Data Protection & Privacy Officer Priorities 2020

Data protection and privacy goes mainstream in the new decade

CPO
MAGAZINE

Survey Highlights

27% named getting budget and available resources as the organization’s No. 1 challenge

49% have made governance of data processing and the formation of a privacy-aware culture a top priority

20% are making new privacy technology implementation a priority only after privacy programs have matured

57% of organizations have an annual budget of no more than $250,000 for data protection and privacy

76% of organizations have fewer than 10 employees in roles focused on data protection and privacy

Data protection and privacy goes mainstream in the new decade

Over the last year, we have seen intense debate over the collection, use and handling of personal data, which has inevitably led to tighter global restrictions.

These debates and regulations have also given consumers a greater awareness of the value of their personal data. As consumers around the world make gains in terms of interactions with private enterprises, they are tending to lose privacy ground to governments as the use of facial recognition technology and mass surveillance increases.

And, of course, the cyber threats are still out there.

High-profile data breaches and leaks

2019 saw over 7,000 data breaches, up from about 6,500 in 2018. Over 15.1 billion records were exposed, making it an extremely active year in spite of fines being larger and more frequent than ever.

Rise of the mega fines in 2019

The U.S. Federal Trade Commission (FTC) slapped Facebook with a $5 billion fine, and penalized Equifax $575 million in the year's two largest actions.

Under the General Data Protection Regulation (GDPR), there were over 200 fines for a cumulative $165 million. Google was hit with the largest penalty of $57 million.

And even more regulatory legislation is forthcoming.

The onslaught of data privacy regulations

The GDPR set in motion a slew of privacy regulations, with more on the way. California's CCPA is already in effect, and a number of countries are considering, enacting or updating national laws, including the U.S. and Brazil, Canada, Japan and South Korea.

All of this has led to an explosion of privacy vendors.

Creating a comprehensive, organization-wide data protection and privacy strategy continues to be a major challenge for DPOs and privacy specialists.

A broader range of technology options

The International Association of Privacy Professionals (IAPP) listed only 51 vendors in its early 2017 Privacy Tech Vendor Report. The most recent edition lists 259. Industry analysts expect continued growth in 2020 given all of the new regulations expected to come online.

There has been a boom market for data privacy attorneys and consultants as well, as they are often the first step in the vendor selection process.

Increased supply, but even greater demand

The IAPP's 2017 study estimated that GDPR regulatory requirements would create at least 75,000 data protection officer (DPO) positions worldwide. In May 2019, one year after the GDPR terms became active, there were estimated to be 500,000 organizations with registered DPOs in the European Economic Area (EEA) alone.

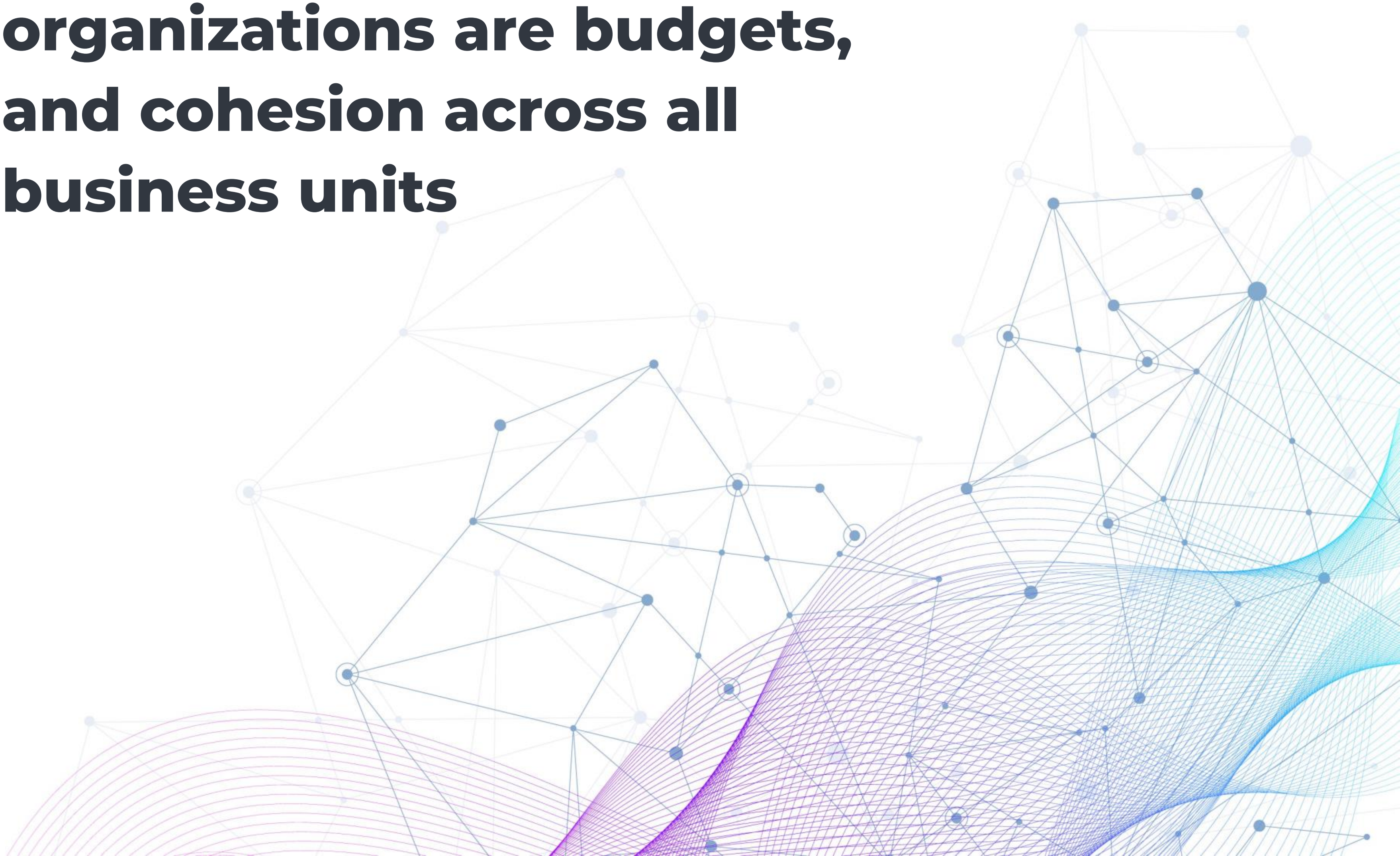
New decade brings new challenges and priorities

Compliance with data protection and privacy regulations is a challenging and complex task, which only becomes tougher as governments create and revise their national standards. DPOs and privacy professionals face not just these constantly shifting externalities, but considerable internal organizational challenges as well.

In this report, we examine the challenges faced by these data protection and privacy officers, along with their priority goals in 2020 and their expected approach of achieving them.

Key Finding 1

Top challenges for half of all organizations are budgets, and cohesion across all business units



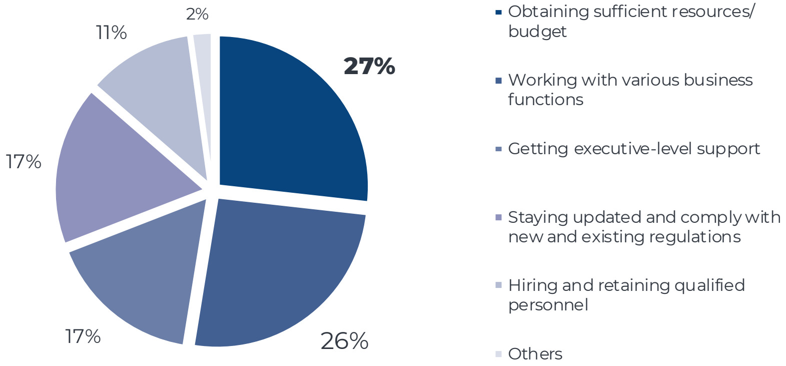
The struggle to get a comprehensive data protection and privacy program in place across the entirety of an organization is one of the main challenges for data protection and privacy officers.

The largest group of respondents (27%) say that their main challenge is budget restrictions and lack of resources.

The second most common issue is an inability to get all business units to integrate data protection and privacy measures.

Surprisingly, getting qualified manpower does not appear to be a widespread problem at present. Only 11% felt that it was a top problem, but this may be something that is masked by the budget issue (given that 57% of respondents are spending less than $250,000 throughout the organization on data protection and privacy measures).

What are the main challenges your organization faces to achieve an effective data protection and privacy program? Please select your top 3 choices.

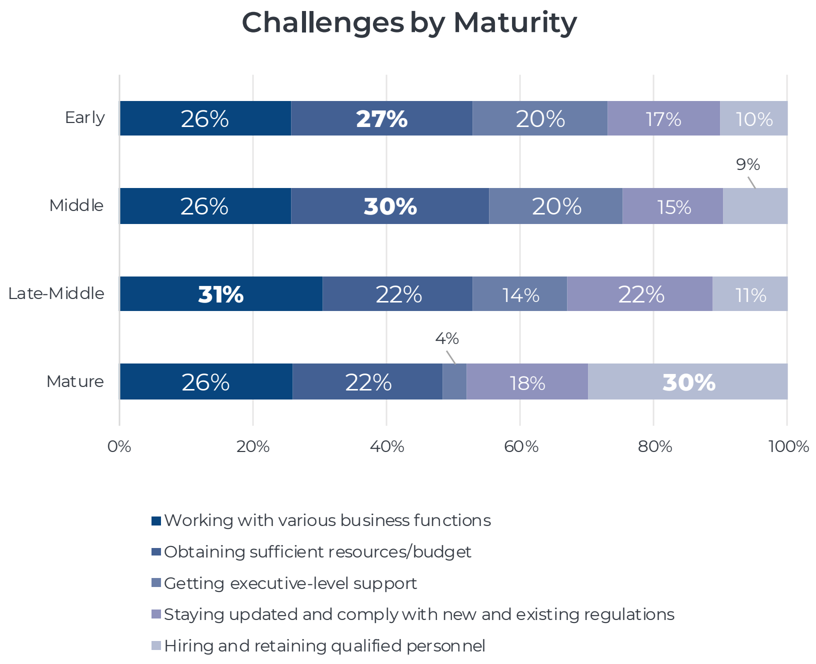


The specific challenges that data protection and privacy officers face depends on the relative maturity of the organization's program.

In the Early and Middle stages of spinning up a data protection and privacy program, the main challenge for data protection and privacy officers is a lack of budget and resources. These same organizations are also facing significant challenges in obtaining support from the executive ranks, compared to those with a higher level of program maturity.

One thing is clear, no matter the level of maturity, organizations continue to face challenges in working with various business functions.

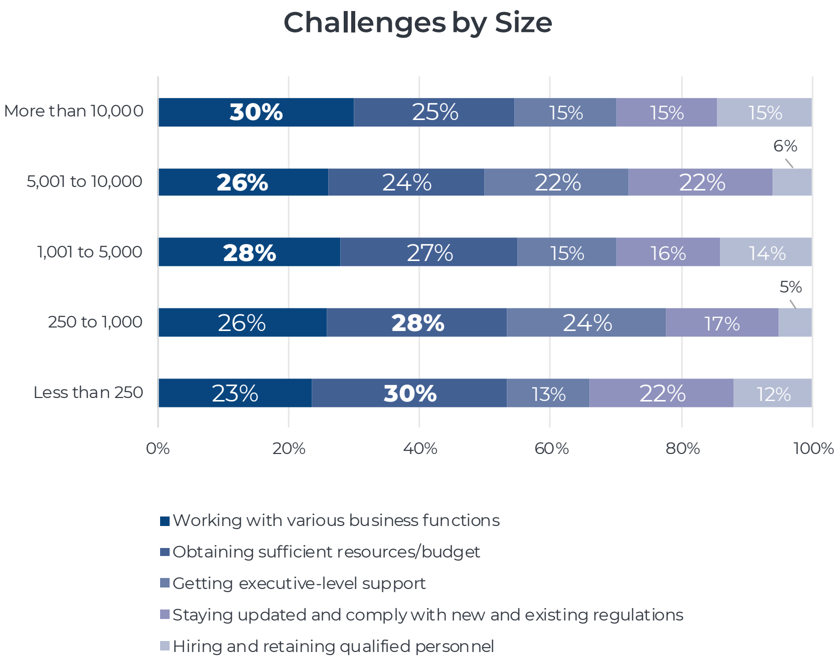
However, once programs become mature, the main challenge is in hiring and retaining qualified personnel. A possible reason for this is that 1 of 5 organizations with Mature programs are maintaining a staff strength of over 100.



Smaller organizations may be underestimating the cost of implementing and maintaining a comprehensive and effective data protection and privacy program.

Larger organizations are more likely to have problems implementing policies and measures across their various business functions (28% of those with over 1,000 employees). Large organizations with complex structures and businesses tend to require more sophisticated programs that are harder to implement and more challenging to get everyone on board.

Among smaller organizations, the problem tends to be resources and budget (29% of those with under 1,000 employees). Despite the media headlines, these organizations may be underestimating the cost of their data protection and privacy compliance needs and not allocating enough resources.



Key Finding 2

Key priorities across half of organizations are enhancing the governance of data processing activities and building a privacy-aware culture

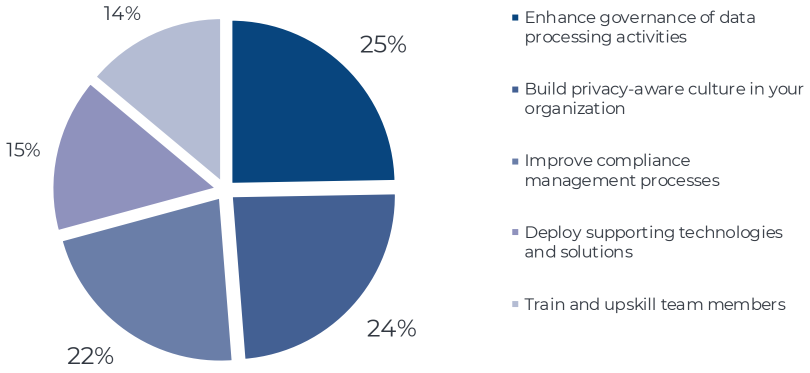
Establishing a solid foundation for governance of data processing and privacy-aware culture remain high on the agenda for data protection and privacy officers.

49% of the respondents placed building a privacy-aware culture and improving governance of data processing as top priorities for their organization. A similar response was seen in the 2019 survey, which means that though these items continue to be cornerstones of many programs some organizations may be having trouble finding lasting solutions.

There is a much lower emphasis on training, hiring and retaining personnel. This is another indication that manpower is not currently a major concern and is taking a backseat as limited budgets are divided up.

Based on their initial response to the priority question, respondents were further asked to identify the activities that will be important to them to meet their program goals.

What are your top data protection and privacy priorities for your organization in 2019? Please select your top 3 choices.

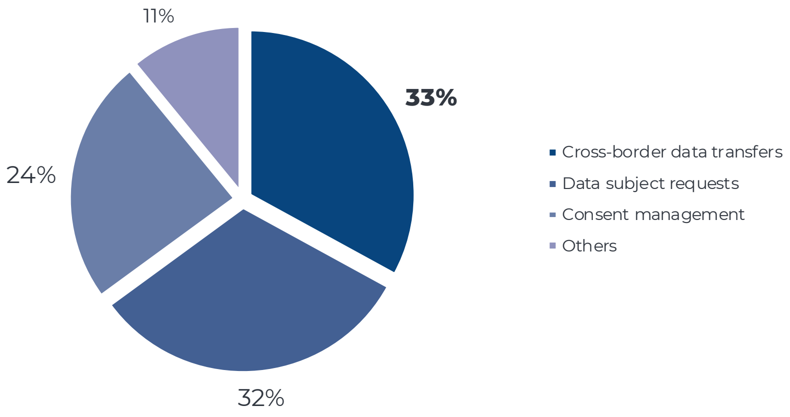


Among specific governance process improvements, better cross-border data transfers and data subject requests are top priorities for data protection and privacy officers.

Among the three specific options respondents were presented with, cross-border data transfers and data subject requests were considered the highest priorities. This trend is very likely to continue given that companies are about to have more international regulations to deal with in 2020 and more potential data subjects looking to access their personal records.

The “Others” option, which 11% of respondents selected, allowed for write-in responses. Contributions most frequently mentioned are for data governance, particularly data retention and deletion. This is hardly surprising due to the increased reliance on data as more organizations embark on digital transformation projects.

What are the focus areas for enhancing the governance of data processing activities? Please select all relevant choices.



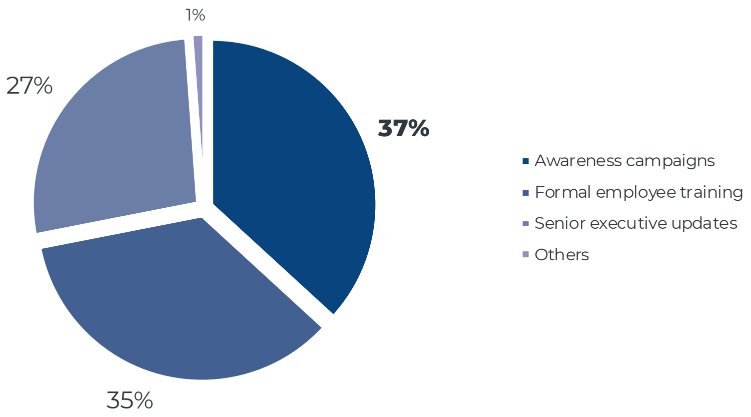
Any successful data protection and privacy program requires employees to be highly aware of their actions and are up-to-date on the latest regulations to make informed decisions.

Organizations that want to have a successful data protection and privacy program need formal employee training and awareness campaigns. The best results come when these efforts get really granular, down to individual responsibilities.

A technique that some organizations are employing is to conduct custom workshops that focus on the responsibilities of specific "privacy-important" teams.

In addition to keeping employees informed, at least 1 of 4 respondents are placing a higher emphasis on ensuring that senior executives are kept updated. Perhaps not surprisingly, 68% of these respondents had also highlighted the challenge of obtaining sufficient resources and budget for their data protection and privacy program.

What are the activities you will implement to build a privacy-aware culture? Please select all relevant choices.



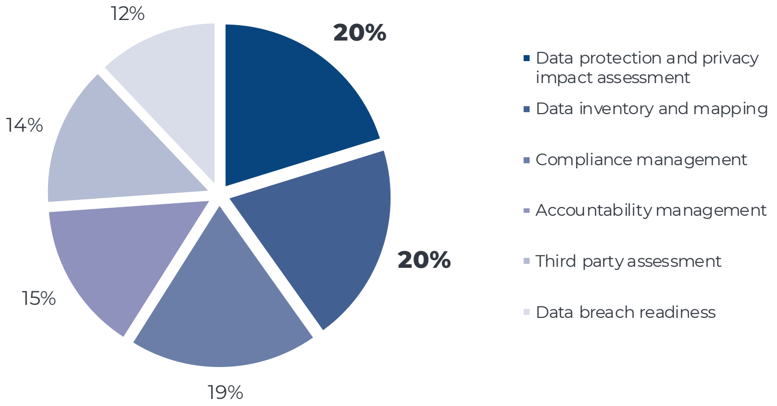
Companies are taking a proactive approach in managing their privacy risks and getting a better visibility of the personal data they are handling.

Almost 60% of respondents are making data protection and privacy impact assessment, data inventory and mapping, and compliance management top priorities at their organizations.

In light of all the high-profile data breaches in 2019 and several involving external service providers, it is surprising that data breach readiness and third party assessments are ranked the lowest among this set of priorities.

Organizations may still feel that the uncertainty of a data breach is less of a priority than the certainty of a hefty fine. While that is not without its logic, businesses still widely tend to underestimate the total cost of a breach.

What are the compliance management processes you will be implementing or enhancing? Please select all relevant choices.

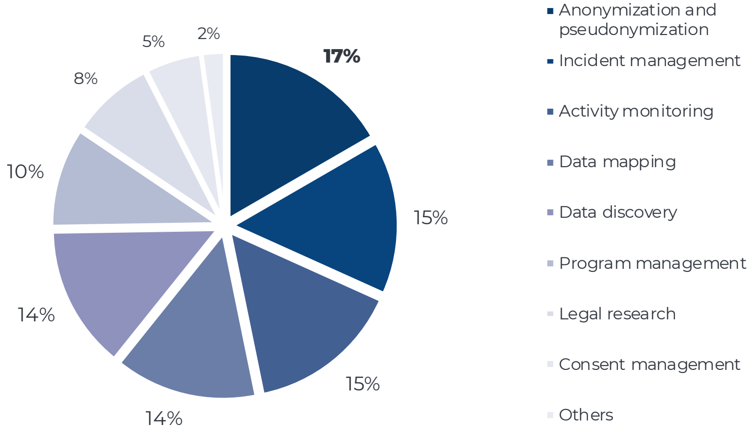


Companies are looking for solutions to reduce data processing risks without a corresponding drop in data utility while ensuring and monitoring for proper data access.

Organizations are primarily looking to reduce their data processing risks with anonymization and pseudonymization solutions. There is also an increased interest in incident management and activity monitoring tools. Risk reduction appears to be strongly focused on the areas of authorized access and ability to quickly defuse any internal security incidents.

The expressed prioritization of data protection and privacy impact assessment is also reflected in the continued interest in data mapping and discovery solutions. While data mapping and discovery tools did drop from the No. 1 and No. 2 spot last year, it is perhaps an indication of widespread investment in these solutions over the course of 2019.

What are the supporting technologies and solutions you will be evaluating or implementing?



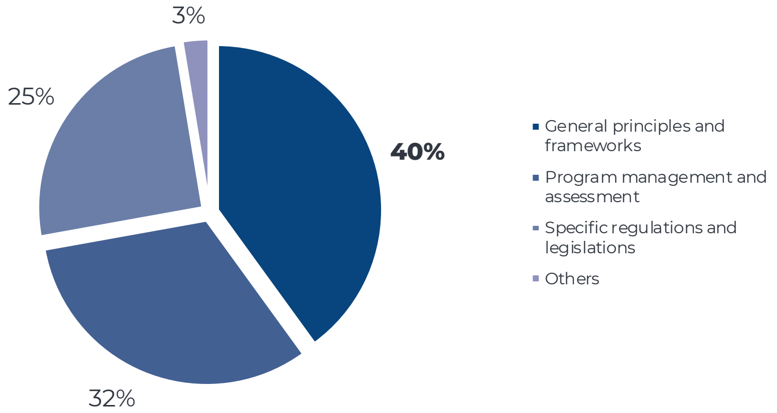
In terms of training, data protection and privacy officers are focusing on foundations and fundamentals to provide a strong base from which to address multiple compliance situations.

This year, respondents are focusing more on general principles and frameworks (40%) than on the specific regulatory situations of regions and countries.

This would appear to be in line with the expectation that many countries will soon pass new or updated national data handling laws.

A more general and adaptable framework makes sense in an environment in which countries are considering several different proposed pieces of legislation and it remains unclear as to what their final data protection regulations will look like.

What are the training areas most relevant for your team members? Please select all relevant choices.



Key Finding 3

Priorities shift with the maturity of data protection and privacy programs

As an organization's data protection and privacy program matures, the focus increasingly shifts from training to deploying supporting technologies and solutions.

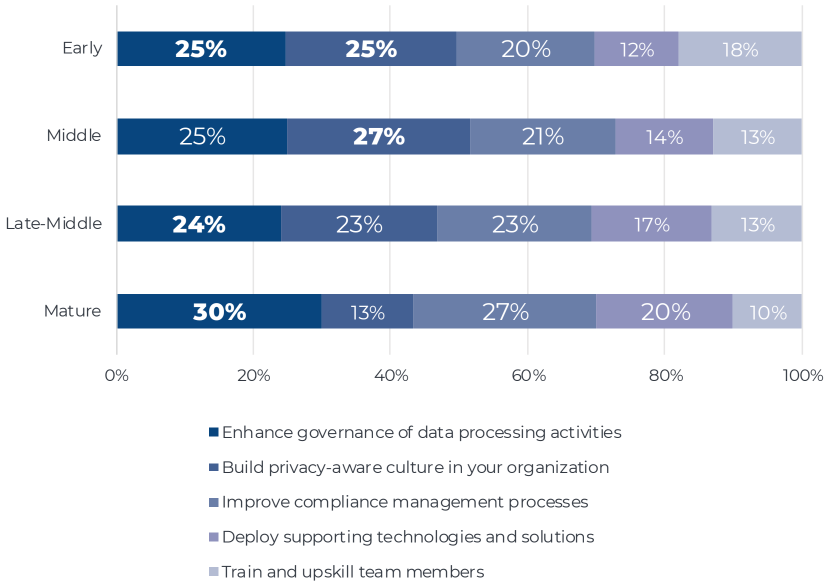
In the Early and Middle stages, organizations place a greatest emphasis (26%) on building a privacy-aware culture as a foundation. There is also a focus on improving the governance of data processing activities.

Even as organizations transition to the Late-Middle and Mature stages, better governance of data processing remains critical, indicative of a continual battle faced by privacy teams.

Organizations are generally not focusing on deploying supporting technologies and solutions until they are in the mature stages. We see an increase from 12% for Early stage organizations to 20% for those at the Mature stage.

Conversely, as organizations move through the phases of maturity, the emphasis on training decreases.

Top Priorities by Maturity



Key Finding 4

Almost half of organizations allocate less than 5% of governance, risk and compliance budget to data protection and privacy

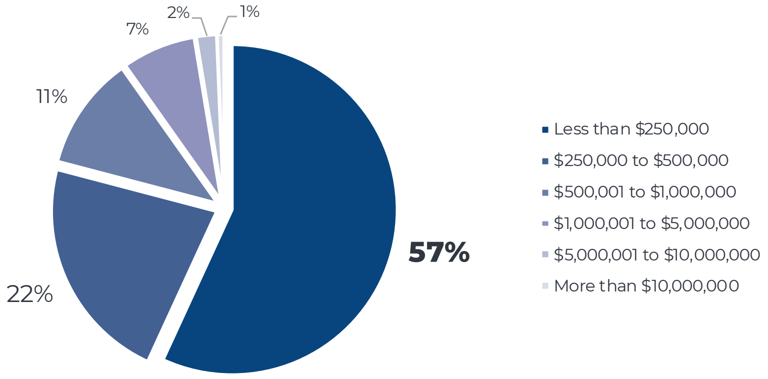
Though data protection has become widely accepted as a priority for every company of any size, almost 4 out of 5 organizations are maintaining only a modest annual budget.

Over half of the organizations surveyed (57%) are spending less than $250,000 on data protection and privacy activities across the entire company.

According to a recent IAPP salary survey, the median salary of a privacy professional is $123,050. This means that 57% of organizations probably have no more than two privacy specialists on staff, and may likely only have one.

Just 1 of 5 organizations (21%) are spending more than $500,000 per year on data privacy and protection. This is somewhat surprising since 31% of respondents work in organizations with more than 10,000 employees.

Approximately, what dollar range best describes the current annual budget for data protection and privacy activities across the enterprise?



A worldwide headcount of 5,000 employees appears to be the point when organizations begin to ramp up their spending on data protection and privacy.

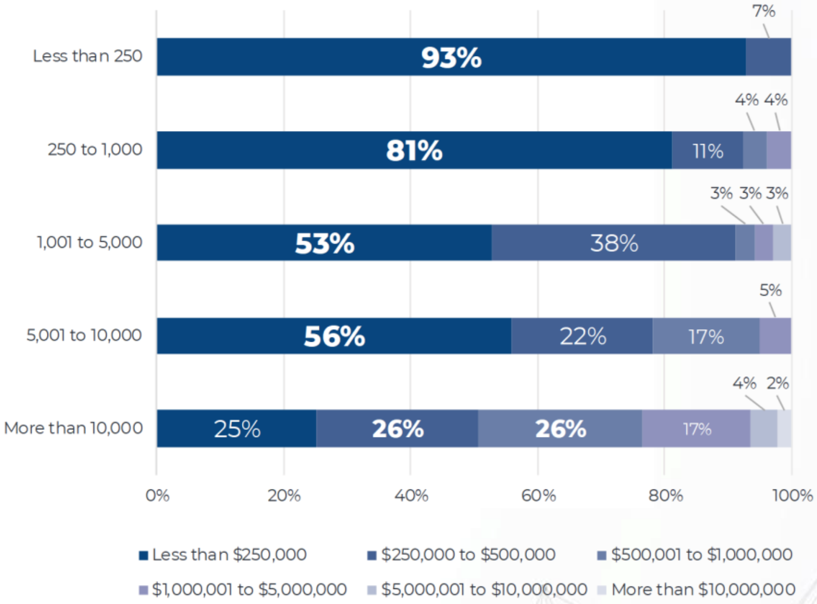
A vast majority of small and medium enterprises (87% of those with less than 1,000 employees) are spending less than $250,000 on data protection and privacy activities.

Slightly more than half of large enterprises (between 1,001 – 10,000 employees) have the same limited budget.

Of the larger enterprises with over 10,000 employees, 23% spend over $1,000,000 annually on data protection and privacy activities.

Well it does not come as a surprise to see budgets increase for bigger enterprises, 94% of enterprises with less than 5,000 employees are still operating with a budget of less than $500,000.

Annual Budget by Organization Size

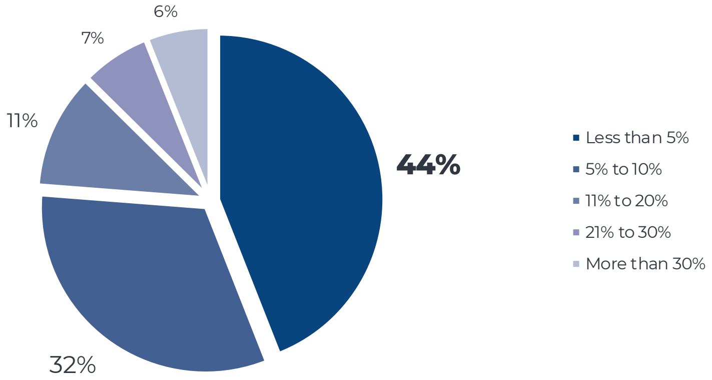


Spending is still relatively low compared to overall governance, risk and compliance budget as 3 of 4 organizations allocate less than 10% to data protection and privacy activities.

Nearly half of all organizations are spending less than 5% of the annual governance, risk and compliance budget on data protection and privacy activities. And 76% of all organizations are allocating less than 10% out of the overall budget.

Though organizations consistently name data protection and privacy compliance as a high priority, there still seems to be broad resistance to increasing annual spend on it. Some combination of preparatory spend in 2018 and the slow roll-out of GDPR fines in 2019 may at least partially explain this. Another possible conclusion is that enterprises still do not fully understand what is required to be compliant. This is further supported by the challenges faced by 53% of respondents in obtaining sufficient budget and executive support.

Approximately, what percentage of the current annual governance, risk and compliance budget will go to data protection and privacy activities?



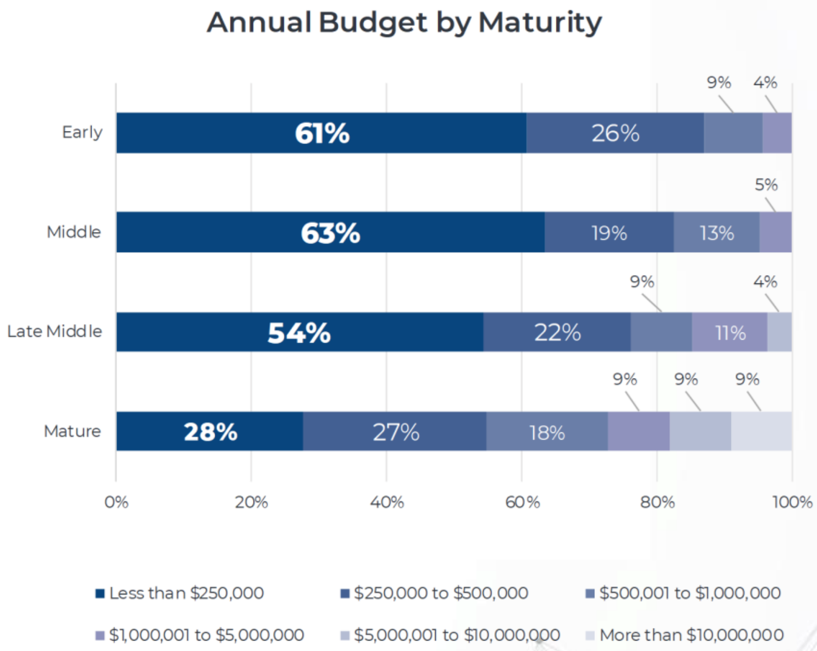
Though more work is required, and presumably more resources are needed in the early stages, spending goes up only as the data protection and privacy program matures.

Though one might assume that organizations at an early stage would be among the biggest spenders in getting new programs established, 87% spend less than $500,000 on their data protection and privacy activities.

Spending patterns do not necessarily increase significantly until a company gets close to maturity. Just 40% of the organizations in the Early to Late-Middle stages are spending more than $250,000 annually.

Organizations in the early stages of maturity clearly have more work to do, but likely tend to spend less due to budget and resource challenges rather than a lack of desire or awareness.

Spending increases consistently correlate with increases in maturity. This is likely due to the establishment of a privacy-aware culture and increased executive support.



Key Finding 5

1 of 4 organizations have just one data protection and privacy specialist on staff

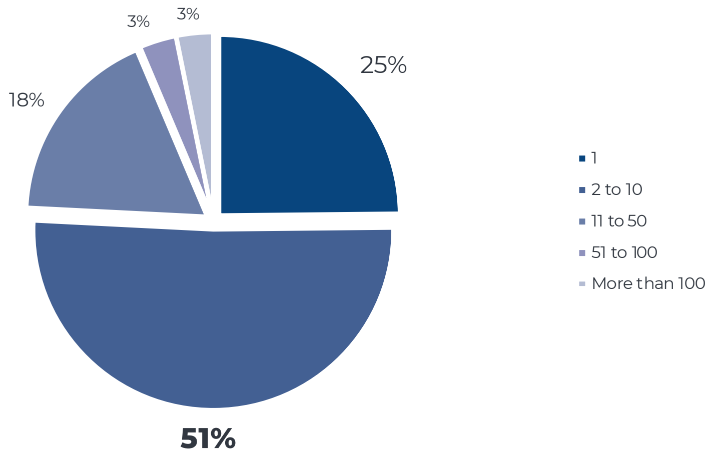
Faced with budgetary challenges, 3 of 4 organizations have fewer than 10 employees staffing their data protection and privacy programs

Our results show that 1 of 4 organizations have just one privacy specialist on staff. And 76% have fewer than 10 employees in the data protection and privacy function.

The fact that 27% of respondents report budget challenges but only 11% face a hiring problem indicates that the problem tends to be one of getting executive support for resources.

This trend of understaffing is likely to continue in 2020 as the passage of new regulations across the globe further strains a tight labor market.

What is the worldwide headcount of the data protection and privacy function?

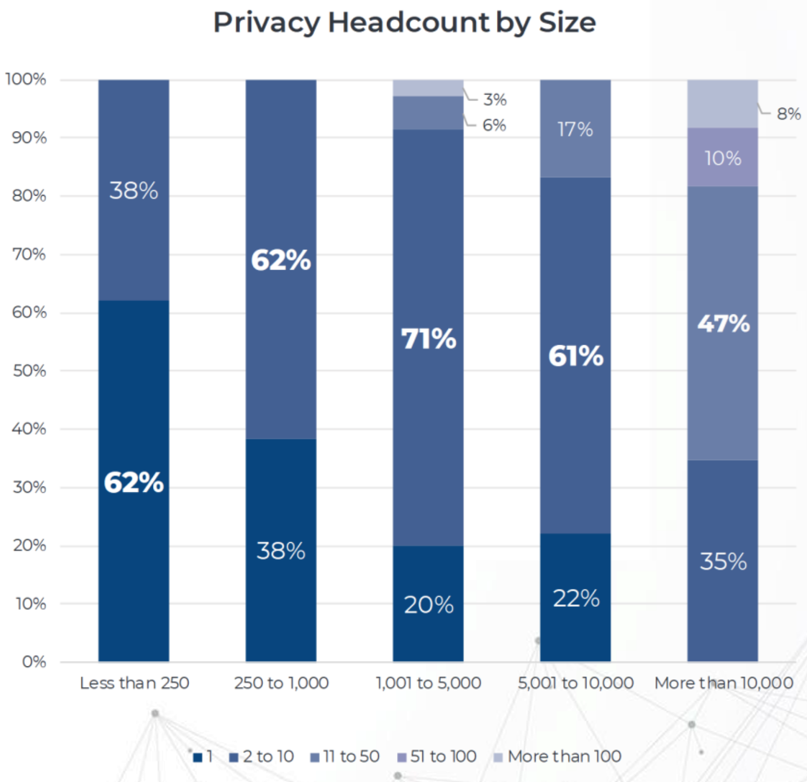


About half of organizations with fewer than 1,000 employees have a data protection and privacy function with only one staff member assigned.

Overall, 94% of organizations with less than 10,000 employees have a privacy function with fewer than 10 headcounts.

While organizations tend to staff up as they increase in size, only half of organizations with more than 5,000 employees have over 10 staff members in the data protection and privacy function.

Headcounts don't change significantly until the size of the organization is over 10,000 employees. These may be large multinationals that operate in a variety of legal jurisdictions, creating an increased number of specific functional roles. The larger organizations are also much less likely to face the budget challenges seen across smaller organizations.



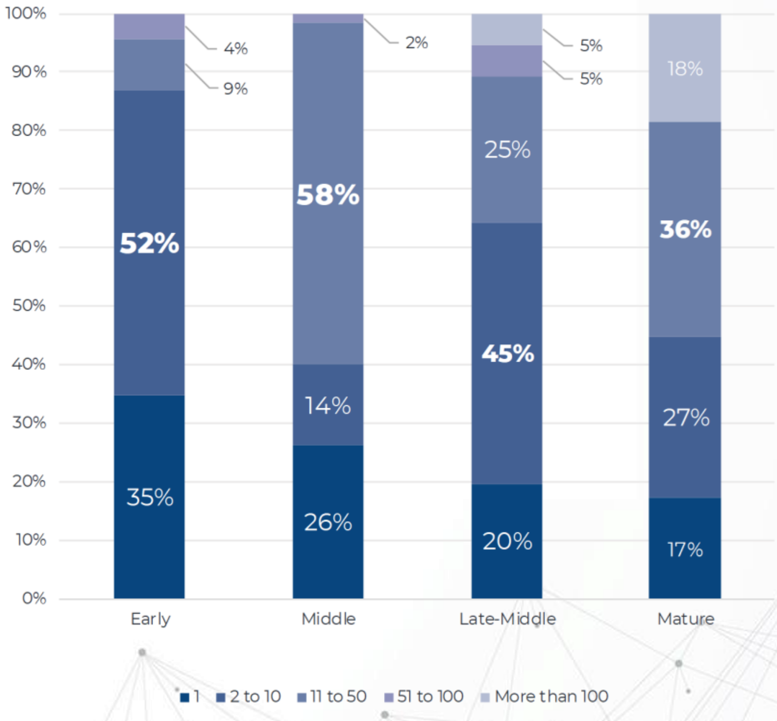
As privacy programs mature, the organizational headcount in the data protection and privacy function increases to meet the demands of a more sophisticated program.

Executing a comprehensive data protection and privacy program with limited resources is difficult, even more so when the organization is just getting started.

In our study, 35% of organizations in the Early stage are getting their programs underway with just one employee assigned. And 87% have fewer than 10 employees in the data protection and privacy function.

Organizations are more likely to staff up as programs get more sophisticated. For organizations with Mature programs, 18% have a headcount of more than 100.

Privacy Headcount by Maturity



Conclusions and Recommendations

Getting executive-level support and leveraging organizational resources and technology may be key to addressing challenges

> Clearly, data protection and privacy officers have a tough job to do. Pulling the right levers can help them do more with less to overcome challenges and achieve their priorities for 2020.

As the regulatory landscape becomes more demanding and enforcement actions more severe, data protection and privacy officers will have to focus on key levers to quickly achieve program maturity and meet program objectives.

Executive support is crucial, along with other measures such as earlier implementation of new technologies and more effective rollouts across all of the organization’s departments and functions.

Executive-level support key for sufficient budget

Getting executive support is particularly crucial in overcoming budget issues. Education of the C-suite is the key. Executives need to confront the actual cost of fines and breaches as compared to preventive expenses. By building an overall roadmap in the early stages of maturity, the data protection and privacy specialist can facilitate both the allocation of needed resources and shared understanding throughout the organization. To get executive-level support, data protection and privacy officers must communicate a clear and pragmatic roadmap and the resources needed to quickly elevate the organization's program.

Companies that have made it to the mature stage of their programs appear to have successfully navigated this particular path, with only 4% continuing to rank executive-level support as a priority and 27% working with an annual budget of at least $1,000,000.

Early use of privacy technology may be crucial

The highest rates of deployment of supporting privacy solutions is seen in mature organizations (20%). In part, this is because organizations at this level also have the most trouble hiring and retaining qualified personnel (30%). Effective use of technology and automation can help alleviate the human resource crunch and allow data protection and privacy officers to focus on high value work.

Organizations still in the earlier stages of maturity may be well-served by getting these solutions in place earlier in the process and heading off the recruiting issue before it begins for them. By reducing their personal data usage footprint, developing organizations can lower compliance costs to offset some of the expense.

Early technology implementation can also help to move program goals at any level within reach, and will be particularly helpful with the high-priority improvement of governance over data processing.

Alleviate resource crunch with privacy champions

Organizations that are experiencing resource and headcount issues are increasingly turning to "data privacy champions" to help fill the knowledge gaps in their data privacy and protection programs. These administrative positions directly support the data protection and privacy officers and include representatives from business units throughout the organization.

This internal network of data privacy champions can directly and effectively address the need to build a unified organization-wide privacy culture and keep all business units within the loop and continually updated as to policies and best practices.

Having privacy champions across the organization functions can also help address the challenge of working with business units to integrate data protection and privacy measures.

About the Survey

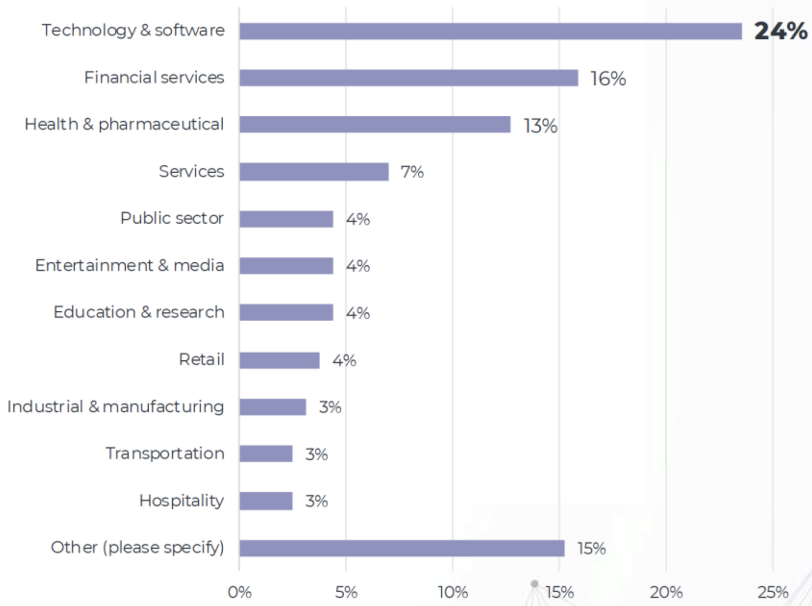
Total of 471 Respondents from around the world representing 16 industries and different maturity levels

For this report, we invited professionals with data protection and privacy responsibilities in their organization to participate in a survey on their challenges and priorities for 2020.

A total of 471 responses were collected and a total of 16 industries were represented. The largest sectors were Technology & Software and Financial Services.

* *Others: Agriculture & food service, communications, consumer products, defense & aerospace and energy & utilities*

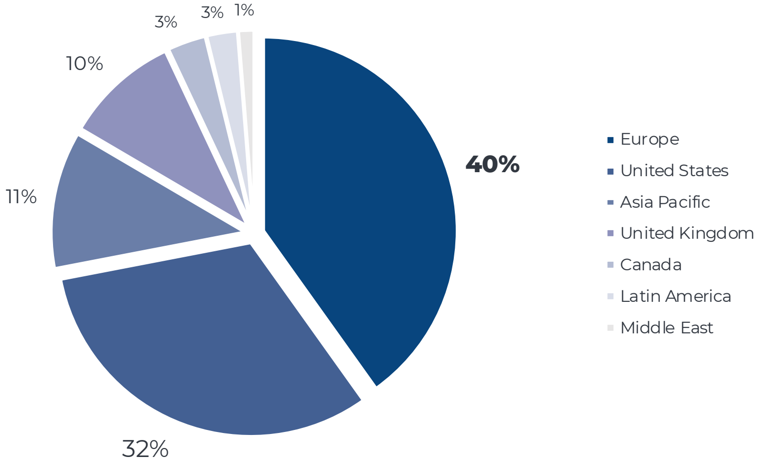
What industry best describes your organization?



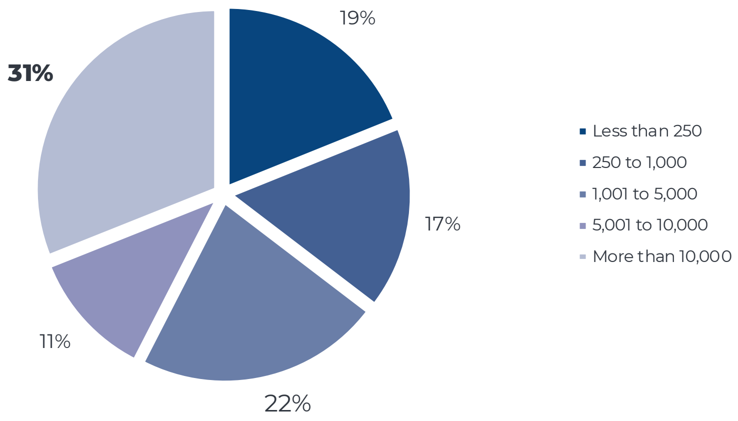
Respondents are working in organizations from around the world with 82% from Europe (including the United Kingdom) and the United States.

Respondents from organizations with more than 10,000 employees represented the largest segment and 64% have more than 1,000 employees.

Where is your organization headquartered?



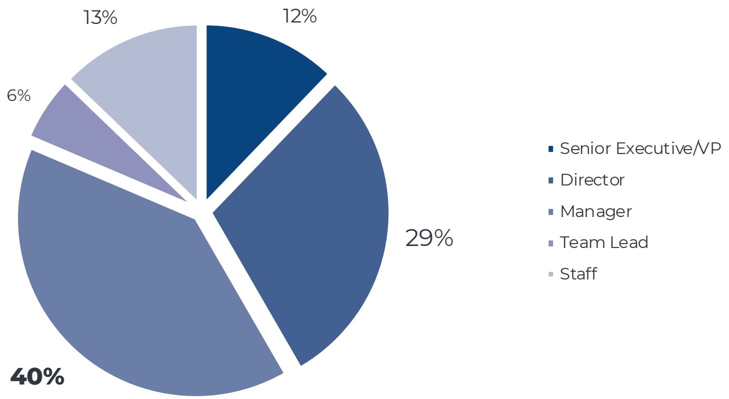
What is the worldwide headcount of your organization?



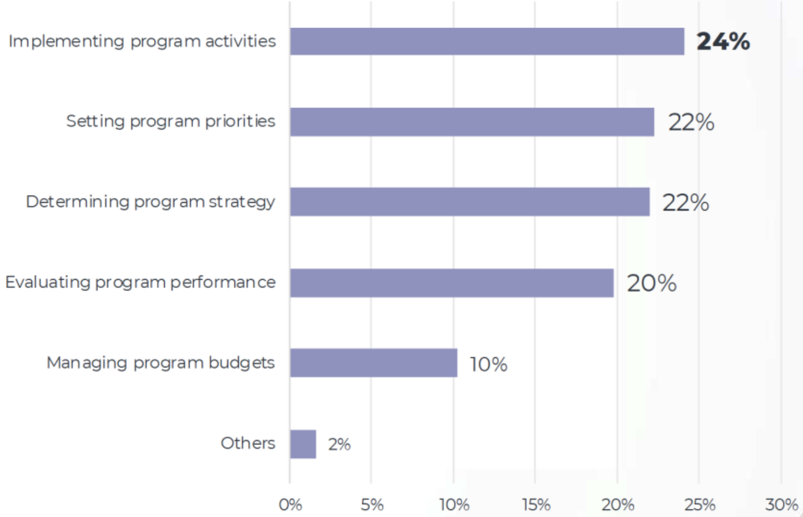
81% of respondents hold managerial positions and above with 41% holding a position of Director or Senior Executive/VP.

Respondents have responsibilities across all areas of a data protection and privacy program.

What organizational level best describes your current position?



What best describes your role in managing the data protection and privacy function or activities within your organization? Check all that apply.

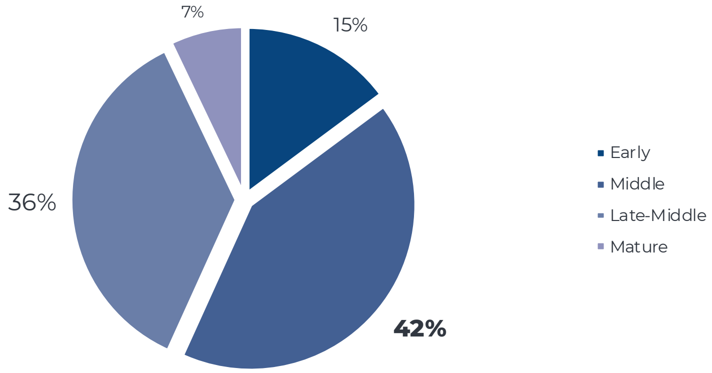


Respondents were asked to rate the maturity of their organization's data protection and privacy program:

- Early stage – Many program activities have not as yet been planned or implemented
- Middle stage – Program activities are planned and defined but only partially implemented
- Late-middle stage – Most program activities are implemented across the enterprise
- Mature stage – Program has successfully been implemented across the enterprise

The majority of organizations (78%) are in the Middle and Late-Middle stage. Only 15% were in the Early stage and 7% were in the Mature stage.

What best describes your organization's stage of maturity in its implementation of a data protection and privacy program?



CPO
MAGAZINE

About us:

We provide news, insights and resources to help data privacy, protection and cyber security leaders make sense of the evolving landscape to better protect their organizations and customers.

enquiries@cpomagazine.com

www.cpomagazine.com

Follow us:

twitter.com/cpomagazine

linkedin.com/company/cpomagazine

facebook.com/cpomagazine