FTI CONSULTING™

FUTURE-PROOFING CORPORATE DATA PRIVACY: BUDGETING AND SOLUTIONS TO ADDRESS TOMORROW'S COMPLIANCE CHALLENGES

EXPERTS WITH IMPACT™

Data privacy is one of the most talked about topics in state and federal legislative sessions today.

A movement that took the international stage with the enactment of the General Data Protection Act (GDPR) in 2018—and gained momentum with the passage of the California Consumer Privacy Act (CCPA) and Brazil's General Data Protection Law (LGPD)—is building into a tidal wave of anticipated regulations worldwide. For multi-national corporations, future-proofing data privacy and compliance programs against the incoming flow of new and evolving global laws may seem futile, or impossible.

To understand how organizations are balancing the costs and risks of managing data in compliance with privacy laws, FTI Consulting recently surveyed more than 500 leaders of large, U.S.-based companies. All of the respondents—60 percent held titles in senior management or the C-suite and 28 percent held other management roles—had knowledge of their organizations' data privacy policies and activities. Survey results showing the present status of corporate privacy initiatives were revealed in part one of this series, *Corporate Data Privacy Today: A Look at the Current State of Readiness, Perception and Compliance*.

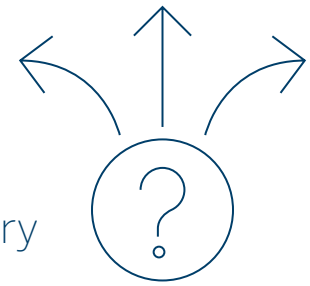
The first report discussed the importance of implementing a strategic combination of people, process and technology to mitigate data privacy risk. Fortunately, most respondents indicated plans to deploy a diverse set of data privacy solutions in the coming year. This suggests that organizations are beginning to understand the importance of expanding their approaches to privacy alongside expanding laws. In this report, we'll cover emerging plans, and share corporations' views of today's uncertainties. Key insights and the many steps being taken to prepare for the challenges of tomorrow include:

- A Radical Increase in Spend
- The Data Risk vs. Value Balancing Act
- Dynamic Problems Require Dynamic Solutions
- Strengthening the Front Lines

A NOTE ON THE SURVEY AND THE COVID-19 PANDEMIC

The data in this survey was collected in late 2019 before the global pandemic took hold and made drastic alterations to work and hiring patterns. While some of the survey data in these areas has changed radically; for example, the trend shown by 77% of survey respondents indicating an increase in Data Privacy hires in the next 12 months has largely morphed into hiring freezes across all sectors of corporate America, a large majority of the findings continue to be relevant. Some are even more crucial in this new normal, where regulators are not backing down from enforcement and new pandemic-related challenges to data privacy and security seem to crop up daily. Likewise, the questions and struggles reflected in the the survey data continue to be best-supported by the strategies of being proactive and prepared when it comes to data privacy.

More than one-third of organizations are concerned about regulatory uncertainty



A RADICAL INCREASE IN SPEND

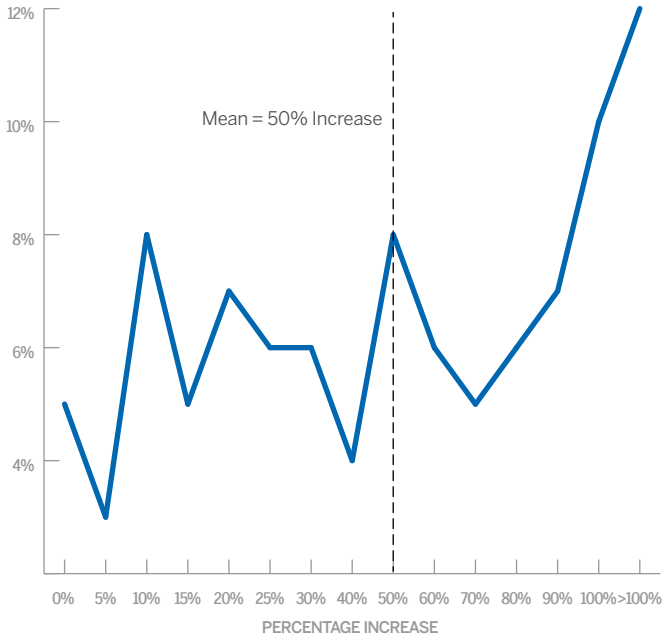
Significant changes—in budgeting, technology implementation, policy and more—are afoot across nearly all organizations surveyed. One of the survey's most compelling findings is around organizations' plans to significantly increase spending in the coming year and beyond.

> "The extent to which organizations said they expect to increase their data privacy spend is both surprising and encouraging. Data privacy enablement involves change across policies, systems, infrastructure and day-to-day business practices—initiatives that can incur substantial costs. Organizations that are realistic about the costs, and adjust their budgets and resource allocations accordingly, will have a much easier time adapting to the continually changing landscape." – **Jake Frazier**, *Senior Managing Director*, FTI Technology

Budgets Will Spike

Ninety-seven percent of organizations will increase their spend on data privacy over the next 12 months, with an average increase of 50 percent. Nearly one-third indicated they will increase data privacy budgets by between 90 percent and more than 100 percent. The manufacturing industry stood out as one of the biggest spenders, with more than 20 percent citing plans to raise budgets by 100 percent or more.

By what percentage do you expect your organization's spend on data privacy compliance overall to change over the next 12 months?



A Growing Resource Gap

To date, 57 percent of respondents said they have appointed in-house staff dedicated to data privacy compliance and crisis response. Despite that fact, and as reported in part one of this series, nearly 60 percent were still concerned about a shortage in resources. With pandemic-related hiring freezes in play, that shortage stands to become more acute as privacy needs continue to rise.

> "Companies have spent substantially to stand up privacy programs to reduce risk and are now confronted with having to scale back -- a whipsaw that can significantly degrade ROI and expose them to even more risk. Access requests continue to come in, Privacy Impact Assessments continue to be submitted, and new vendors continue to need review and onboarding despite internal shortages. Companies may ultimately find that hiring freezes do more damage than good in the compliance function." - **Andrew Shaxted**, *Senior Director*, FTI Technology

More Costs, One Way or Another

Among current data privacy laws, fines are on a steady increase—as of January 2020, fines under GDPR had exceeded €114,000,000, and early estimates by the California Attorney General[1] pinned the initial cost of CCPA compliance at $55 billion. Survey respondents said they expect, on average, a nine percent drop in global turnover as a result of a data privacy crisis event, which can be extrapolated to a total loss of $79 million. Organizations should consider the reality that data privacy costs are going to increase in one form or another. Investing that money proactively in preparedness and compliance will generate returns in customer confidence, brand reputation, risk mitigation and avoidance of penalties. Conversely, non-compliance, and the related investigations, fines and reputational damage, has the potential to wreak havoc, and cost as much or far more.

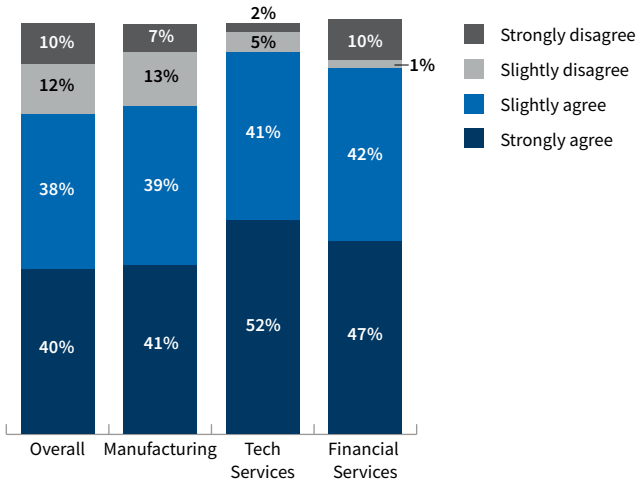
THE DATA RISK VS. VALUE BALANCING ACT

Data holds tremendous value. Still, the more data a corporation holds, the more risk it introduces. As the landscape increases in complexity, and data volumes continue to explode, corporations face a delicate balance between retaining data for its business worth and minimizing it to mitigate risk.

Some Risk is Worthwhile

Many organizations are willing take risks on the compliance front in the interest of gaining more value from their data. In the survey, 78 percent agreed with the statement: "The value of data is encouraging organizations to find ways to avoid complying fully with data privacy regulation". The sentiment was even stronger among respondents in the tech sector, with 93 percent in agreement.

How strongly do you agree or disagree with the following statements: "The value of data is encouraging organizations to find ways to avoid complying fully with data privacy regulation"?

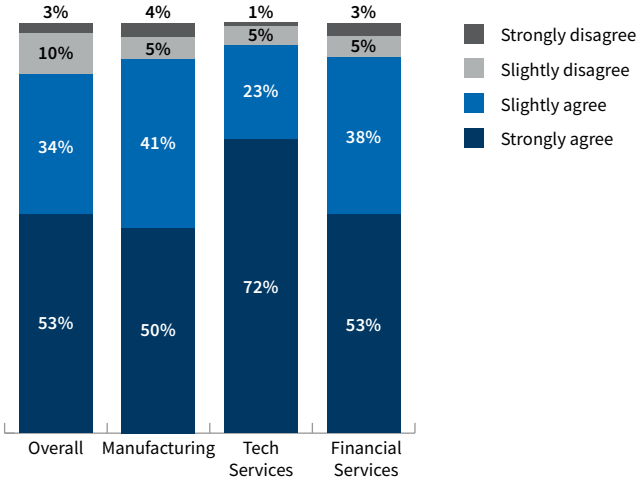


"Recognizing the interconnectedness of data and risk from different vantage points will inform critical decisions about how an organization balances data value and risk. More, investing in strategic initiatives to deal with data risk will make the difference between success and failure—across long-term business viability, consumer trust and compliance." –**Sonia Cheng**, *Managing Director*, FTI Technology

Is Good Faith Good Enough?

Just as data is valued differently from company-to-company, data privacy risk tolerance is highly nuanced and unique for each organization. When forming a position on risk tolerance, many corporations weigh whether, and to what extent, regulators will consider their existing efforts "good enough". Most respondents (87 percent) believe that steps towards compliance will mitigate regulatory scrutiny. In fact, more than half strongly agreed with this idea.

How strongly do you agree or disagree with the following statements: "As long as you show you're making steps to be compliant with data privacy, organizations can mitigate regulatory scrutiny"?



"To remain competitive, you need to run a fluid and tactile business. Products change, services adapt, and the needs of customers shift. "Good enough" is a relative term. Being comfortable with current readiness should not shut down innovation and progress. Keep moving forward, document progress, and continuously scan the horizon for new risks." – **T. Sean Kelly**, *Senior Director*, FTI Technology

Dynamic Problems Require Dynamic Solutions

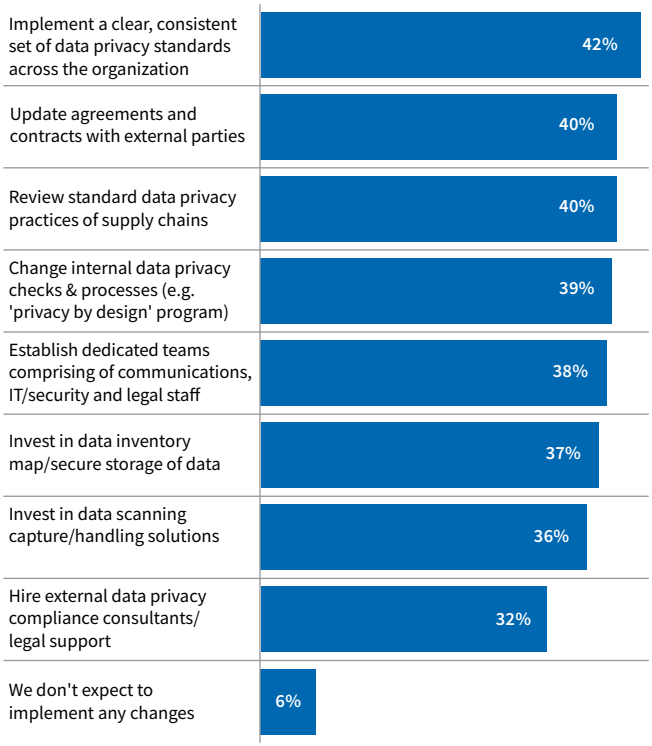
Most respondents demonstrated a strong technology position, but room for improvement in internal expertise and process. The good news is that most indicated substantial plans for progress in the coming 12 months.

A Wide Range of Programs are Set to Move Forward

Of the solutions ranked in the survey, most were evenly stacked. Solutions planned for implementation over the next 12 months include the following (a mere six percent noted they had no changes planned):

- Establish dedicated teams
- Change internal data privacy checks/build privacy by design programs
- Data scanning/handling solutions
- Data inventory map/secure storage of data
- Hire external data privacy compliance consultants
- Update agreements and contracts with external parties
- Review standard data privacy practices of supply chains

Which of the following do you expect your organization to implement over the next 12 months to prepare for regulatory change and requirements relating to data privacy? (Please select all that apply)



Consistency is Key

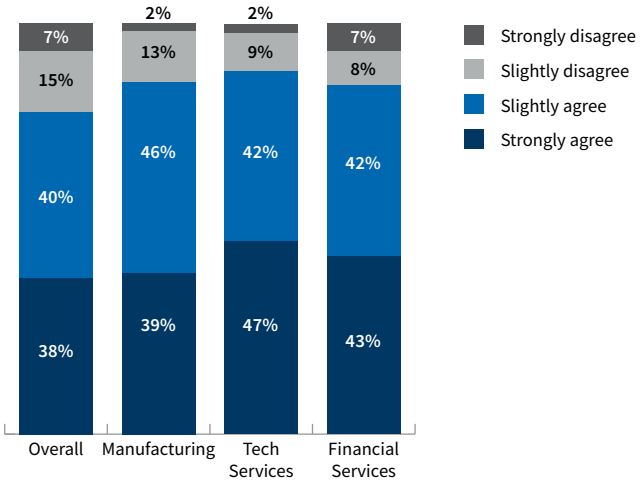
Most respondents said they are focused on establishing a clear, consistent set of data privacy standards across their organizations. When asked about plans to prepare for regulatory change and requirements relating to data privacy in the coming year, 42 percent cited this approach (more than any other solution).

STRENGTHENING THE FRONT LINES

Some privacy regulations, including the GDPR, require training and awareness programs. Under laws with these types of guidelines, failure to embed a culture of privacy into the organization may be interpreted as a lack of compliance.

> "More than 75 percent of organizations agreed that they should be doing more to communicate data privacy compliance protocols. Robust training and awareness campaigns are essential to maintaining long-term data privacy compliance. Looking ahead, the front lines of an organization—its employees and close partners—will need to be better supported in carrying out and maintaining programs and adopting new privacy technology." – **Chris Zohlen**, *Managing Director*, FTI Technology

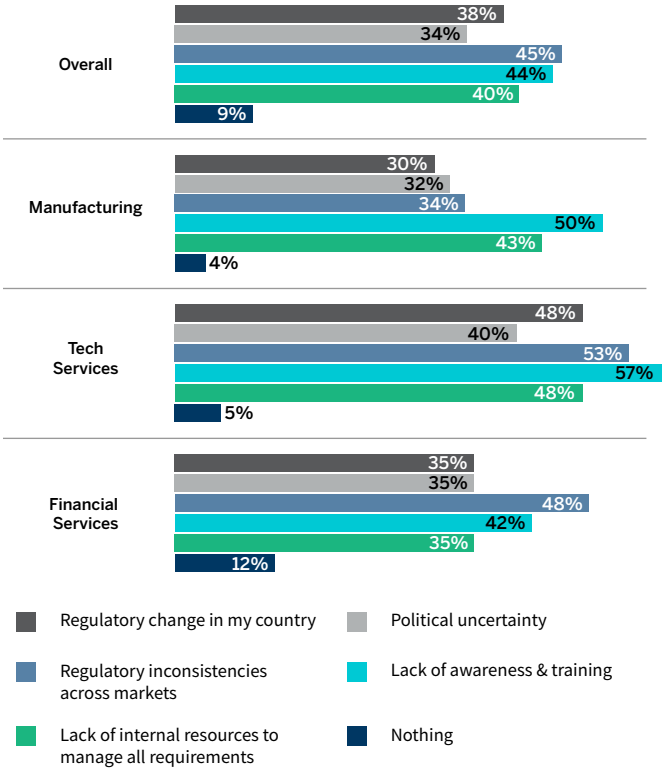
How strongly do you agree or disagree with the following statements: "Our organization needs to do more to communicate our data privacy compliance protocols"?



Lack of Awareness and Training Remains Pervasive

While a large majority of respondents said they think they need to do more to communicate their privacy protocols, another 44 percent said they expect lack of awareness and training to be the key data privacy challenge of the coming year. Still, training receives only 17 percent of privacy-related spending. This raises a flag for in-house teams to consider whether they need to realign increases in spending to better fit with their top known and expected challenges.

Which of the following do you feel are key challenges for data privacy over the next 12 months? (Please select all that apply)



CONCLUSION

The pandemic and the world changes it has wrought have made the future of data privacy more uncertain than ever, and today's ambiguous landscape is top of mind for many legal, compliance and executive teams. Laws will continue to emerge and evolve. The nature of how we work will continue to change, while enforcement priorities among regulators will not abate. Corporations are still at the tip of the iceberg in terms of the scope of requirements that may ultimately come into play.

What the experts do know is that **corporations have a wide range of best practices and solutions that will help future-proof their position for constant change. A global data privacy framework that is at once encompassing of an organization's full regulatory obligations and malleable to align with nuances at a regional or local level is essential.** Comprehensive awareness and training campaigns will support compliance and reduce the risks of accidental breach. When employees are aware of the issues and trained on how to execute on the global privacy framework, they are less likely to fall afoul.

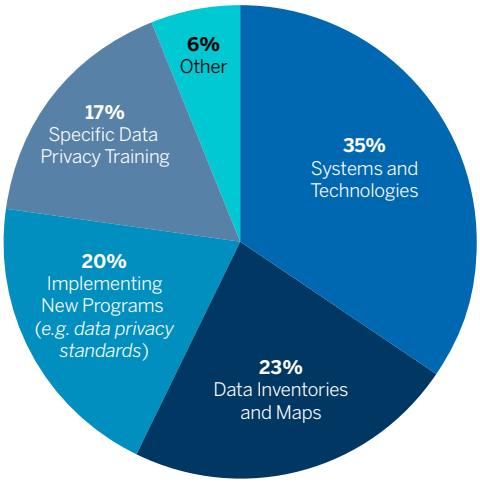
Organizations that take these steps, allocate adequate resources and develop a holistic culture of privacy will be ahead of the curve and bolstered to weather the tides of ongoing global change.

METHODOLOGY

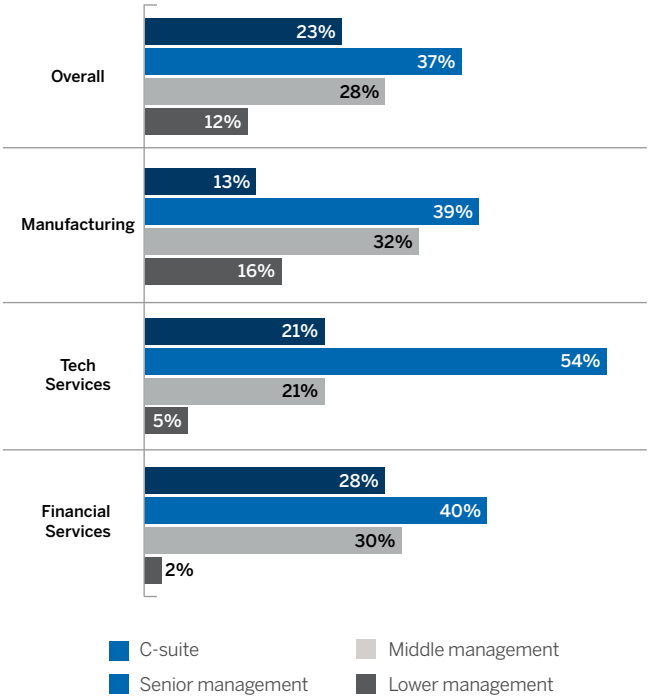
This survey was conducted by FTI Consulting's Digital & Insights practice during November 2019. More than 500 leaders of large-sized private sector companies, based in the U.S., with knowledge of data privacy policies and strategies, were polled. For any queries on the methodology, please contact James Condon, a Senior Director in FTI's Digital & Insights practice, at james.condon@fticonsulting.com.

The profile of the respondents includes the following:

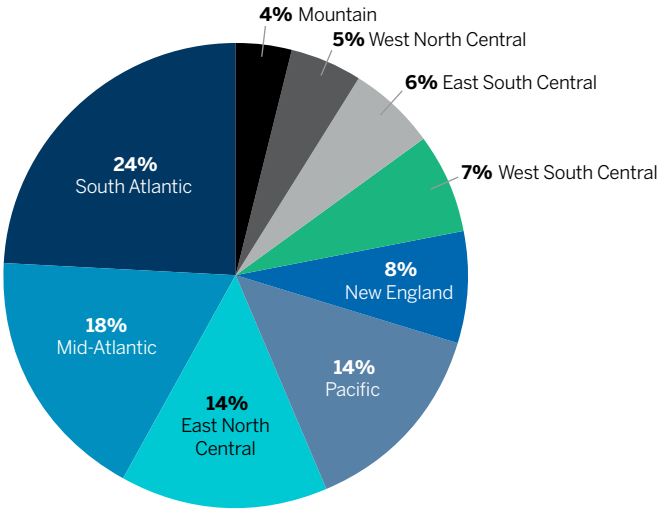
How would you best proportion your organization's spend on data privacy solutions and strategies over the last 12 months? (Please allocate 100 points on how your organization's spend is distributed)



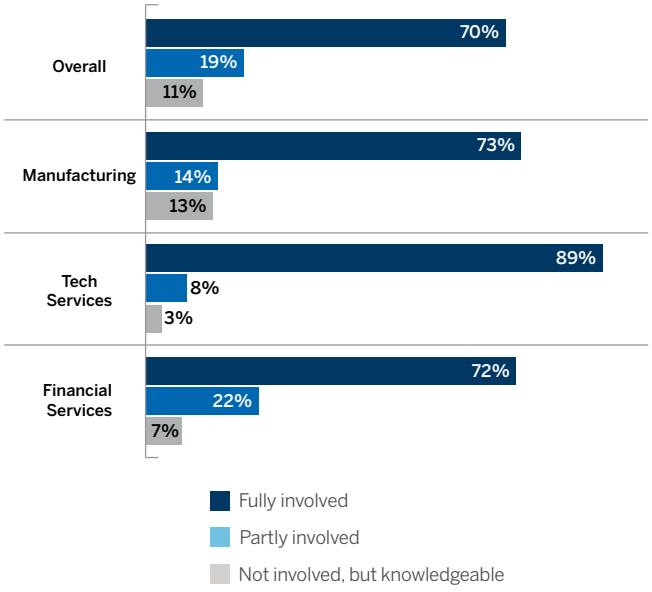
Which of the following best describes your position in your organization?



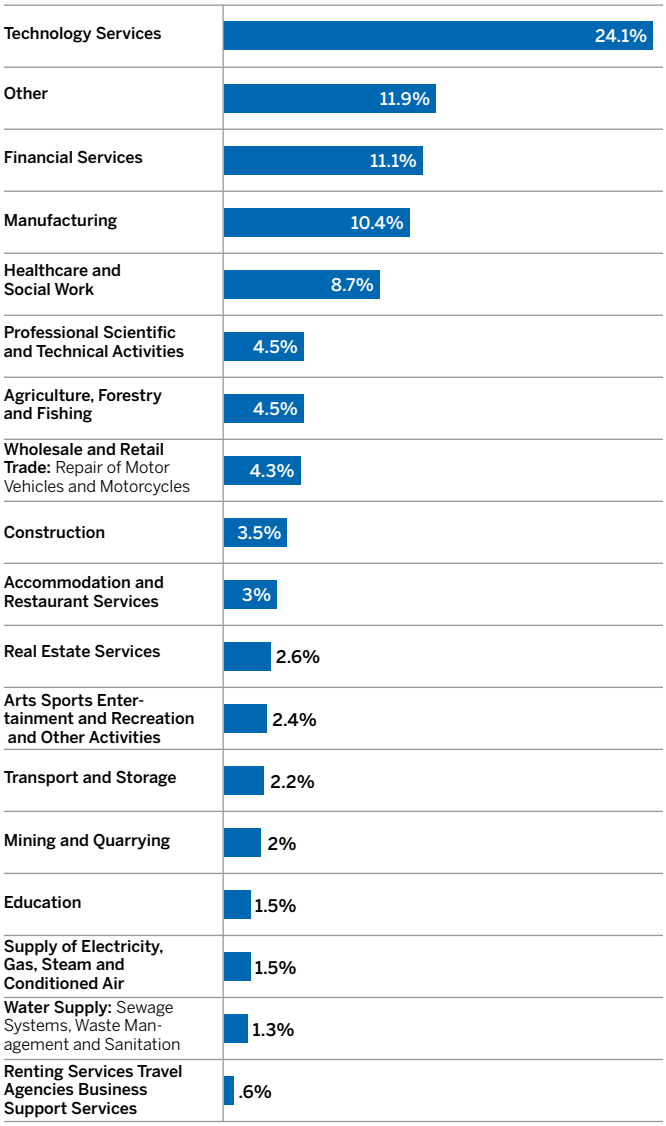
Where in the US are you mainly based for work?



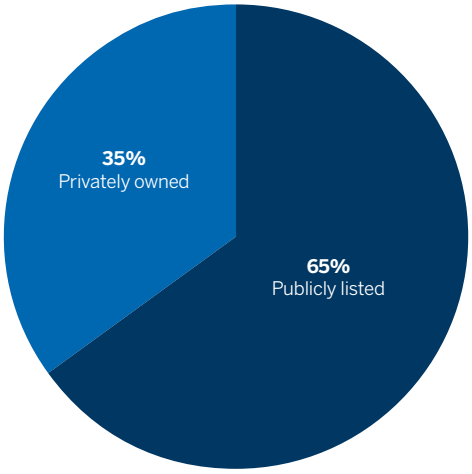
How involved are you in data protection, privacy, compliance and regulation for your organization?



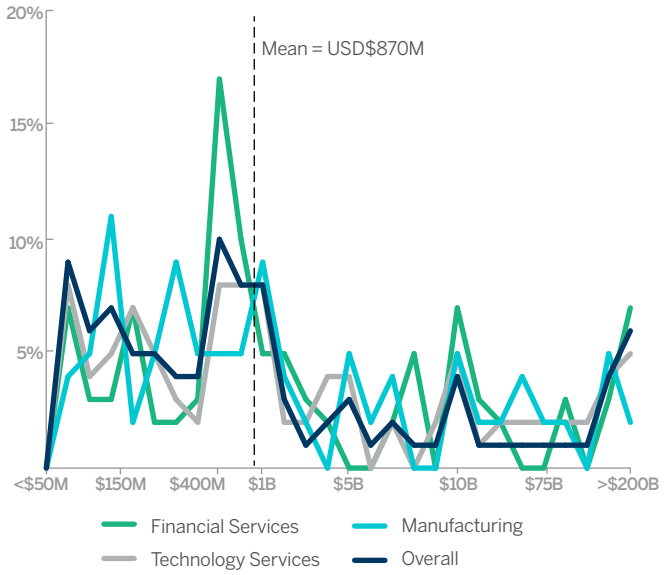
What industry does your company mainly work in?



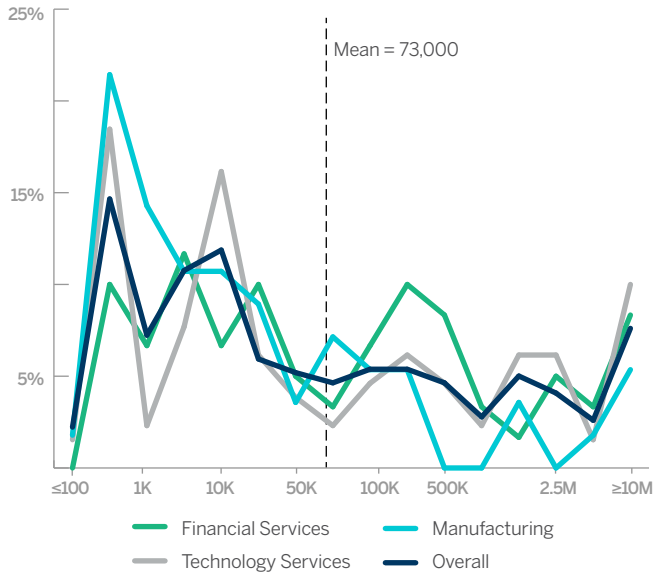
Which of the following would you use to describe your organization?



Approximately, what is your global turnover?



Approximately how many data subjects (individuals) does your organization hold?



Jake Frazier
Senior Managing Director
+1 (512) 971-6246
jake.frazier@fticonsulting.com

Chris Zohlen
Managing Director
+1 (415) 307-4956
chris.zohlen@fticonsulting.com

T. Sean Kelly
Senior Director
+1 (215) 606-4374
sean.kelly@fticonsulting.com

Andrew Shaxted
Senior Director
+1 (773) 658-0241
andrew.shaxted@fticonsulting.com

Deana Uhl
Senior Director
+1 (832) 667-5123
deana.uhl@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT™

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. For more information, visit www.fticonsulting.com and connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

00051220