of data on employees that is covered under the CPRA for any employee that is a resident of California. Covered data types include postal addresses, email addresses, Social Security numbers, professional and employment-related information, and bank account details. Between one third and two fifths of organizations say they lack sufficient capabilities to identify data covered by the CPRA in these systems. This is especially concerning with the adoption of cloud services for HR and payroll functions, where a data breach has the potential to implicate thousands of organizations and millions of sensitive records.[7]

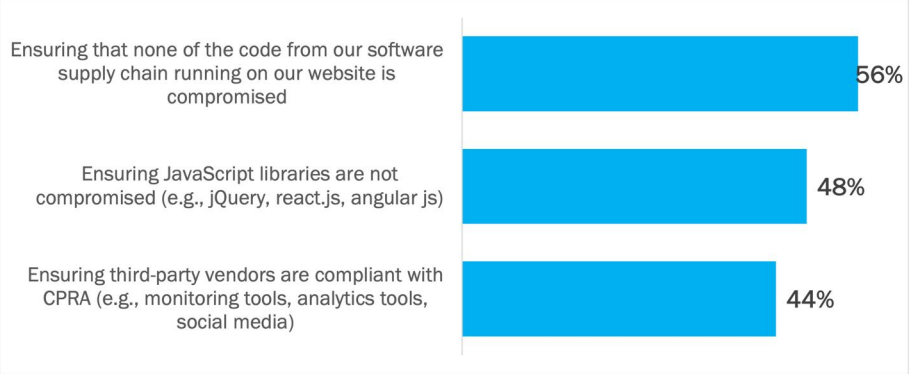
57%

Organizations without adequate controls over content shared in Microsoft Teams, Slack, and other chat tools.

RISKS FOR CPRA COMPLIANCE ON CORPORATE WEBSITE

Code obtained from third-party vendors for a customer-facing website is a risk vector that can introduce vulnerabilities, open backdoors for data theft, and compromise the exercise of data rights under CPRA. Organizations using third-party vendors for website code need methods for assuring that the code is not compromised. On average, only half of respondents indicate they have effective approaches in place for addressing several risks associated with third-party website code. See Figure 13.

Figure 13
Controls on Customer-Facing Websites for CPRA
Percentage of respondents indicating "highly" or "extremely" effective



Source: Osterman Research (2021)

By implication, on average, one half of organizations lack effective processes to ensure code supplied by third-party vendors is compliant with CPRA and not compromised. Although the code is sourced from another party, the use of vulnerable third-party code directly impacts the firm using it. Specific risks include:

- **Inability to assure the security integrity of third-party code (44% of organizations have inadequate protections)**
  With corporate websites being a key channel for collecting and processing customer data, the inability to assure the security integrity of all code is extremely worrying for any firm representing that they abide by CPRA provisions. On the one hand, the firm says that it extends CPRA rights to residents of California, while on the other hand it is unable to assure that no data is being exfiltrated by compromised website code. More than two out of five organizations indicate they lack the means of ensuring that code from their software supply chain is not compromised.
- **Lack of awareness of status of CPRA compliance by third-party vendors (56% of organizations have inadequate methods)**
  Data breaches have severe consequences for organizations, including brand damage, loss of corporate reputation, loss of future revenue, and potential lawsuits resulting from an attack. Third-party website tools are added to corporate websites to cover a variety of purposes, including monitoring, analytics, and social media, all of which have differing levels of access to website data. Almost three out of five organizations do not have the ability to ensure third-party vendors are compliant with the CPRA.

56%

Organizations lacking the ability to ensure third-party vendors are compliant with CPRA.

TIMEFRAMES FOR PRACTICES ESSENTIAL TO CPRA COMPLIANCE

The CPRA is being introduced through a series of rolling implementation deadlines, with several deadlines in 2022 and full enforcement from mid-2023. Organizations have up to 18 months to get fully ready for the coming CPRA mandates, but many have yet to complete important preparatory tasks (see Figure 14).

Figure 14
Getting Ready for the CPRA
Percentage of respondents

Source: Osterman Research (2021)

- **End-to-end data privacy required for CPRA compliance**
  Securing personal and sensitive personal data demands an end-to-end approach, not merely getting the initial collection perfect. If employees send or share protected data using unprotected methods that are easily breached, organizations will quickly fall out of compliance with the CPRA mandates and expose themselves to liability from regulators. One half of organizations have not yet considered all forms of data privacy throughout its full lifecycle and in all the forms it may take, e.g., electronic, paper, etc.
- **Current data protection policies need to be audited for CPRA alignment**
  The CPRA introduces new and modified rights for residents of California, and whatever approach a firm currently takes in their data protection policies will need to be reviewed for alignment, completeness, and accuracy against the elevated requirements in the CPRA. Half of organizations have not yet audited their current data protection policies to make this assessment.
- **Consent has a specific definition, and general terms of use do not count**
  Consent from a consumer provides a business with the legal basis for using personal or sensitive personal information. Consent must be a "freely given, specific, informed and unambiguous indication of the consumer's wishes," and excludes the use of a general "Terms of Use" document that mixes details of personal information processing with other unrelated provisions. Three out of five organizations have not yet reviewed how they obtain consent in light of the CPRA.
- **Over half of organizations do not yet have a training program on CPRA responsibilities**
  Technology solutions to enable CPRA compliance are implemented within the context of organizational processes and employee behaviors. All three aspects must work together to deliver maximum effect, as employee actions that are ill-advised, careless, or negligent can undermine a firm's CPRA compliance posture. Offering a training program customized to the needs of the firm in order to inform, educate, and equip employees to meet their part of the overall CPRA compliance strategy is an essential task for organizations to address.

54%

Organizations without a training program on CPRA for employees.

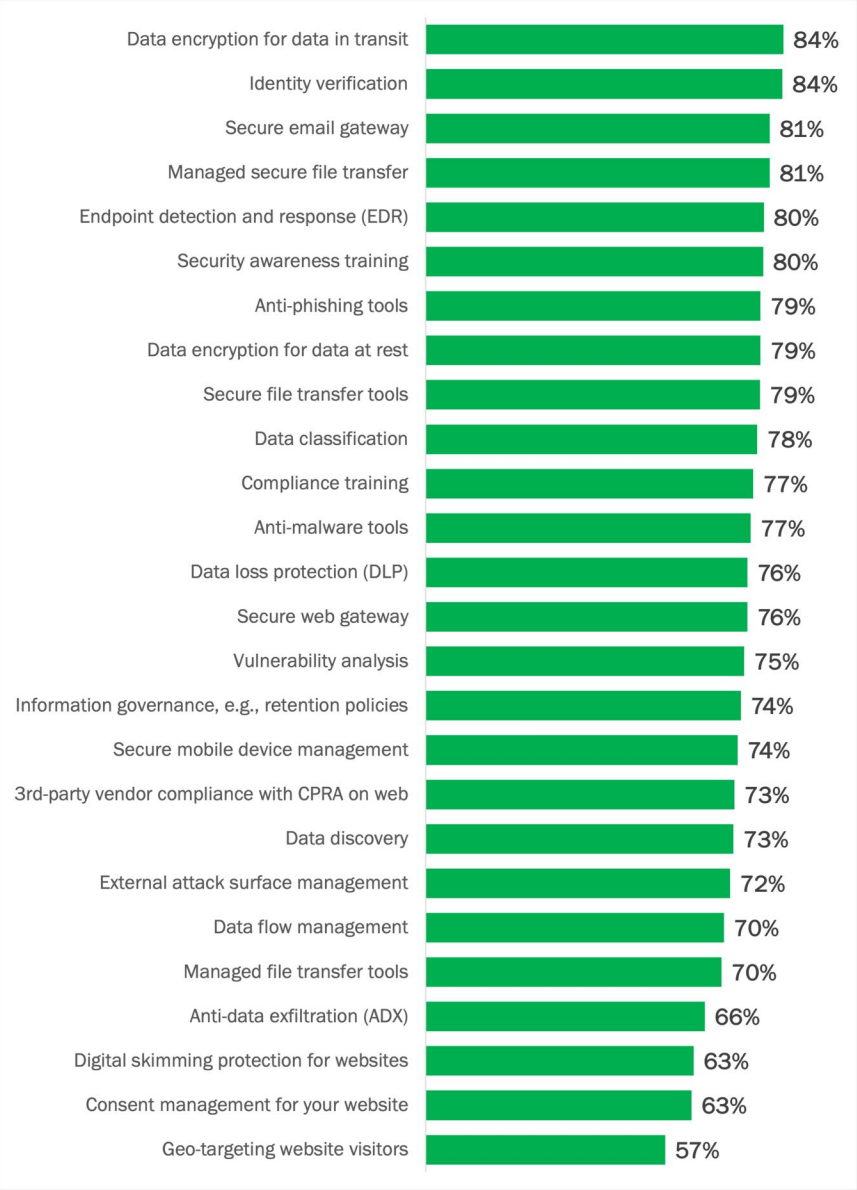
Solutions for CPRA Compliance

In this section, we look at the solutions available for achieving CPRA compliance.

IMPORTANCE OF SOLUTIONS FOR CPRA COMPLIANCE

Organizations see a range of solutions as important for achieving CPRA compliance, with data encryption, identity verification, and a secure email gateway the highest-rated solutions. Many of these solutions are viewed as being of high importance, as the variation between the top 10 is only 6% and the top 17 out of the 24 is only 10%. See Figure 15.

Figure 15
Solutions That are Important for CPRA Compliance
Percentage of respondents indicating "important" or "extremely important"



Source: Osterman Research (2021)

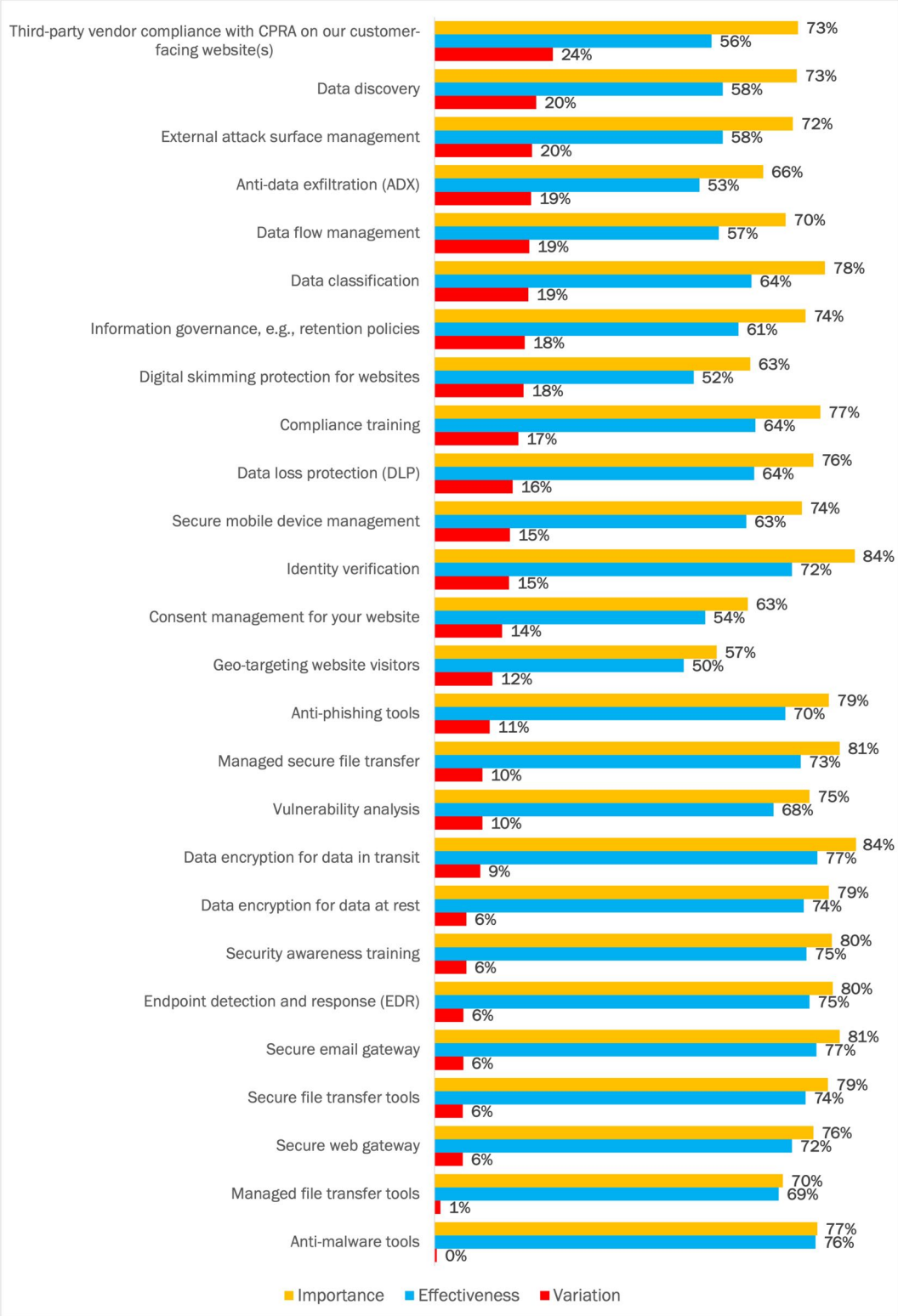
Data encryption, identity verification, and a secure email gateway are viewed as the most important solutions for achieving CPRA compliance.

There is a variation or unfilled gap between the importance of a solution category and the effectiveness of currently deployed solutions in that category. In every case, organizations see higher levels of importance than what their current solutions can deliver. See Figure 16. We make the following observations on the variation between importance and current effectiveness:

- **The three largest gaps relate to website, data discovery, and attack surface**
  Ensuring third-party vendor compliance with CPRA on customer-facing websites is the solution category with the largest variation between importance and current effectiveness. Any firm using a customer-facing website to capture customer data needs to ensure that any third-party code running on their website does not create vulnerabilities for data theft, overexposure, and non-compliance. The ability to discover where personal and sensitive personal data is stored within and across the firm—including on-premises and cloud-based applications—is the solution category with the second highest variation between importance and current effectiveness. External attack surface management is in third place; this solution category enables the proactive identification of weaknesses and vulnerabilities in cybersecurity defenses that could be compromised.
- **Solutions for a group of core data disciplines and practices are lacking**
  Data discovery (20% variation between importance and current effectiveness), data flow management (19%), data classification (19%), and information governance (18%) are four of the top seven solution categories ranked by the variation between importance and current effectiveness. These four solution categories represent a group of core disciplines and practices related to all things data—from discovery, management, protection, retention, and managed disposition. Protecting data in light of the CPRA and delivering on the requirements of rights requests for data subjects requires a significant uplift in core data disciplines. There is work required over the next 18 months to add solutions, processes, and training to address these current shortcomings.
- **Organizations believe that some of the most important categories are well covered**
  Several of the solution categories that ranked highly for importance in Figure 15 rank towards the lower end of Figure 16, such as a secure email gateway (81% importance, 77% current effectiveness) and secure file transfer tools (79% importance, 74% current effectiveness). This means that organizations believe they have adequately addressed some of the more highly important areas.
- **Identity verification is going to become critically important**
  Identity verification is viewed as the second most important solution (84%). This issue will become critically important so that rights requests can be tied to the actual individual rather than an imposter using stolen account credentials. Identity fraud will become a much more significant problem when rights are processed due to a request made by an imposter. False deletion requests will wipe the actual individual's data footprint from a service. Access requests will see the firm participating willingly—albeit under false pretenses—in a data breach of personal and sensitive data. Stronger forms of verifying customer identity, with biometric methods among the strongest, will become essential to ensure data rights can be exercised only by the right person.

Solutions that enable identity verification will become critically important so that rights requests can be tied to the actual individual rather than an imposter using stolen account credentials.

Figure 16
Importance and Effectiveness of Solutions for Achieving CPRA Compliance
Percentage of respondents indicating high importance and high effectiveness, and the percentage variation between the two



Source: Osterman Research (2021)

- **Solutions for increasing privacy protections for files**
  There are several solutions aimed at increasing privacy protections for files, which are a highly sought-after container of confidential, sensitive, and personal data. Much of this data is stored in loosely controlled Microsoft Office documents. An individual file can relate to a single individual (e.g., a contract for service) or thousands of employees or customers (e.g., an Excel spreadsheet with payroll details for employees, purchase history for customers, or an export of customer details for an email marketing campaign)—all of which are data types covered by CPRA requirements. Files are under threat from multiple directions, such as cybercriminals who want access to mine files for personally identifiable information that can be used in attacks against individuals, as well as accidental insider incidents where sensitive data attached to an email is misdirected. Misdirected emails are a growing problem in organizations; one study found an average of 800 misdirected emails per year for an organization firm with 1,000 employees.[8] In the United Kingdom, misdirected emails were more commonly implicated in data breaches than phishing campaigns in 3Q 2021.[9]

  Managed secure file transfer solutions ranks in fourth place on the importance scale (Figure 15) and is the solution with the highest variation out of three types of file transfer tools (Figure 16). The other two types are secure file transfer tools (with a 6% variation between importance and current effectiveness) and managed file transfer tools (1% variation). Organizations are pivoting towards the combination of a managed service with secure file transfer rather than only managed services or only secure transfer. Both managed secure file transfer and secure file transfer tools also deliver the benefit of data encryption for data in transit, the solution ranked as most important overall.

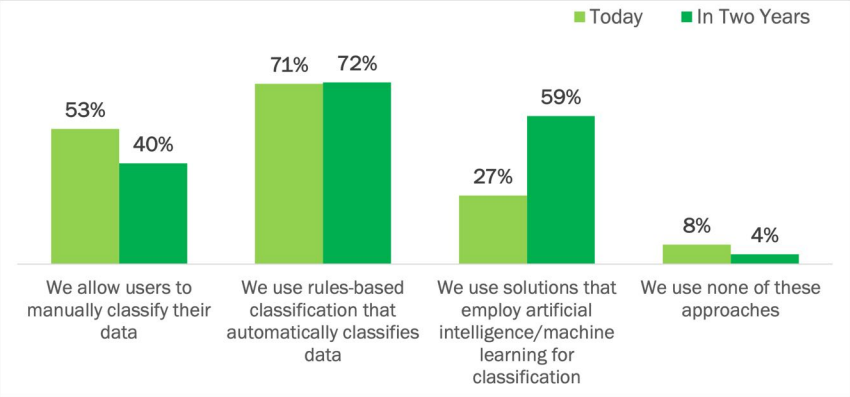
USE MORE ADVANCED FORMS OF AUTOMATED DATA CLASSIFICATION

Classifying data as personal or sensitive information is one of the first steps in ensuring that appropriate protections are enforced. The most common approach currently for classifying data is automatic classification based on rule sets (71% of respondents are currently using this approach), with manual data classification in second place (by 53% of respondents). See Figure 17.

220%

Expected growth in the use of AI/ML for data classification over the next two years.

Figure 17
Use of Data Classification Methods Today and In Two Years
Percentage of respondents



Source: Osterman Research (2021)

Over the next two years, fewer organizations expect to use manual classification approaches—with a drop in usage from 53% to 40%. Manual classification approaches rely on people to get the classification right every time, and perfect practice in perpetuity is impossible to achieve. In line with this limitation, many more organizations will adopt solutions that employ artificial intelligence and machine learning (AI/ML) for data classification—with anticipated growth in usage from 27% of organizations to 59% of organizations (growth rate of 220%).

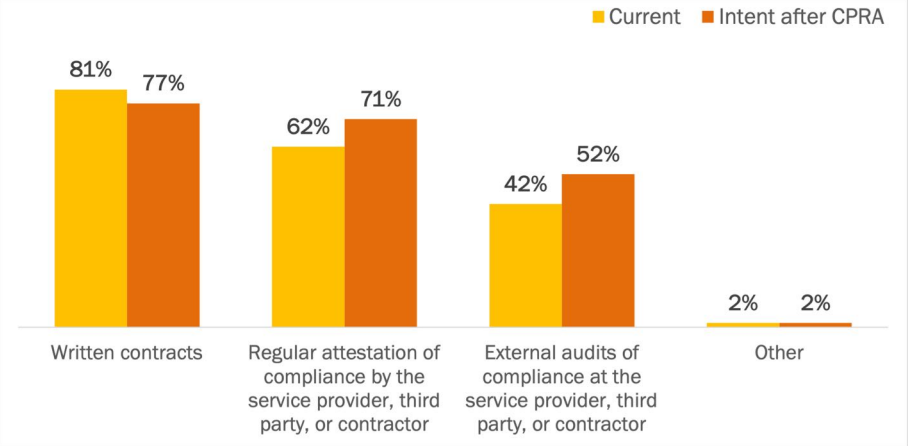
AI/ML promises a less labor-intensive and more accurate way of automatically classifying data across a corpus than relying on rule sets for automatic classification (not to mention manual classification approaches). For rule sets to work effectively, organizations need data classification professionals to monitor rule-based classification decisions and assess false negatives and false positives, and then tune the rule sets accordingly to minimize the incidence of both. On the other hand, AI/ML classification will still require human oversight to ensure that private data is not inadvertently misclassified as public data and thus unwittingly exposing the firm to compliance violation risks.

ACTIVELY MANAGE DATA RISK WITH EXTERNAL PARTIES

Organizations currently use several methods of managing the data risk posed by external parties, with written contracts the most used method (by 81% of organizations). After the CPRA goes into force—where businesses bear higher levels of responsibility for what external parties do with covered data—the use of written contracts is expected to decline slightly (to 77% of organizations), while two other more regular and challenging approaches will increase in usage. See Figure 18.

Static point-in-time agreements for managing data risk with external parties are ineffective at identifying and mitigating data risks in practice.

Figure 18
Methods Use for Managing Data Risk with External Parties
Percentage of respondents



Source: Osterman Research (2021)

Static point-in-time agreements for managing data risk with external parties are effective at outlining the legally binding agreements on both sides but are ineffective at identifying and mitigating data risks in practice. Regular attestation of compliance raises the standard of compliance for external parties, and external audits of compliance increase the standard even further. How many organizations go even further and use real-time compliance assessments for assessing data risks at external parties remains to be seen.

Best Practices for CPRA Compliance

The CPRA is coming—rapidly—and many organizations are ill-prepared to deal with its requirements. We offer the following best practices for complying with the CPRA. These practices require a healthy mix of competent people, well-designed organizational processes, and technology solutions to enable, enact, and meet.

1. **Understand what you are required to do**
   What data rights are you required to extend to residents of California? This may vary depending on what types of data you collect and process on California residents, what data is sold or shared with other entities, and how many California residents have shared their personal and sensitive information. It will also dictate the need for formal agreements with other entities, annual auditing, and the types of solutions required for compliance.

2. **Know where your covered data is collected, processed, stored, and shared**
   Perform an end-to-end audit of where personal and sensitive personal information is collected from California residents, and how your firm processes, stores, and shares that data. Data discovery and classification tools will be very helpful here. Are there places in the lifecycle of data usage where inferences are made as part of automated decision-making processes? You will need to know those points. It is essential also to have the optics to identify unforeseen data leakage in compromised third-party website code, for example, where a plugin surreptitiously shares personal data with unauthorized entities. Starting with a point-in-time inventory of data assets and covered data is great but stopping there is not. You will need the optics to discover and classify covered data in perpetuity.

3. **Combine process design, education, and technology for compliance**
   People work with technology solutions within organizational processes to deliver the requirements of the CPRA. Combine the three components so they work together: design effective processes using efficient technologies and a team of competent individuals. Deploy technology solutions to directly enable specific parts of the CPRA, such as tools for data discovery, data masking and encryption, secure transfer of data, marking data for exclusion from automated decision-making, and managed disposition to minimize data retained on California residents. But also deploy new or strengthen current technology solutions that address data protections more generally, such as stronger forms of identity verification for employees and customers, anti-phishing to reduce credential theft, and cloud security tools that continually scan cloud services for configuration errors, drift, and data covered by CPRA.

4. **Equip employees with the knowledge, competence, and confidence to comply with the CPRA**
   The design of processes that contravene the CPRA starts with people innocently, negligently, or deliberately going outside of its parameters. Employees need to know what they are allowed to do with personal and sensitive personal information within the framework of the CPRA (and the wider dynamic regulatory landscape), what is disallowed, and what risky processing looks like. Educate employees to create clarity of expectations, while also using technology such as insider risk analytics to provide visibility into employee behavior that is trending towards negligent or malicious. Continual visibility of employee behavior provides direction for corrective actions at the organizational level—e.g., coaching, training, or sanctions.

Design effective processes using efficient technologies and a team of competent individuals to meet CPRA requirements.

5. **Comply with CPRA and get ready for a changing regulatory landscape**
   CPRA applies specifically and exclusively to data on California residents, and while many organizations are planning on extending the rights in CPRA to all customers in the United States, that works only if other states have no specific requirements, there is no harmonized federal regulation, and the rights in CPRA are equivalent to or do not conflict with other current and emerging state-specific regulations. CPRA provides a pattern for what is likely to emerge, not its final formulation. Design organizational processes to support flexibility in the future, choose solutions that enable differential treatments over subsets of data, and equip employees with the skills and competencies needed to work within a dynamic regulatory landscape.

Conclusion

The CPRA is already law, and its rolling implementation timeframe is well underway. The CPRA extends the current CCPA legislation, adds new rights for California residents, creates a new dedicated agency to oversee its implementation and enforcement, and modifies definitions and applicability from the original CCPA. Complying with the CPRA requires organizations to mature their organizational and technical approaches to data privacy, a journey which many have begun but in which few are currently excelling. Organizations subject to the CPRA need to rapidly address current shortcomings in organizational and technical approaches to data privacy, and those not immediately subject to CPRA should take note of the changing regulatory landscape for how personal and sensitive personal information is used.

Comply with CPRA and get ready for a changing regulatory landscape.

Sponsored by ActiveNav

ActiveNav is a data privacy and governance software provider and innovator of DMaaS (Data Mapping as a Service). With ActiveNav, organizations can map, clean, classify, quarantine, and delete sensitive, redundant, obsolete, and trivial data. Hundreds of leading companies and government agencies trust ActiveNav to help them control sensitive data and support compliance with various data privacy regulations such as the CPRA, CCPA, and GDPR. ActiveNav Inc. is headquartered in the DC metro area and has offices in Europe and Australia.

For more information, please visit ActiveNav.com.

www.activenav.com
@ActiveNav
usa-sales@activenav.com
+1 571 375 2780

[1] Osterman Research, Key Steps in Satisfying Your CCPA and Other Privacy Obligations, December 2019, at https://ostermanresearch.com/2019/12/18/orwp_0318/
[2] See https://cppa.ca.gov
[3] California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21), September 2021, at https://www.cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf
[4] The National Law Review, How Many Access Requests Do Retailers Receive on Average Each Year?, September 2021, at https://www.natlawreview.com/article/how-many-access-requests-do-retailers-receive-average-each-year
[5] Netskope, Cloud and Threat Report - July 2021, July 2021, at https://resources.netskope.com/cloud-reports/cloud-and-threat-report-july-2021
[6] Osterman Research, Archiving and Data Protection with Microsoft Teams, May 2021, at https://ostermanresearch.com/2021/05/11/orwp_0338/
[7] Emily Kuhnert, Payroll Security Breaches, February 2020, at https://papayaglobal.com/blog/list-of-payroll-security-breaches/
[8] Tessian, Why DLP Has Failed and What the Future Looks Like, December 2020, at https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/
[9] ICO, Data security incident trends: Q2 2021-22, October 2021, at https://ico.org.uk/action-weve-taken/data-security-incident-trends/