Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2023**
Sponsored by **OpenText Cybersecurity**

Privacy Compliance in North America: Status and Progress in 2023

Executive Summary

Organizations collect, process, and store a wide range of data on individuals—including data that is personal, sensitive, related to healthcare and education, and financial. In addition to data collected with the knowledge of individuals, the widespread adoption of new digital channels for people to meet, share, and shop has dramatically increased the scope for organizations to capture data surreptitiously. Current and emerging regulations set a baseline expectation that organizations will, firstly, protect all such data appropriately, and secondly, extend a set of rights to the individuals whose data has been collected, processed, and stored. The implications of elevated privacy requirements are reverberating inside organizations across many industries.

This white paper reports on how organizations in the United States and Canada are meeting the requirements of current and emerging privacy regulations.

KEY TAKEAWAYS

- **Claims of maturity not supported by security realities**
  Organizations claim higher levels of maturity in complying with privacy regulations, but these claims of maturity are not met by security realities. More organizations are experiencing a higher number of data breach types.
- **Growing intent to extend a synthesized set of rights from state-level regulations to all residents in the United States**
  More organizations are treating the rise of state-level privacy regulations as a signal for taking a unified approach to offering privacy rights to all United States residents, even without the forced demand of federal regulation.
- **Compliance and legal teams evidence a lower commitment to privacy**
  Understanding new and emerging regulations is a core responsibility for compliance and legal teams, as is strategizing how to mitigate the associated risks to which an organization is exposed. The conceptual understanding of the importance of privacy regulations is declining in these groups, which bodes poorly for the wider organization.
- **Insufficient capabilities to discover data requiring protection**
  Only half of organizations are confident in their ability to discover personal and sensitive data in the commonly used cloud services, servers, and systems where such data is likely to be found. Widespread adoption of SaaS apps, for example, is not being met with an equivalent emphasis on security.
- **Elevating protections and readiness key for the next wave**
  Achieving higher levels of maturity with emerging privacy regulations requires organizations to invest the time to establish required controls, engage with the right groups across the organization, and deploy new and more effective technical solutions. Data classification and data encryption play a vital role in this process, along with better ways of managing risks of third-party data access and SaaS misconfigurations.
- **Employees remain a key threat to privacy compliance**
  Employees have authorized access to personal and sensitive data on people, and hence can breach data through unintended, unwitting, or deliberate actions.

The widespread adoption of new digital channels for people to meet, share, and shop has dramatically increased the scope for organizations to capture data surreptitiously.

ABOUT THIS WHITE PAPER

This white paper is sponsored by OpenText Cybersecurity. Information about OpenText Cybersecurity is provided at the end of this paper.

ABOUT THE 2023 SURVEY

This white paper references data from an in-depth survey conducted in March and April 2023 of 131 professionals in North America. All respondents were familiar with how their organization was addressing the requirements of privacy regulations applicable to their organization. This is the second year we have conducted this survey.

The 2023 survey on privacy compliance is largely consistent with our 2022 survey, with most of the questions asked in both years. Both surveys collected data from a random sampling of organizations. There are three main differences between the two surveys which somewhat alter the efficacy of year-on-year comparisons:

- **Expanded geographical focus**
  The 2022 survey was fielded exclusively in the United States. The 2023 survey was fielded in both Canada and the United States to provide a North American view. Just under 20% of respondents were from Canada.
- **Reduced scope for differential interpretation of questions**
  Several questions in the 2022 survey allowed respondents latitude to interpret the wording, for example what was meant by a "medium" or "extreme" amount of time. In the 2023 survey, we tightened the wording to include pre-specified timeframes, for example "4 to 6 months" and "more than 12 months."
- **New questions on SaaS apps**
  A couple of new questions were added on the use of and protections for SaaS apps, given the widespread adoption and usage of these apps by organizations. In addition, nuances were added to a few existing questions to probe SaaS app-related issues.

For the 2022 edition of this research, see Privacy Compliance in the United States: Status and Progress in 2022 (published April 2022).

Organizations are subject to a range of federal, industry-specific, and state-level privacy regulations.

ABOUT PRIVACY REGULATIONS

The privacy regulations of particular interest in this survey were:

- **HIPAA (Health Insurance Portability and Accountability Act)**
  A federal law in the United States for the healthcare sector. Focused on protecting sensitive health information on patients. Requires protections against internal and external risks, along with a holistic group of safeguards to assure confidentiality, integrity, and availability of covered data.
- **New and emerging state-level data privacy regulations**
  Several US states had state-specific privacy regulations at the time of the survey: California (the combined CCPA/CPRA—California Consumer Privacy Act and California Privacy Rights Act), Virginia (Virginia Consumer Data Protection Act or VCDPA), Colorado (Colorado Privacy Act or CPA), and Utah (Utah Consumer Privacy Act or UCPA). All apply based on holding personal data on residents of the state, not based on where the organization holding the data is located. All extend a set of rights to data subjects, such as access to their data. Several other states are also developing privacy laws.
- **GLBA (Gramm-Leach-Bliley Act)**
  Requires financial services institutions, including those offering loans, advice, and insurance, to protect and safeguard sensitive customer data. Includes the need to assure the privacy of financial information held or collected on customers. Financial services institutions must develop a comprehensive security program to protect customer data.

- **FERPA (Family Educational Rights and Privacy Act)**
  A federal law in the United States for the education sector, specifying protections for student records. Certain rights of access and correction are granted to parents until students are 18 or at advanced institutions.
- **PIPEDA (Personal Information Protection and Electronic Documents Act)**
  A Canadian data privacy law that requires private sector organizations in Canada to gain consent to collect, use, or disclose personal data on individuals, and to extend rights of access and correction. Organizations must not use data for purposes beyond which it was originally collected without gaining additional consent from the affected party.
- **GDPR (General Data Protection Regulation)**
  The harmonized data protection regulation for Europe, introduced in May 2018. GDPR ushered in a new standard in data protection and privacy requirements, with obligations for organizations and their data partners and data rights for data subjects. Other countries and states have taken inspiration from GDPR in establishing their own data protection regulations. GDPR applies based on collecting or processing data on European data subjects, rather than on an organization having a physical presence in Europe.

GDPR ushered in a new standard in data protection and privacy requirements, with obligations for organizations and their data partners, and data rights for data subjects.

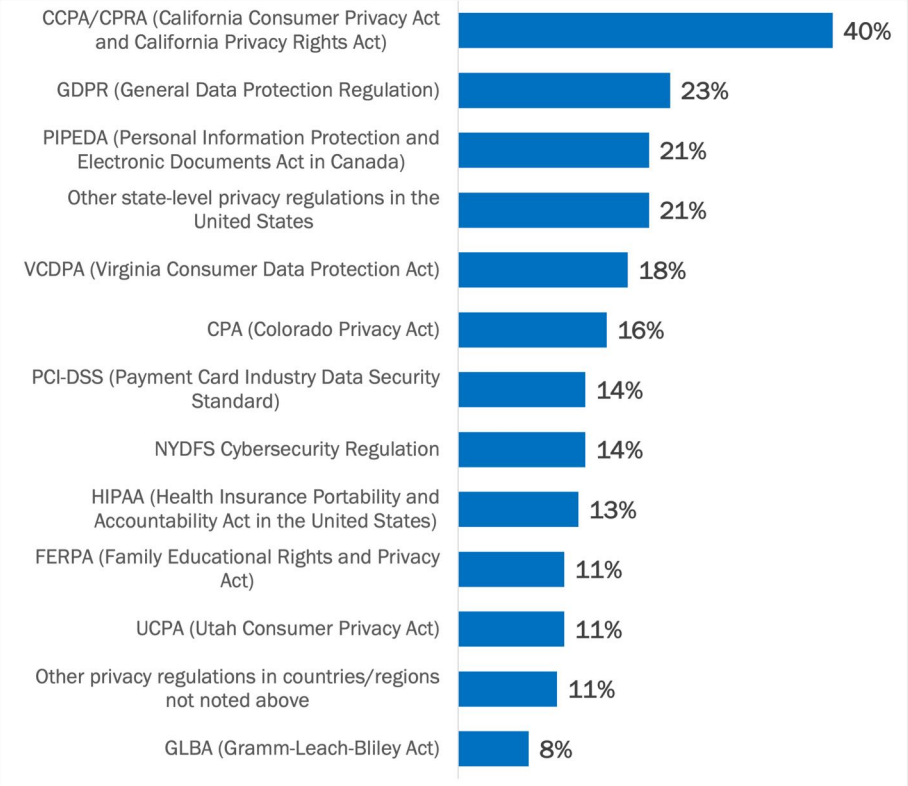
Snapshot of Privacy Compliance in 2023

This section looks at how organizations are currently complying with privacy regulations, including applicable regulations, maturity of compliance, and data breaches over the past 12 months, among others.

PRIVACY REGULATIONS APPLICABLE TO RESPONDENTS

All the organizations in this research are subject to the requirements of one or more privacy regulations. CCPA/CPRA is the most common regulation applicable to respondents (at 40% of organizations), followed by GDPR (23%). See Figure 1. Half of respondents indicated their organization is subject to two or more privacy regulations.

Figure 1
Privacy Regulations Applicable to Respondent Organizations
Percentage of organizations



Source: Osterman Research (2023)

Half of organizations in this research are subject to two or more privacy regulations.

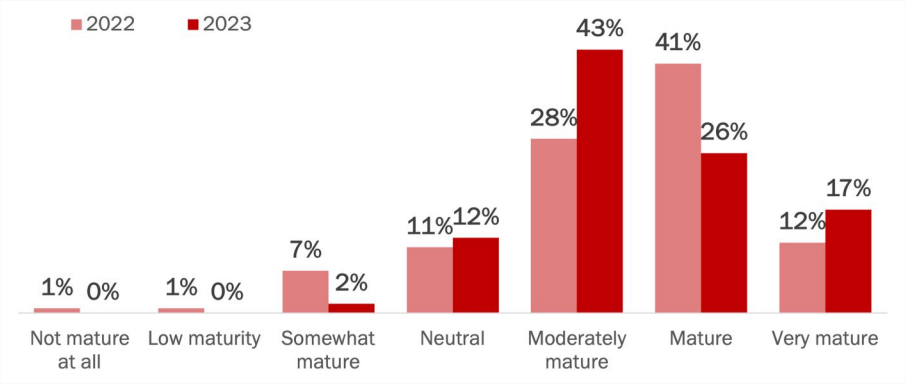
The high rate of applicability of CCPA/CPRA in comparison to the rates of applicability of VCDPA (Virginia), CPA (Colorado), and UCPA (Utah) could be due to various reasons, including the relative size of the Californian economy versus the other states, the location of survey respondents, the longer timeframe that CCPA/CPRA has been in force compared to the newer regulations, and lower levels of understanding on the newer regulations. We expect rates of applicability across the states to even out over time.

In comparison to the 2022 survey findings, the organizations in this research were less affected by HIPAA (67% in 2022) and GDPR (62% in 2022).

MATURITY WITH PRIVACY COMPLIANCE

Forty-three (43%) percent of respondents say their organizations are "mature" or "very mature" in complying with the privacy regulations that are currently enforced (e.g., GDPR, CCPA, HIPAA) versus 53% in the 2022 survey. The shape of maturity is changing year on year, with more respondents this year saying their organizations are "moderately mature" or "very mature," while fewer say they are "mature." In other words, instead of maturity being attained in a stepwise fashion, the changing regulatory environment is causing reversion for some organizations. See Figure 2.

Figure 2
Maturity with Privacy Regulations Currently Enforced: 2022 vs. 2023
Percentage of organizations



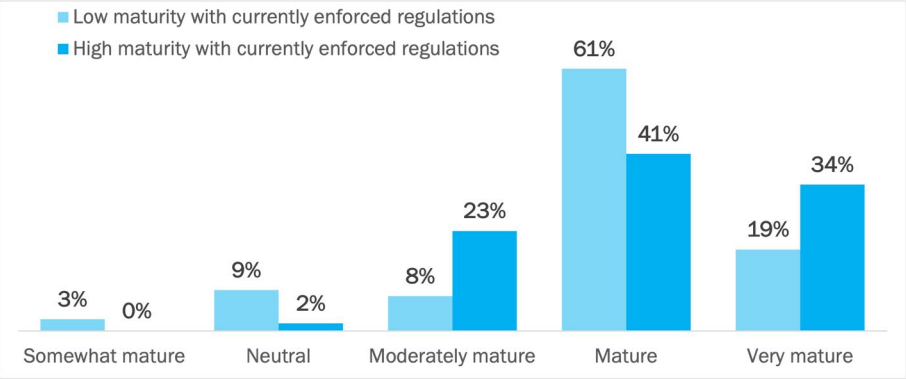
Source: Osterman Research (2023)

Several regulations will transition to enforcement mode in 2023-2024, including VCDPA, CPRA, and UCPA. We split the answers on maturity level for forthcoming regulations by the level of maturity with currently enforced regulations. Among the "low maturity" group (respondents who did not indicate "mature" or "very mature" approaches in 2023), the highest number believe their approach for forthcoming regulations is "mature." This appears ironic since their current foundation is insufficient.

Alternately, most of the "high maturity" group believe their approach is "mature" or "very mature," and that the foundation created by their current compliance efforts is strong enough to carry the weight of what is yet to come. See Figure 3.

Organizations with low maturity in complying with currently enforced regulations ironically believe their approach for forthcoming regulations is highly mature.

Figure 3
Maturity with Forthcoming Privacy Regulations: Low vs. High Maturity
Percentage of organizations

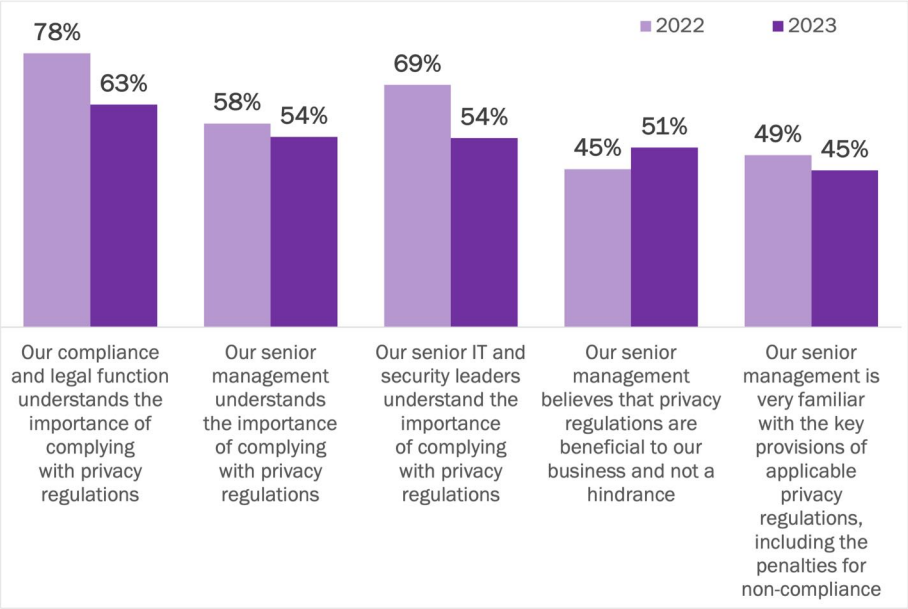


Source: Osterman Research (2023)

WAVERING DECISION-MAKER SUPPORT FOR PRIVACY REGULATIONS

In comparison to our 2022 survey, four types of decision-maker support for complying with privacy regulations have trended downward in this year's survey. On the other hand, more senior managers believe that privacy regulations are beneficial to a business instead of a hindrance—which is progress. See Figure 4.

Figure 4
Support for Privacy Regulations Among Decision-Makers
Percentage of respondents indicating "agree" or "strongly agree"



Source: Osterman Research (2023)

Support for privacy regulations has declined even among groups for whom regulatory and legal compliance is a core responsibility:

- **Compliance and legal function: 19% decline in understanding importance**
  Understanding new and emerging regulations is a core responsibility for compliance and legal teams, as is strategizing how to mitigate the associated risks to which an organization is exposed. Declining levels of conceptual understanding among these groups bodes poorly for the wider organization.
- **Senior IT and security leaders: 22% decline in understanding importance**
  Ensuring that the right mix of technical protections is deployed for data privacy and data security is a core responsibility for senior IT and security leaders. Declining levels of understanding on the importance of privacy regulations establishes a less responsive context for new technical initiatives.

We see two potential reasons. Firstly, the relative lack of enforcement to date doesn't help with setting the expectation that privacy compliance requirements are real. Secondly, the complexity of complying with state-level privacy regulations is increasing. When systematic complexity increases too fast due to divergence of requirements and nuanced demands, senior leaders may take the view that compliance is increasingly impossible. Divergence of regulations with precise and specific demands that apply in unique situations becomes counterproductive to achieving the overall outcome of enhanced privacy rights. By comparison, harmonization of requirements across EU member states was a key driver of GDPR, not variation and nuance in different EU markets.

Declining levels of conceptual understanding among compliance and legal groups of the importance of privacy regulations bodes poorly for the wider organization.

TYPES AND FREQUENCY OF DATA BREACHES HAVE INCREASED

Four out of five organizations have experienced data breaches of personal, sensitive, or confidential data in the past 12 months, up from three out of five in 2022. See Figure 5. The frequency of all data types being breached has also increased year on year, including a 342% increase in the frequency of employee health data being breached, a 290% increase in breaches of corporate intellectual property, and a 140% increase in breaches of employee personal data. Organizations that cannot rely on their framework of organizational and technical protections for any given type of data will be likely to suffer from other types of breaches, too.

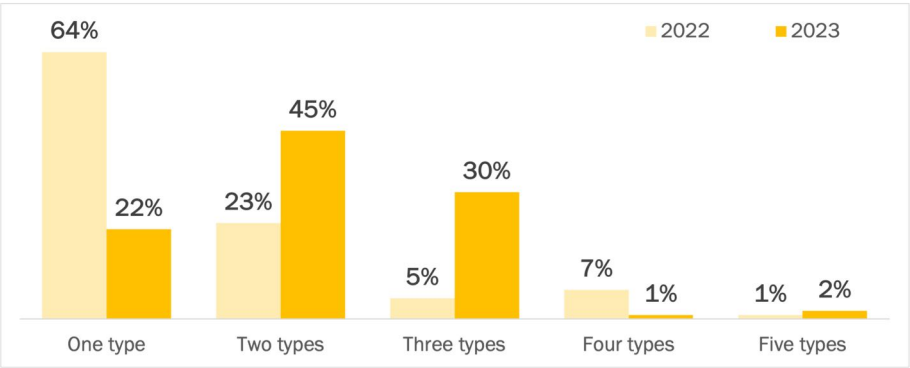
Figure 5
Types of Data Breached During the Past 12 Months
Percentage of organizations

Source: Osterman Research (2023)

Six times as many organizations experienced three types of breach compared to last year.

Year on year, more organizations are experiencing a high number of breach types. The percentage of organizations that experienced two types of breaches doubled from 2022, and the percentage that saw three types of breach increased sixfold. See Figure 6.

Figure 6
Types of Data Breached During the Past 12 Months—Count of Breach Types
Percentage of organizations disclosing types of data breaches

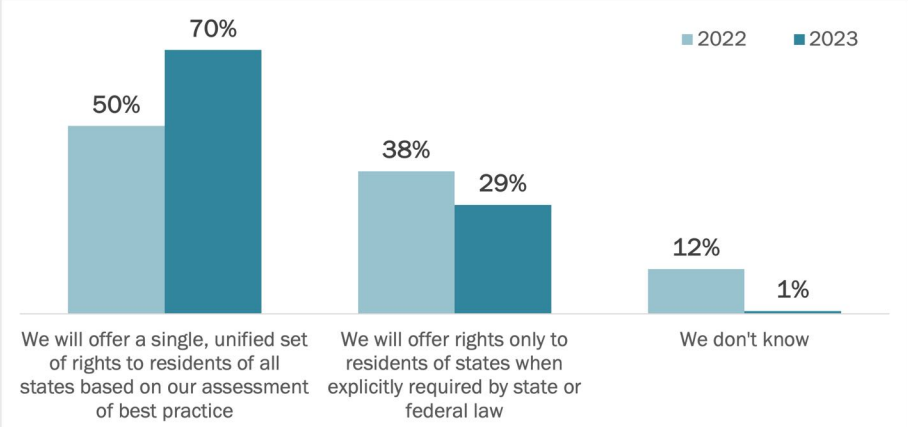


Source: Osterman Research (2023)

ORGANIZATIONS EMBRACING A UNIFIED PRIVACY FRAMEWORK

In the absence of a federal-level privacy regulation in the United States, organizations are pushing in the direction of offering a single unified set of rights to residents of all states based on an assessment of best practices. Embracing a synthesized approach that applies across the board is the preferred approach for organizations in 2023, compared to withholding data rights when state and federal laws do not exist. Unlike in 2022, when one in eight organizations had not decided how to handle this conundrum, only one in a hundred remain undecided in 2023. See Figure 7.

Figure 7
Extending Data Privacy Rights to States with No Data Privacy Regulation
Percentage of organizations

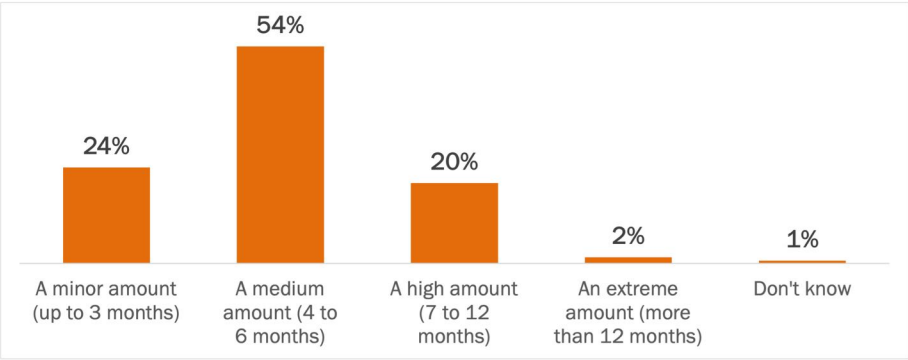


Source: Osterman Research (2023)

Embracing a unified privacy framework that extends rights to everyone irrespective of geography is a positive and commendable development but may not offer a complete approach. The need for flexibility in addressing regulatory nuances by state will be essential if new state-level regulations impose irreconcilable requirements that cannot be synthesized. Inflexible data privacy controls will impose high costs on organizations downstream if requirements cannot be synthesized.

If the United States introduced a federal data privacy regulation that was broadly equivalent to current state-level data privacy regulations, most respondents believe their organization would be able to comply within six months. See Figure 8.

Figure 8
Expected Time to Comply with a Hypothetical US Federal Privacy Regulation
Percentage of organizations



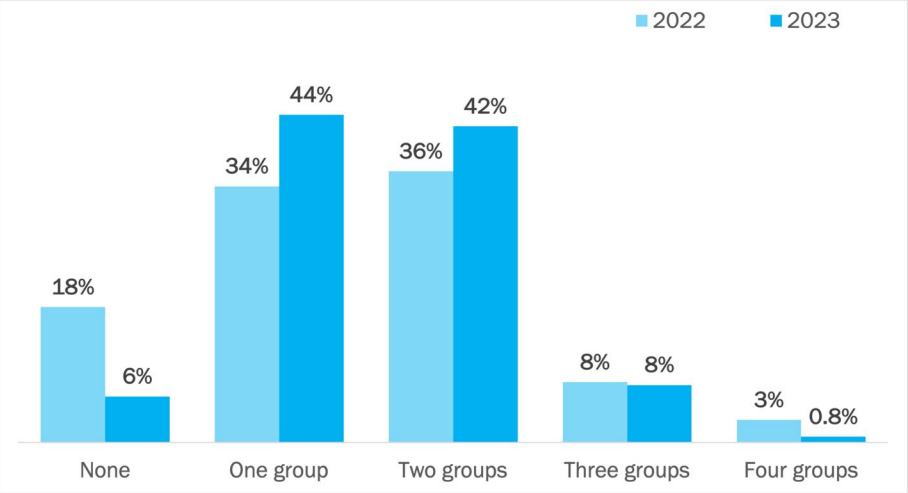
Source: Osterman Research (2023)

Most organizations plan on offering a single unified set of rights to residents of all states based on an assessment of best practices.

GREATER CLARITY ON OWNERSHIP AND OVERSIGHT OF PRIVACY

During the past year, organizations have made progress in defining who is responsible for overseeing privacy compliance. In 2023, more organizations are relying on one or two defined groups for providing oversight, with the largest migration away from having no group defined (which decreased from 18% of organizations in 2022 to 6% in 2023). Fewer organizations are also relying on four groups. Clearly defined lines of responsibility for overseeing privacy compliance mean an organization has a greater chance of moving in the right direction and minimizing instances when privacy requirements are ignored. See Figure 9.

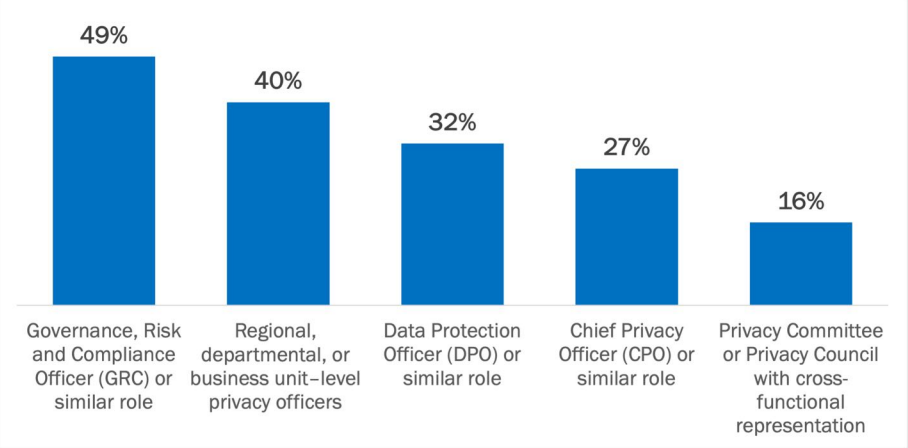
Figure 9
Roles or Groups for Providing Oversight for Privacy Compliance: 2022 vs. 2023
Percentage of organizations



Source: Osterman Research (2023)

The most common group for holding oversight responsibility in 2023 is a Governance, Risk and Compliance officer (at 49% of organizations), followed by regional, departmental, or business unit–level privacy officers (40%). See Figure 10.

Figure 10
Roles or Groups for Providing Oversight for Privacy Compliance
Percentage of organizations (half have two or more of the roles/groups below)



Source: Osterman Research (2023)

Clearly defined lines of responsibility for overseeing privacy compliance minimize the likelihood that privacy requirements are ignored.

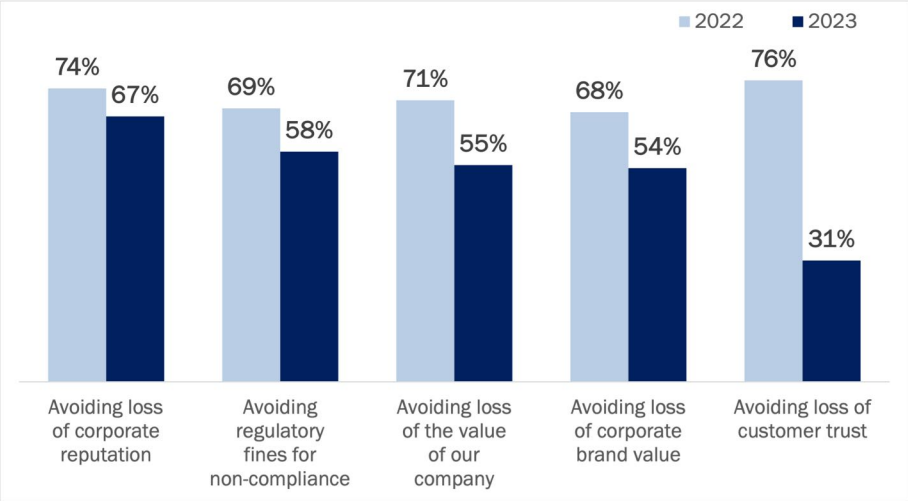
Moving Toward Maturity: Setting the Organizational and Technical Context

This section explores how organizations are moving toward maturity in complying with privacy regulations, including motivators, data classification, and the efficacy of data discovery across commonly used data sources.

DECIDE WHY PRIVACY COMPLIANCE IS IMPORTANT TO YOUR ORGANIZATION

Loss of corporate reputation is the leading motivator in 2023 for complying with privacy regulations (67%), followed by avoiding regulatory fines for non-compliance (58%). The "reputation" of an organization is an overall synthesis of all behaviors, approaches, and practices that affect other people and organizations; it is a pre-engagement assertion of how others should expect to be treated. All five motivators have declined in intensity for the respondents to the survey this year compared to the 2022 survey. See Figure 11.

Figure 11
Importance of Motivators for Complying with Privacy Regulations
Percentage of respondents indicating "important" or "extremely important"



Source: Osterman Research (2023)

Organizations do not appear to be connecting the dots between customer trust and corporate reputation, market value, and brand value.

The importance of avoiding loss of customer trust significantly changed year on year, dropping in ranking from first place in 2022 (76%) to fifth place in 2023 (31%). As it stands this year, the initial four motivators—focused largely inward on the organization—are rated twice as important on average than the loss of customer trust. This demotion of customer trust to such an insignificant concern is perplexing, since customer trust is an input to corporate reputation, company value, and corporate brand value. Losing customer trust through a data breach or poor data handling practices can rapidly erase value that has taken years or decades to build.

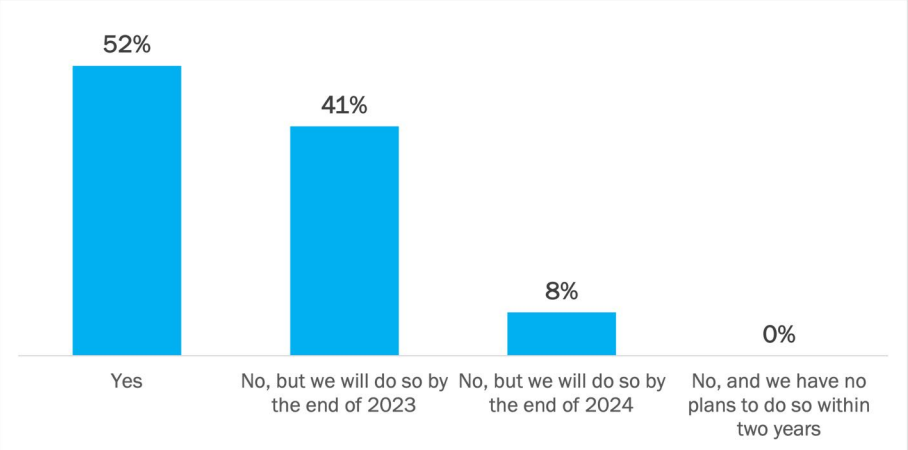
Alternately, perhaps organizations have decided that some level of breach is now acceptable and that the loss of customer trust is only short-term.

AUDIT WHERE PERSONAL DATA IS LOCATED

One approach to protecting personal data is to protect all data through technologies like encryption, irrespective of the different types of data held across corporate data stores. Such a blunt approach to data protection is often viewed as the solution for organizations with low maturity in data handling practices,[1] even though higher energy consumption costs are required to handle the additional computing load. It also does not guarantee against data breaches when employees are not taught to respect nuances between data types.

Organizations with higher maturity in data handling evidence a greater proclivity for data discovery and data classification processes. In this research, just over half of respondents have already conducted a data audit to determine where personal and sensitive personal data is located across their organization (52%), and a further 41% plan on doing so by the end of 2023. This leaves less than one in ten organizations unaccounted for. See Figure 12.

Figure 12
Timeline for Conducting a Data Audit of Personal and Sensitive Personal Data
Percentage of respondents



Source: Osterman Research (2023)

Encryption does not guarantee against data breaches when employees are not taught to respect nuances between data types.

Fewer organizations in this year's research have completed a data audit than indicated by the 2022 forecast, in which 80% of organizations were planning to have completed a data audit by the end of 2022. Intent towards planned activities is an essential first step but requires execution to complete. It seems like many organizations are struggling to translate the intent into a completed data audit.

The other change year-on-year is that 8% of organizations in the 2022 survey indicated they had no plans to complete a data audit by the end of 2024. In this survey, all organizations indicate that a data audit has been or will be completed by the end of 2024. No organizations are still planning to avoid the task.

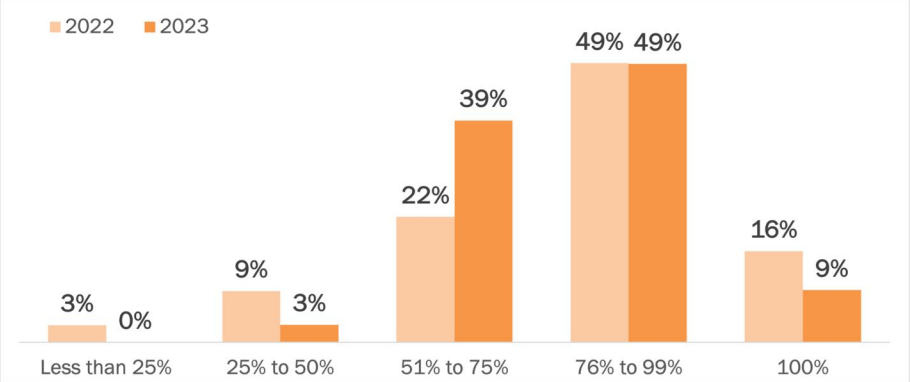
Conducting a point-in-time data audit is an essential first step for organizations in creating a data inventory, but they should not stop there. Regular data audits map the evolving storage locations and hidden drift of personal data across organizations, and real-time data auditing tools for data discovery, analysis, and classification offer real-time optics to drive real-time protections.

CLASSIFY ALL CORPORATE-OWNED DATA

Appropriately protecting data depends on the ability to classify data. Personal health data covered by HIPAA, financial data covered by GLBA (among others), educational records by FERPA, and personal and sensitive personal data by state-level privacy regulations have different protection requirements and breach consequences. Without the capability to classify all data, an organization can never be certain that everything that requires protection is protected. Organizations should ensure they have privacy-enhancing technology available—for classification by data type and risk scoring for prioritization of mitigation projects.

In this research, around 60% of organizations indicate they can classify more than three-fourths of corporate-owned data, including 9% saying they can classify everything. In comparison to the 2022 survey, fewer can classify everything (decreased from 16% in 2022 to 9% currently) and more can classify 51% to 75% of corporate-owned data (increased from 22% to 39%). See Figure 13.

Figure 13
Capability to Classify Corporate-Owned Data
Percentage of organizations

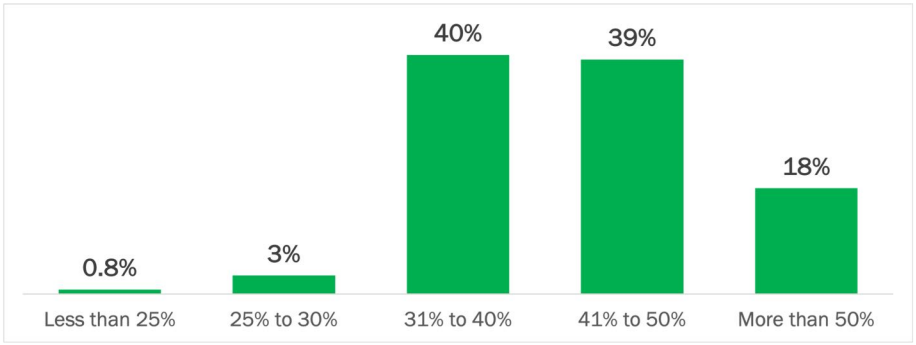


Source: Osterman Research (2023)

Lacking the capability to classify 100% of data means that an organization can never be certain that everything that requires protection is protected.

In a sign of how critical SaaS apps have become to organizations, 96% of respondents indicate that more than 30% of their classifiable corporate-owned data resides in such apps. The widespread adoption and usage of SaaS apps for creating, capturing, storing, and processing corporate data must be met by appropriate data, access, and security protections. See Figure 14.

Figure 14
Data in SaaS Apps
Percentage of organizations

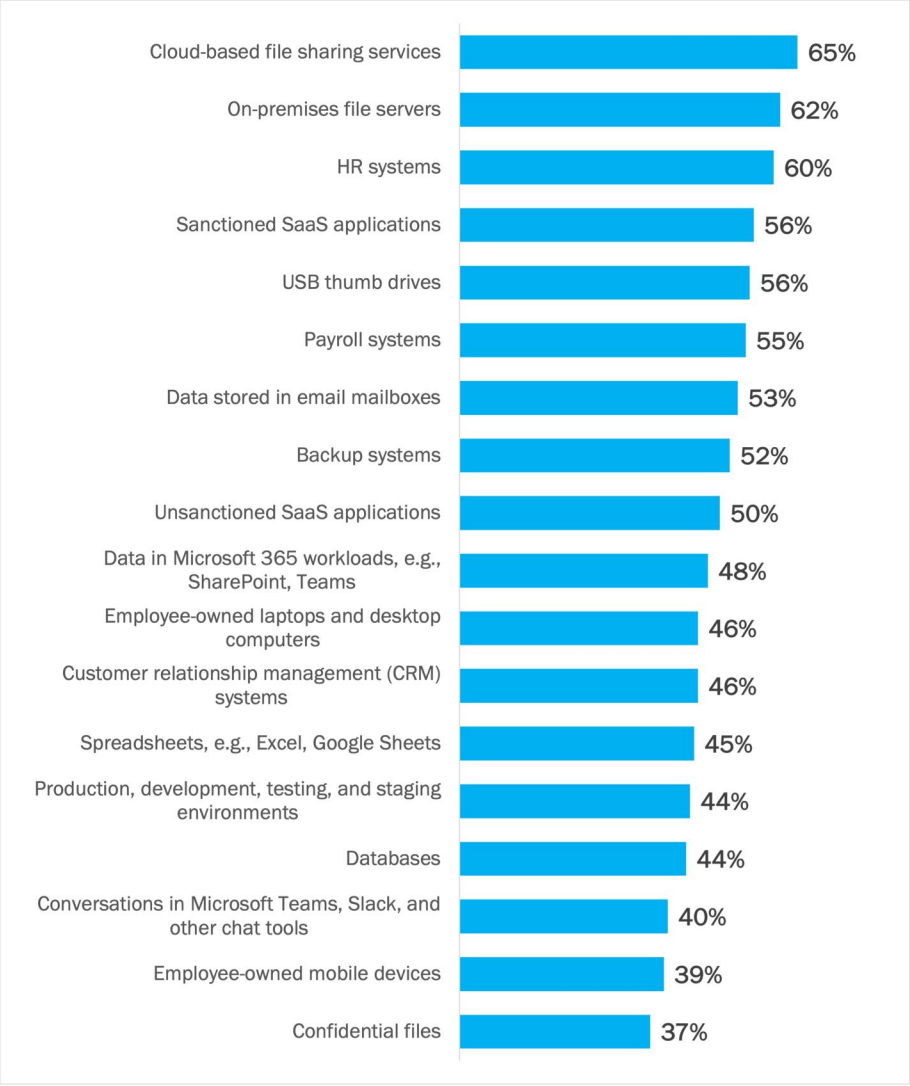


Source: Osterman Research (2023)

IMPROVE EFFICACY AT DISCOVERING DATA THAT REQUIRES PROTECTION

On average, only half of organizations have high efficacy at discovering personal and sensitive personal information requiring protection across all the data sources shown in Figure 15. Of note are sanctioned SaaS applications (56% of organizations indicate high efficacy), unsanctioned SaaS applications (50%), data in Microsoft 365 (48%), and conversations in cloud-based chat tools (40%). This, despite 96% of respondents indicating that 30% or more of corporate-owned data resides in these types of SaaS apps. In addition, widespread adoption of Microsoft 365, email, and spreadsheets like Excel and Google Sheets has not parlayed into appropriate data discovery and protection capabilities.

Figure 15
Effectiveness of Discovering Personal and Sensitive Data Across Data Sources
Percentage of respondents indicating "effective" or "extremely effective"



Source: Osterman Research (2023)

Only half of organizations have high efficacy at discovering personal and sensitive personal information requiring protection across data sources.

Organizations with higher maturity in how they comply with current privacy regulations (see page 7) report a 32% average higher ability to discover data across the above sources, compared to organizations with low maturity.

APPROACHES AND PROTECTIONS FOR PRIVACY COMPLIANCE

Achieving, maintaining, and extending privacy compliance for all types of regulated data relies on a plethora of approaches and protections working in concert. Respondents indicate that some approaches and protections have been addressed properly, while others are lagging. Many of the approaches cluster into related groupings.

In reviewing the approaches in Figure 16 on the next page, we observe the following:

- **Data maps and classification are highly rated this year**
  The top three approaches for privacy compliance are all related to data mapping and classification, including the top-rated approach of monthly or quarterly production of a data map (with 66% of respondents indicating this is going "well" or "extremely well"), policy-based data classification (63%), and real-time or near real-time data mapping (63%). These approaches and protections have increased from the 2022 survey from 34%, 45%, and 33% respectively. If this is reflective of wider trends across organizations, the elevation of these approaches is good to see.

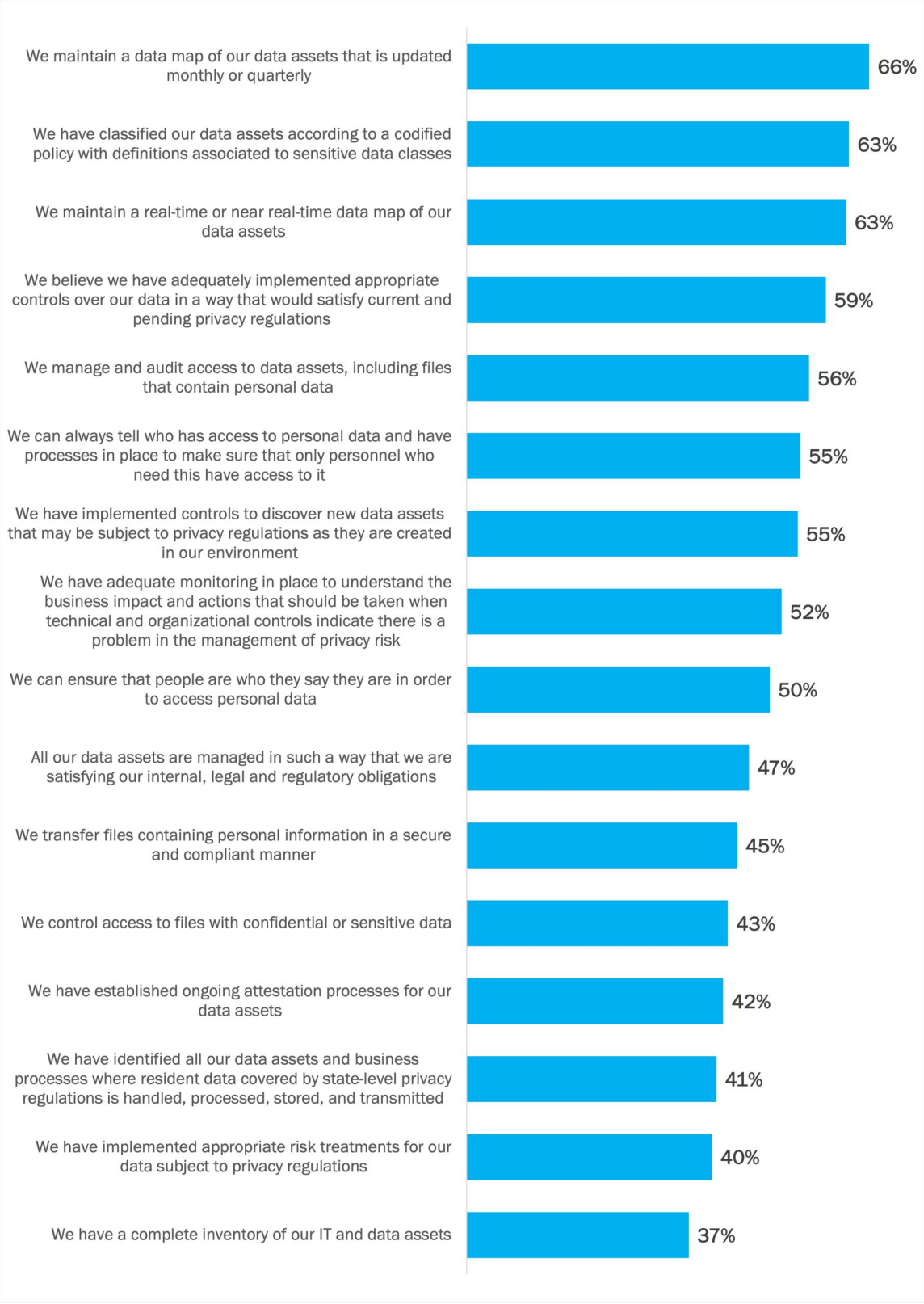
- **Usage of access controls, secure file transfer, and identity verification has regressed year on year**
  Controlling access to files containing confidential or sensitive data was the top-rated approach in 2022 (66%), followed by secure file transfer and the ability to verify the identity of an individual before providing access to personal data (63% each). In 2023, these approaches have declined significantly to 43% for access control (12th place), 45% for secure file transfer (11th place), and 50% for identify verification (9th place). Each of these approaches is essential to protecting data from unauthorized access, and hence the decline at organizations in how well these processes are enacted is extremely concerning.

- **Support for geo-segmenting of data has declined slightly**
  New and emerging state-level data privacy regulations demand elevated data protections and extend privacy rights for residents in specific geographies only. In 2022, only 45% of organizations had identified their data assets and business processes that handle, process, store, and transmit data covered by these regulations. In 2023, this declined slightly to 41% of organizations. This change aligns with the finding in this research that more organizations have decided to extend privacy rights to all United States residents regardless of geography (hence making geo-segmentation less important). However, whether the decline is due to this strategic direction or merely reflective of normal inter-survey variation remains to be seen.

- **Data discovery and classification approaches must be complemented with approaches for protecting data**
  The top-rated approaches in Figure 16 focus on data discovery and data classification. These are fundamental disciplines for protecting data that we encourage every organization to get right, but they must be complemented by approaches that enact appropriate organizational and technical protections on the discovered and classified data. Access control, secure file transfer, identity verification, monitoring, and implementing appropriate risk treatments (including data minimization, defensible deletion, and retention for legal hold) are the other side of the coin. While discovery and classification are fundamental, organizations cannot leave it at that.

While data discovery and classification are fundamental disciplines, they must be complemented with approaches for protecting data.

Figure 16
Approaches to Handling Privacy Regulations
Percentage of respondents indicating issues have been addressed "well" or "extremely well"



Source: Osterman Research (2023)

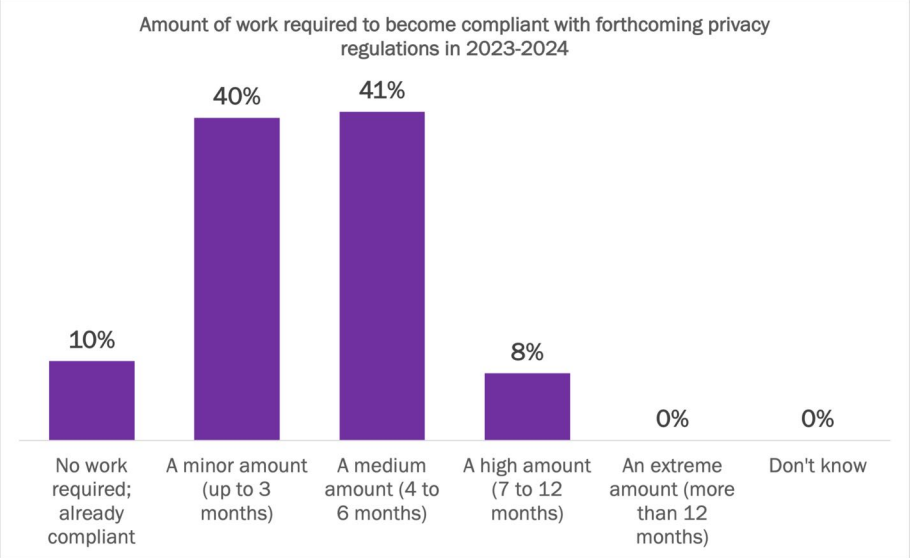
Getting Ready for the Next Wave

New and emerging state-level privacy regulations impose data protection requirements on organizations in the United States and beyond. Organizations impacted by these new regulations must take steps to ensure their organizational and technical approaches are ready, tested, and verified. In this section, we outline a game plan.

BUDGET FOR THE TIME AND EFFORT REQUIRED

Becoming compliant with new state-level privacy regulations is not an automatic, flip-the-switch type of process for any organization. Work is required to prepare the organizational context (e.g., decision-maker support), train employees on their duties and responsibilities, deploy appropriate technical solutions, and more. One in ten organizations say they have already completed the required work, but for the bulk of organizations, up to six months of work remains outstanding. See Figure 17.

Figure 17
Work Required to Comply with Forthcoming Privacy Regulations
Percentage of organizations



Source: Osterman Research (2023)

Work is required to prepare the organizational context for emerging state-level privacy regulations.

In comparison to the survey findings from 2022, half as many respondents said it will require a "high amount of work" (8% in 2023 vs. 16% in 2022), and no respondents said the amount of work would be extreme (vs. 3% in 2022) or was still unquantified (vs. 8% in 2022).

ACTION POINT

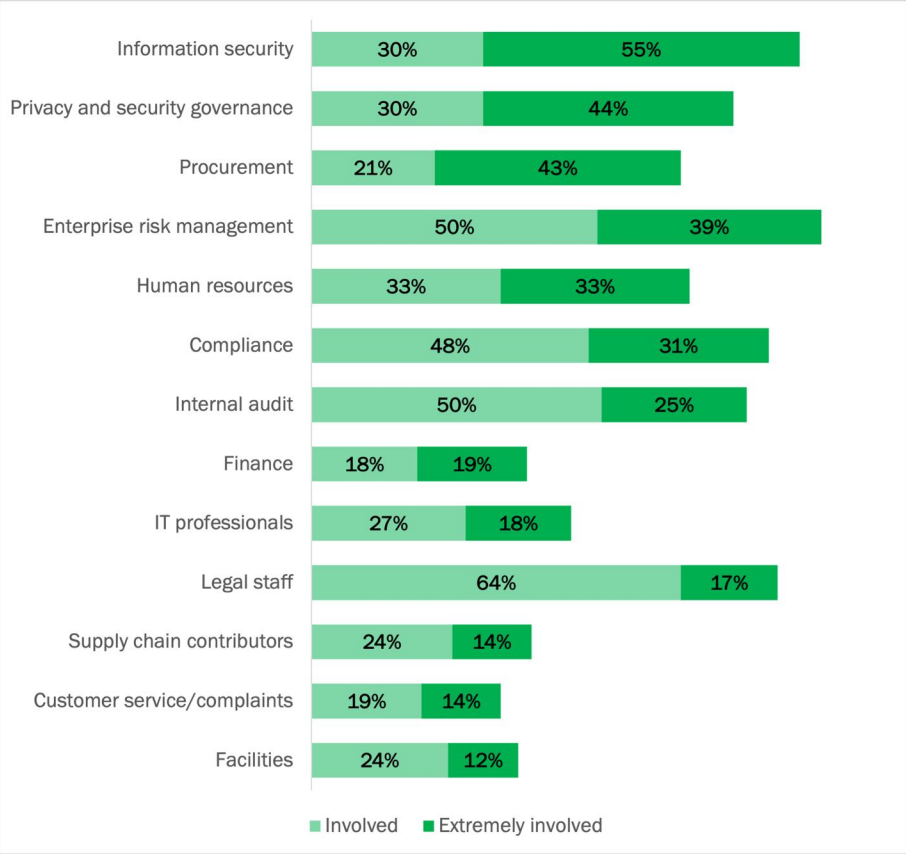
Assess your compliance readiness with new and emerging state-level privacy regulations and ensure the people, time, and budget are allocated for getting to where your organization needs to be.

BROADEN PARTICIPATION IN ACHIEVING COMPLIANCE

Many different groups in an organization are affected by new and emerging state-level privacy regulations. These different groups have input to offer in achieving and maintaining compliance, even those that have historically not been associated with privacy, e.g., procurement staff who need to factor privacy considerations into third-party agreements and cloud services contracts.

In this research, information security (55%), privacy and security governance (44%), and procurement (43%) are the three groups with the highest representation for ensuring privacy compliance. The high involvement of these groups indicates greater privacy maturity as organizations move into implementing a privacy program (rather than just working out what privacy means). Other groups have much higher involvement at a lower level, such as legal staff (64% at the "involved" level), enterprise risk management (50%), and internal audit (50%). On average, organizations have 4.4 groups participating at the "extremely involved" level and 3.6 groups at the "involved" level. See Figure 18.

Figure 18
Groups Involved in Ensuring Compliance with Privacy Regulations
Percentage of respondents indicating "involved" or "extremely involved"



Source: Osterman Research (2023)

Many groups in an organization are affected by new and emerging state-level privacy regulations and have input to offer in achieving and maintaining compliance.

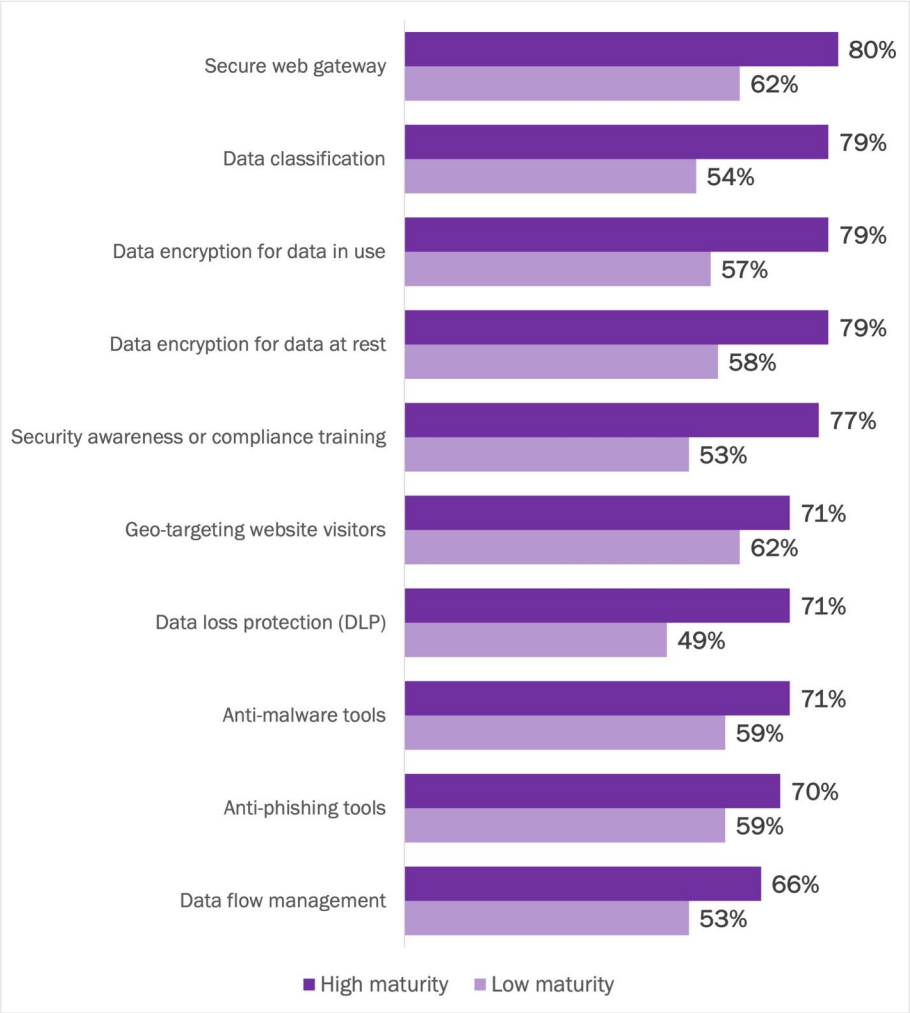
ACTION POINT

Decide who at your organization should be involved in complying with new and emerging state-level privacy regulations, and to what degree each group should be involved. Not every group must be "extremely involved" in the journey to compliance, but few groups should be totally excluded. What does your organization need?

DEPLOY NEW SOLUTIONS TO IMPROVE COMPLIANCE POSTURE

Organizations with higher maturity in meeting the compliance requirements of currently enforced privacy regulations attribute higher importance to a range of solutions than organizations with lower maturity in meeting currently enforced requirements (see page 7). Five solutions are very closely ranked as highly important among the high-maturity cohort of organizations: a secure web gateway, data classification, data encryption for data in use, data encryption for data at rest, and security awareness or compliance training. See Figure 19.

Figure 19
Importance of Solutions for Privacy Compliance: High Maturity vs. Low Maturity
Percentage of respondents indicating solutions are "important" or "extremely important"



Source: Osterman Research (2023)

High-maturity organizations place greater importance on a range of solutions for privacy compliance.

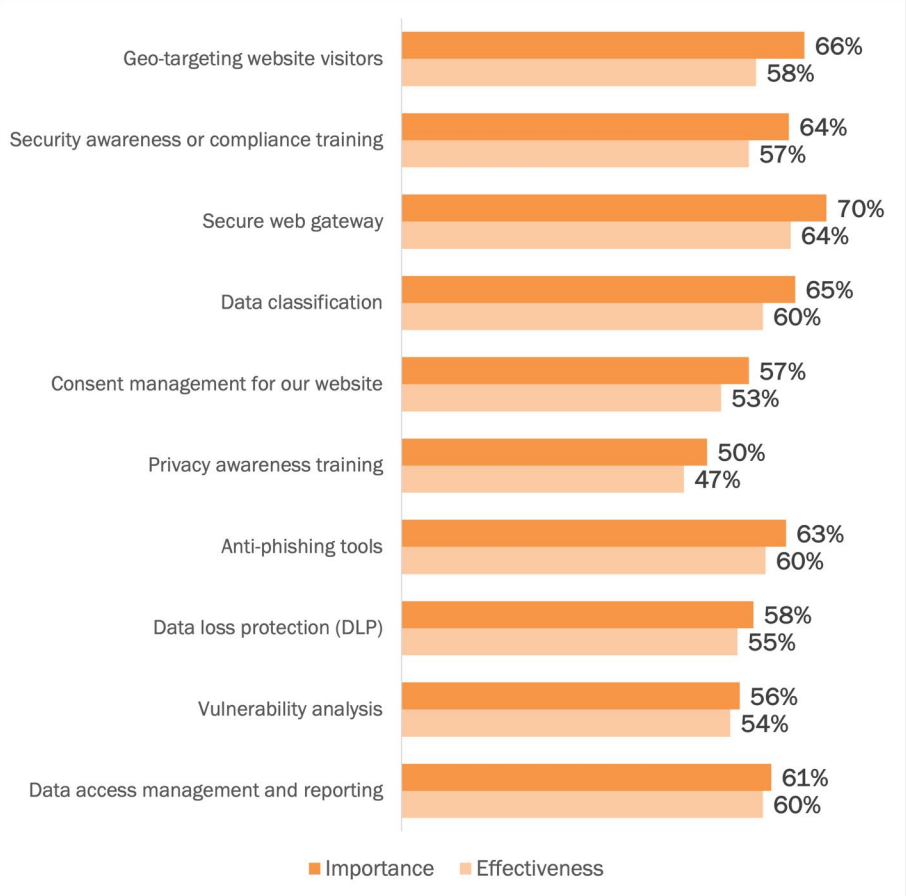
ACTION POINT

Review the technical protections your organization uses to drive compliance with privacy regulations. Where are the most significant gaps in your approach compared to high-maturity organizations? Are there opportunities for platform approaches that address multiple use cases to replace disparate point solutions?

RESOLVE GAPS IN EFFECTIVENESS IN ESSENTIAL SOLUTIONS

Various solutions that organizations have deployed for achieving privacy compliance are underperforming compared with the level of importance they play in enabling an organization to be compliant with privacy regulations. Respondents in this research indicate the most significant gaps are in the solutions they are currently using for geo-targeting website visitors, security awareness or compliance training, and a secure web gateway. For instance, geo-targeting website visitors is essential to organizations that extend differential data rights to visitors based on the state in which they reside. When currently deployed solutions cannot automate the detection with a high degree of accuracy, extending differential data rights is built on a shaky foundation and a more advanced solution should be investigated. See Figure 20.

Figure 20
Importance and Effectiveness of Solutions for Privacy Compliance
Percentage of respondents indicating solutions are "important" or "extremely important" versus percentage of respondents indicating currently deployed solutions are "effective" or "extremely effective"



Source: Osterman Research (2023)

Organizations must revisit their choice of technical solutions when efficacy trails importance.

ACTION POINT

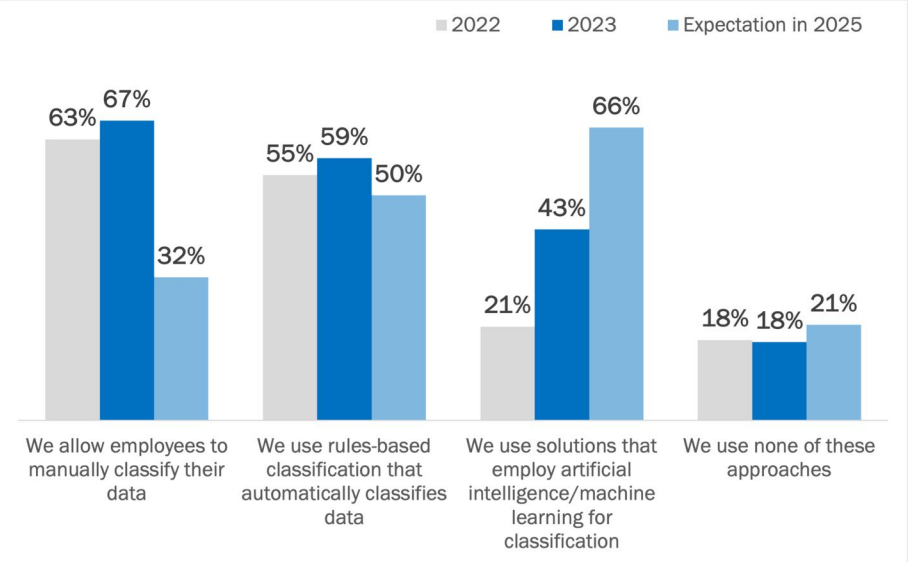
Review the effectiveness of your currently deployed solutions for meeting the privacy requirements your organization has. New and emerging regulations may require the deployment of next-generation technologies and solutions to achieve privacy compliance.

IMPROVE METHODS OF CLASSIFYING DATA

The need for classifying data has already been discussed in this white paper, and organizations appear to be putting increased emphasis on this process. This is a good development and an essential direction. There are, however, different methods for classifying data, including employee-driven manual classification and classification based on artificial intelligence and machine learning (AI/ML) models.

In this research, organizations expect to use less manual and rules-based classification in two years compared to today, and significantly more AI/ML. Once we layer on the current state of data from the 2022 survey, the usage baseline has not changed dramatically year on year for employee and rules-based classification. By comparison, usage has doubled for AI/ML from 2022 to 2023 and is expected to increase by another 50% over the next two years. Clearly, organizations are putting increased focus on the opportunities presented by AI/ML. The continued movement toward automated data classification and away from earlier generations of manual and rules-based classification is good to see. Automated approaches also benefit subsequent data processes such as risk scoring and usage analysis. See Figure 21.

Figure 21
Approaches for Classifying Data
Percentage of organizations using each approach



Source: Osterman Research (2023)

As methods of classifying data evolve, retraining employees and assessing legacy technology must not be overlooked.

The lingering contribution of employee and rules-based classification highlights the need for taking specific action to reduce usage of earlier approaches. Deploying new technology such as AI/ML is but one step. Retraining employees and removing legacy technology are essential second and third steps.

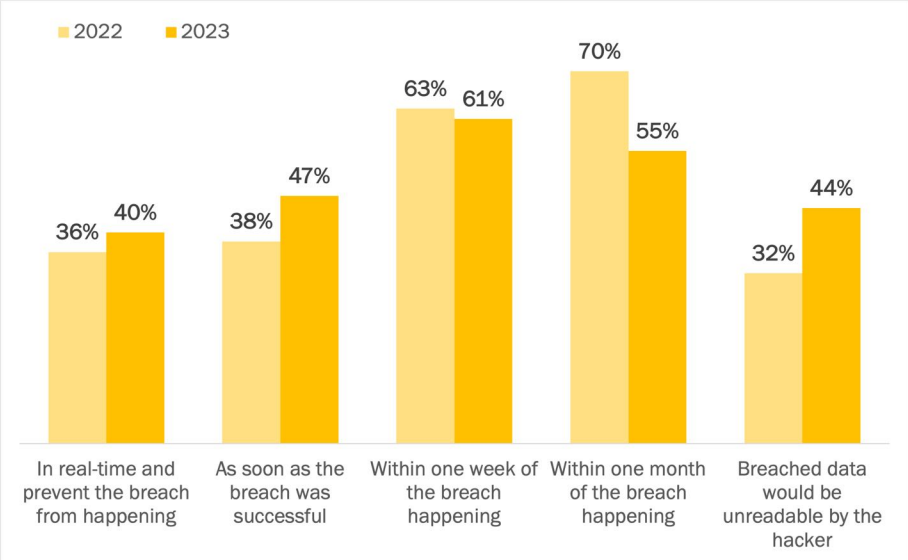
ACTION POINT

Assess the usage of different classification approaches across your organization. If new AI/ML solutions are being deployed to improve classification efficacy, address technical debt by reducing reliance on previous approaches. Retrain employees on the new approaches and what these require of them.

STRENGTHEN PROTECTIONS AGAINST DATA BREACHES

The ability to detect a breach in real time and prevent it from happening is the ideal standard for organizations. In this research, 40% of respondents are confident that their organization can achieve this standard, which is up from 36% in the 2022 survey. If real-time detection and interruption of an in-progress data breach is not possible, the second-best option is that breached data is unreadable by a hacker, which has also increased over the past year (from 32% to 44%). Preventing readable data from being breached is the domain of strong encryption technologies. See Figure 22.

Figure 22
Confidence to Detect a Breach of Data Covered by Privacy Regulations
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2023)

The three middle options are all problematic, although the timeframe for breach detection is significantly different between them. Shorter detection timeframes indicate a higher level of process maturity inside the organization and signal data protection competence (albeit not perfection) to regulators and other groups charged with oversight. Irrespective of the detection timeframe, the options remain problematic because a successful data breach still occurs. This often necessitates full incident response, including notifying regulators and affected customers. Strengthening real-time detection capabilities with technology and employee preparedness through security awareness training increases the likelihood that a data breach attempt can be stopped in flight.

If real-time detection and interruption of an in-progress data breach is not possible, the second-best option is that breached data is unreadable by a hacker.

ACTION POINT

Assess your organization's ability to detect a data breach attempt in real time and interrupt it before data is successfully breached. Deploy new technology and employee training to increase the efficacy of breach detection, along with strong data encryption to mitigate breach attempts that are successful.

PROTECT DATA WITH DATA MASKING

Protecting data through encryption, tokenization, and pseudonymization obfuscates the underlying data, rendering it unusable when breached and reducing unnecessary disclosures to employees while they are accessing corporate systems. The three approaches are different but complementary:

- **Encryption**
  Uses a mathematical algorithm to transform cleartext into ciphered data. Relies on cryptography. Strong encryption keys make it almost impossible for breached data to be decrypted computationally (although advances in quantum computing may change that over the long term).
- **Tokenization**
  Moves cleartext out of one system into another system, replacing the original value with a randomly generated lookup or mapping value. The token is used to find the original value for authorized users.
- **Pseudonymization**
  The process of transforming cleartext into a substitute value. Unlike tokenization, pseudonymization does not require a separate system to hold the original value.

In this research, 95% of organizations are using various forms of data masking to protect data across its lifecycle, with protections for data at rest the most common (at 97% of organizations). In comparison to the 2022 survey, usage of data masking across the three stages has increased from an average of 80%, with the most significant difference being the increased adoption of data masking for data in use (at 71% in 2022 versus 93% currently). This elevation of protections for personal data when employees are accessing corporate systems is very positive—and even more so when data-in-use tools allow secure analysis without decrypting the data. See Figure 23.

Protecting data in use has historically lagged protections enacted for data in transit and data at rest.

Figure 23
Use of Data Masking During the Data Lifecycle
Percentage of organizations

Source: Osterman Research (2023)

ACTION POINT

Revisit how data in your organization is protected in transit, at rest, and in use. Address weaknesses through improved technical solutions and organizational processes. Pay particular attention to how data in use is protected, as it has historically lagged protections enacted for data in transit and data at rest.

UPLEVEL DELIVERY OF DATA SUBJECT RIGHTS

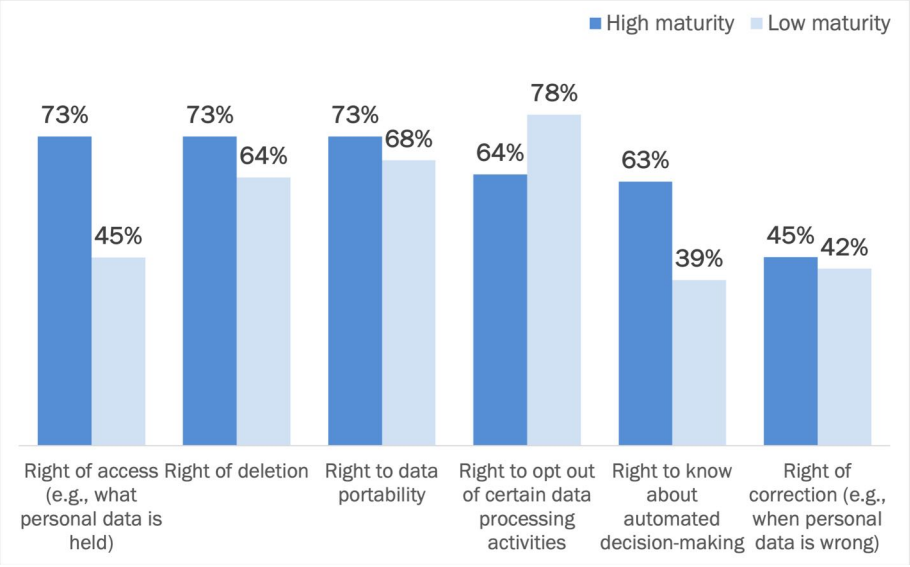
Data privacy regulations assign a set of rights to data subjects—the people whose data is held and processed by organizations. The right of access is the most assigned right, but other rights are widely conferred, too. Organizations must be able to uniquely identify the individual requesting the exercise of a right and have the technical and organizational processes in place to meet the requirements of each right. Unique identification and strengthened verification mechanisms to identify fraudulent requests or requests from compromised accounts are essential, otherwise organizations will unwittingly expose personal data to a threat actor impersonating a customer.

In this research, organizations with higher maturity in meeting the compliance requirements of currently enforced privacy regulations (see discussion on page 7) have higher capability to deliver five of the six data subject rights in Figure 24. Right of access, deletion, and data portability lead for this cohort of organizations.

Among organizations with lower maturity in meeting the compliance requirements of currently enforced privacy regulations, the highest-ranked right is to opt out of certain data processing activities (78%). The nature of this right indicates a preference among this cohort of organizations for a broad-stroke opt-out rather than the delivery of nuanced data rights, such as access, deletion, and data portability. The thinking appears to be that if data subjects opt out, less data is captured, held, and processed. While there is a small degree of truth to this approach, it offers a very shaky foundation for privacy. See Figure 24.

Organizations must be able to uniquely identify the individual requesting the exercise of a right and have the technical and organizational processes in place to meet the requirements of each right.

Figure 24
Ability to Deliver Data Subject Rights: High Maturity vs. Low Maturity
Percentage of respondents indicating "effective" or "extremely effective"



Source: Osterman Research (2023)

ACTION POINT

Check the data rights that must be extended under new and emerging privacy regulations. Ensure appropriate technical and organizational processes are in place to enable the efficient delivery of these rights, including heightened identification and verification processes for data subjects (e.g., customers, employees). Data rights apply to data across the entire data inventory, e.g., applications, data warehouses, backups, archives, etc.

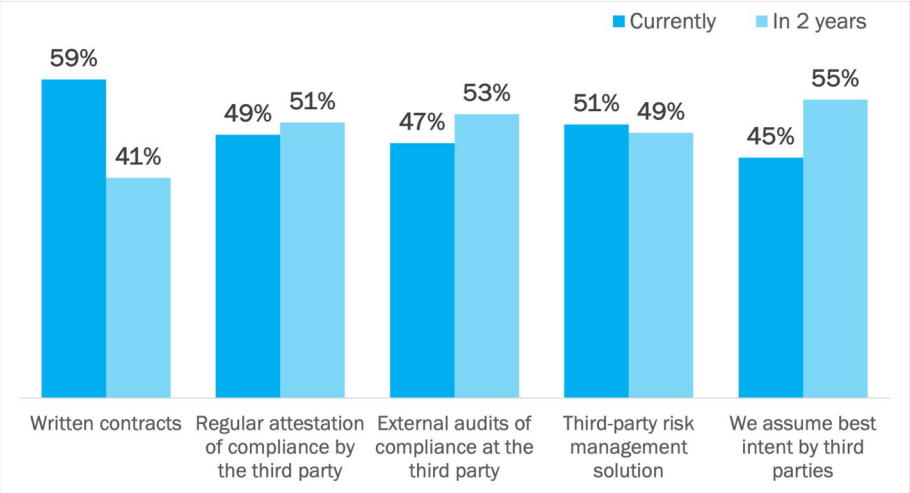
STRENGTHEN PROTECTIONS WHEN WORKING WITH THIRD PARTIES

Organizations commonly share the personal and sensitive personal data they have collected and control about customers with third-party organizations. These third-party organizations analyze the data, check its accuracy, and use it in the processes they have been engaged to perform. Making this data available to third-party organizations raises the risk of unauthorized processing, data breach, and data exposure for the primary organization, since their own organizational and technical protections do not travel with the data. How organizations manage their risk exposure for their data when it is under third-party control is beginning to change. See Figure 25.

Fewer organizations expect to rely on written contracts—which will decrease from 59% currently to 41% in two years. Perplexingly, more organizations indicate they will assume best intent by third parties; this is a high-risk strategy if it is done in isolation from the other approaches below. For the three middle approaches to managing data risk, only slight movement is expected. Slightly more expect to use regular attestation of compliance and external audits of compliance, and slightly fewer expect to use a third-party risk management solution. Decisions about how to best handle third-party risk appear uncertain for the organizations in this research.

Personal and sensitive data shared with third parties exposes the organization to the risk of unauthorized processing, data breach, and data exposure.

Figure 25
Managing Third-Party Data Risk
Percentage of organizations



Source: Osterman Research (2023)

At Osterman Research, we believe the right direction for organizations is composed of external audits of compliance at the third-party level and/or a third-party risk management solution, along with regular attestation of compliance by the third party. The first two increase the likelihood that actual testing of the third party's data processes is carried out, something which is often missing in written contracts, attestation, and assuming best intent.

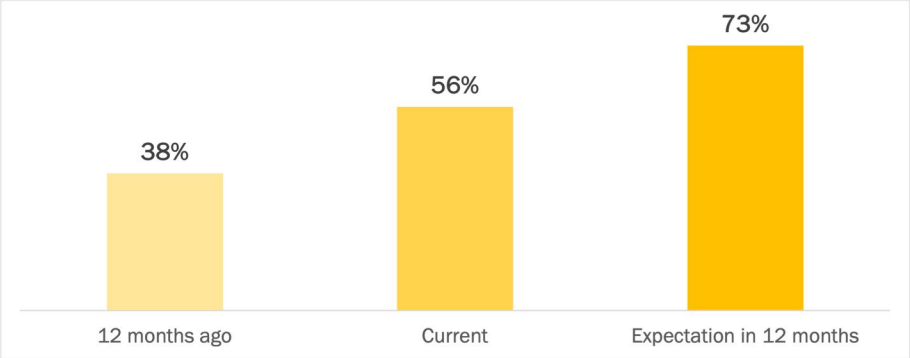
ACTION POINT

Reexamine the risk exposure to your organization due to data shared with third-party organizations. Investigate how to strengthen controls over data that your organization is responsible for, even when it is not under your control.

USE AUTOMATION TO STREAMLINE COMPLIANCE MONITORING

Organizations are rapidly increasing their use of automated processes for monitoring compliance of SaaS apps with privacy regulations. Automated processes are used for validating controls and settings (including alerting or automatically correcting unintentional drift) and correlating alerts to reduce noise. More than half of activities are currently performed using automated processes, and this is expected to increase to almost three quarters in 12 months. Assuming the current three-year rate of growth continues, all monitoring activities will be performed using automated processes within two years. See Figure 26.

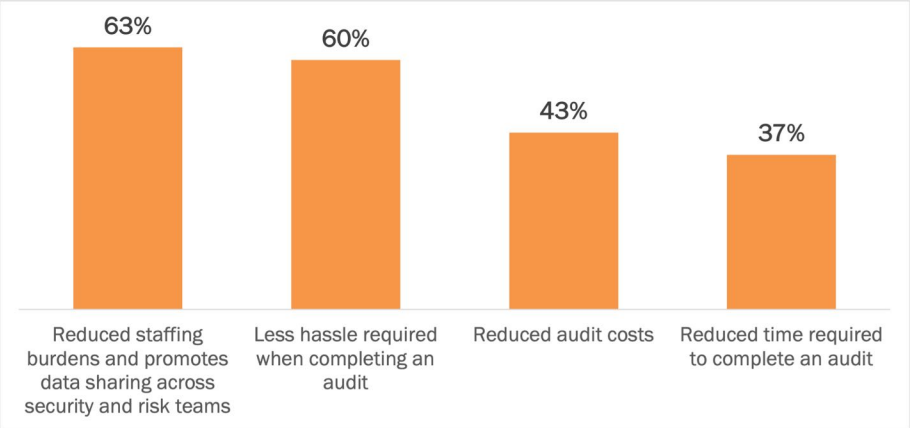
Figure 26
Monitoring SaaS Compliance with Automated Processes
Percentage of activities completed using automated processes



Source: Osterman Research (2023)

Respondents indicate that the primary benefit of using automated processes is a reduced staffing burden and the promotion of better data sharing across security and risk teams. See Figure 27.

Figure 27
Benefits of Using Automated Processes for Monitoring SaaS Compliance
Percentage of respondents indicating "agree" or "strongly agree"



Source: Osterman Research (2023)

Assuming the current three-year rate of growth continues, all SaaS compliance monitoring will be performed using automated processes within two years.

ACTION POINT

Check how compliance with privacy regulations in SaaS apps is being managed at your organization. Increase the use of automation to validate settings, correlate alerts, and reduce the burden on staff when manual processes are required.

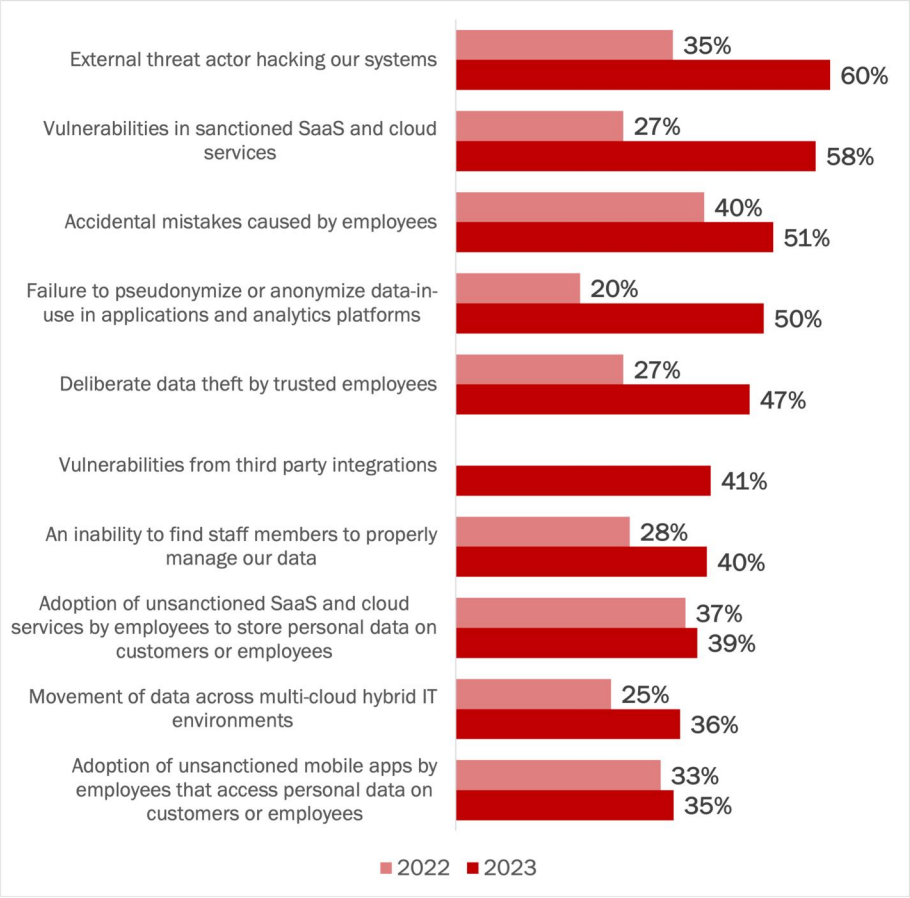
Address the Employee Threat

Employees (along with managers and executives) represent a special type of threat to organizations because they have authorized access to the systems that contain personal and sensitive personal data covered by privacy regulations.

UNDERSTAND THE TYPES OF RISKS POSED BY EMPLOYEES

There are several types of employee threats to watch out for. The highest-rated employee issues that threaten compliance with privacy regulations are accidental mistakes caused by employees (51%), deliberate data theft by trusted employees (47%), inability to find staff members to properly manage data (40%), and adoption of unsanctioned SaaS and cloud services by employees to store personal data on customers or employees (39%). See Figure 28.

Figure 28
Issues That Threaten Compliance with Privacy Regulations
Percentage of respondents indicating "threat" or "extreme threat"



Source: Osterman Research (2023)

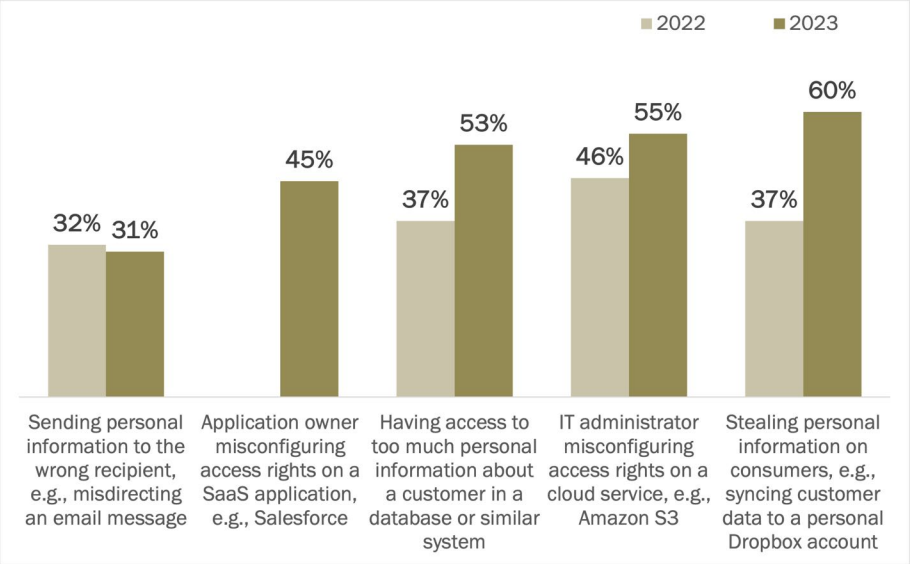
External threat actors, vulnerable SaaS apps, and employees threaten compliance with privacy regulations.

In comparison to the 2022 survey, the level of threat posed by each of these issues has increased across the board. This has also elevated two issues that were in second and fourth place last year to first and second place in this year's research: an external threat actor hacking systems (almost doubled in threat level and moved into first place this year) and vulnerabilities in sanctioned SaaS and cloud services (more than doubled and moved into second place this year). Vulnerabilities from third-party integrations was not asked in 2022.

ADDRESS LOW CONFIDENCE IN TECHNICAL AND ORGANIZATIONAL PROTECTIONS TO PREVENT DATA BREACHES

Organizations face data breach possibilities from multiple vectors involving employees, such as employees sending personal information to the wrong recipient, misconfiguring access rights on a SaaS application, and having access to too much personal information about a customer in a database. In this year's research, only half of respondents on average indicate confidence in their current technical and organizational protections to prevent data breaches. Confidence levels in misdirected email messages remain stubbornly low (31%), while confidence levels in three of the other breach vectors have improved year on year—from 40% on average in 2022 to 56% on average this year. See Figure 29.

Figure 29
Confidence in Protections to Stop Data Breaches by Employees
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2023)

We asked about confidence in application owners configuring access rights on a SaaS application correctly for the first time this year—versus an IT administrator doing the same. As shown in Figure 29, only 45% of respondents believe that application owners will configure access rights correctly; this is the second-lowest level of confidence across the five breach vectors. Strengthening protections for access rights is a key area to focus on at any organization where business unit managers and group leaders make their own decisions on SaaS applications outside the purview of the IT and security teams.

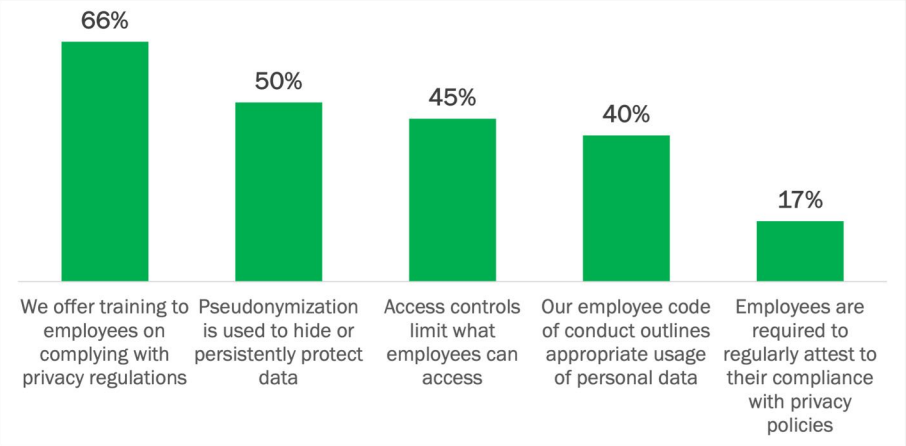
Unless some form of data masking is used in databases and other systems containing customer information, every time employees look at a customer record for a valid business reason, they may be given access to more data than is needed to meet the requirements of the specific task. Confidence levels in current protections have increased 43% year on year, and while this is trending in the right direction, only just above half of organizations have confidence in their current protections.

Strengthening protections for access rights is a key area to focus on at any organization where business unit managers and group leaders make their own decisions on SaaS applications outside the purview of the IT and security teams.

MITIGATE EMPLOYEE THREATS WITH BETTER ORGANIZATIONAL AND TECHNICAL SOLUTIONS

Organizations make use of several organizational and technical mitigations to reduce the risk of data breaches by employees. Most organizations rely on up to three methods, with employee training the most popular (at 66% of organizations). See Figure 30.

Figure 30
Organizational and Technical Mitigations to Minimize Data Risk by Employees
Percentage of organizations



Source: Osterman Research (2023)

The mitigations above can be divided into two groups:

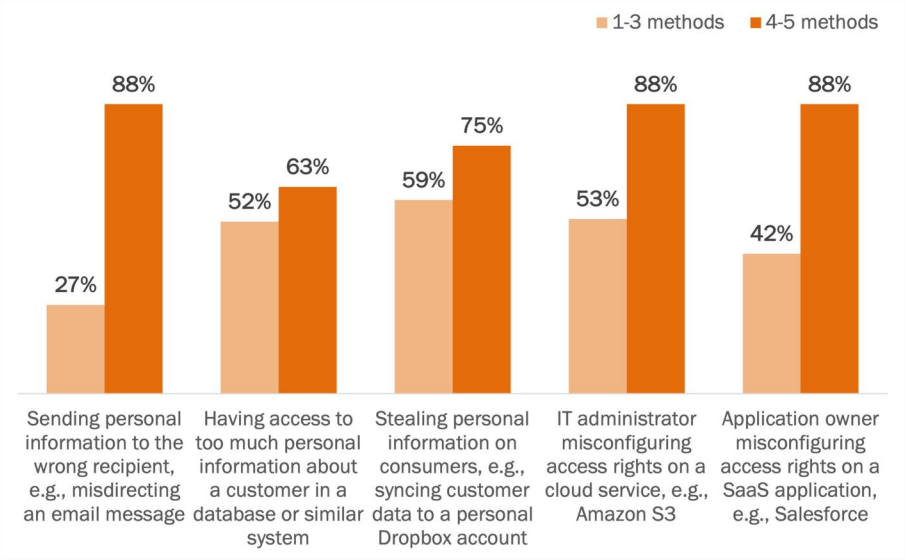
- **Setting the organizational context on privacy regulations: employee training, code of conduct, and periodic attestation**
  Employee training and an employee code of conduct set expectations on what employees should do with data covered by privacy regulations. Attestation requirements periodically remind employees of these responsibilities and create an audit trail of asserted compliance. However, none of these mitigations enforce protections over the data that employees can access.
- **Reducing the scope of access to data: access controls and pseudonymization**
  Access controls systematically reduce the scope of data that is accessible by employees. These must be rigorously maintained to achieve this outcome, otherwise too much data will be presented to authorized users and data will be exposed to unauthorized ones. In addition, correct access controls without strong identity management will succumb to cyberattacks that leverage phishing, credential stuffing, or social engineering to gain account credentials from employees.

  Pseudonymization and other approaches that de-identify data with encryption and tokenization also systematically reduce the scope of access to data, albeit in a different way from access controls. Pseudonymization hides or persistently protects personal and sensitive personal information from employees unless it is explicitly required by the task at hand. Some solutions offer persistent protection even for data in use. Whether pseudonymization can foil phishing, credential stuffing, and social engineering cyberattacks depends on how pseudonymization is configured to mask data and how the process has been designed for approving special requests to access personal data.

Employee training, a code of conduct, and regular attestation of compliance don't enforce protections over data employees can access.

Organizations using four or all five of the methods in Figure 30 report higher confidence in their organizational and technical protections to stop various types of data breaches caused by employees. See Figure 31.

Figure 31
Confidence in Protections to Stop Data Breaches by Employees
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2023)

Conclusion

The regulators' intent in introducing new privacy regulations is to force organizations to enact better protections over the personal and sensitive data they hold on individuals. As explored in this white paper, some progress has been made toward this goal over the past 12 months, yet much remains unaddressed. This white paper profiles the essential organizational innovations and technical solutions required to enable organizations to meet the changing regulatory environment for data privacy.

Organizations more highly invested in protecting data are more confident in their ability to stop data breaches by employees.

Sponsored by OpenText Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention to detection and response, to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience, and simplified security to help manage business risk.

Visit opentext.com.

opentext™ | Cybersecurity

www.opentext.com

@OpenText

+1 800 499 6544

Methodology

This white paper is based on findings from a survey conducted by Osterman Research. One hundred thirty-one (131) respondents who play a role in developing, approving, enforcing, or reviewing their organization's policies and practices for complying with privacy regulations were surveyed during March and April 2023. To qualify, respondents had to work at organizations with at least 100 employees. The surveys were conducted in the United States and Canada. The survey was cross-industry, and no industries were excluded or restricted.

GEOGRAPHY

United States	80.9%
Canada	19.1%

INDUSTRY

Computer Hardware, Computer Software	10.7%
Healthcare	9.9%
Professional Services (Law, Consulting, etc.)	9.9%
Transport, Logistics	9.9%
Hospitality, Food, Leisure Travel	9.2%
Retail, eCommerce	9.2%
Financial Services	8.4%
Industrials (Manufacturing, Construction, etc.)	6.9%
Energy, Utilities	6.1%
Life Sciences	6.1%
Data Infrastructure, Telecom	5.3%
Education	4.6%
Media, Creative Industries	2.3%
Agriculture, Forestry, Mining	0.8%
Public Service, Social Service	0.8%

[1] Osterman Research, *CISO and CIO Investment Priorities for Cybersecurity in 2023*, February 2023, at https://ostermanresearch.com/2023/02/15/orwp_0356/