DON'T LET DATA PRIVACY DISASTERS DERAIL DIGITAL TRANSFORMATION (SURVEY INSIGHTS)

BDO 2020 Digital Transformation Survey: Data Privacy Takeaways

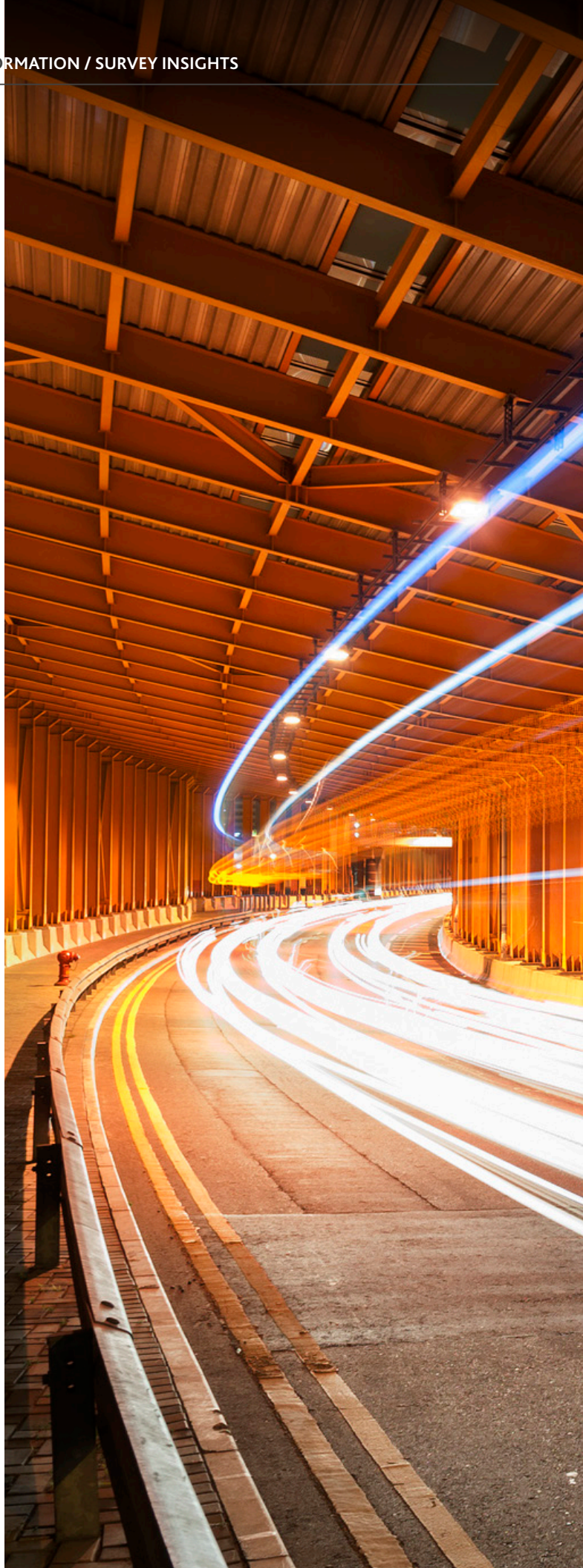
BDO

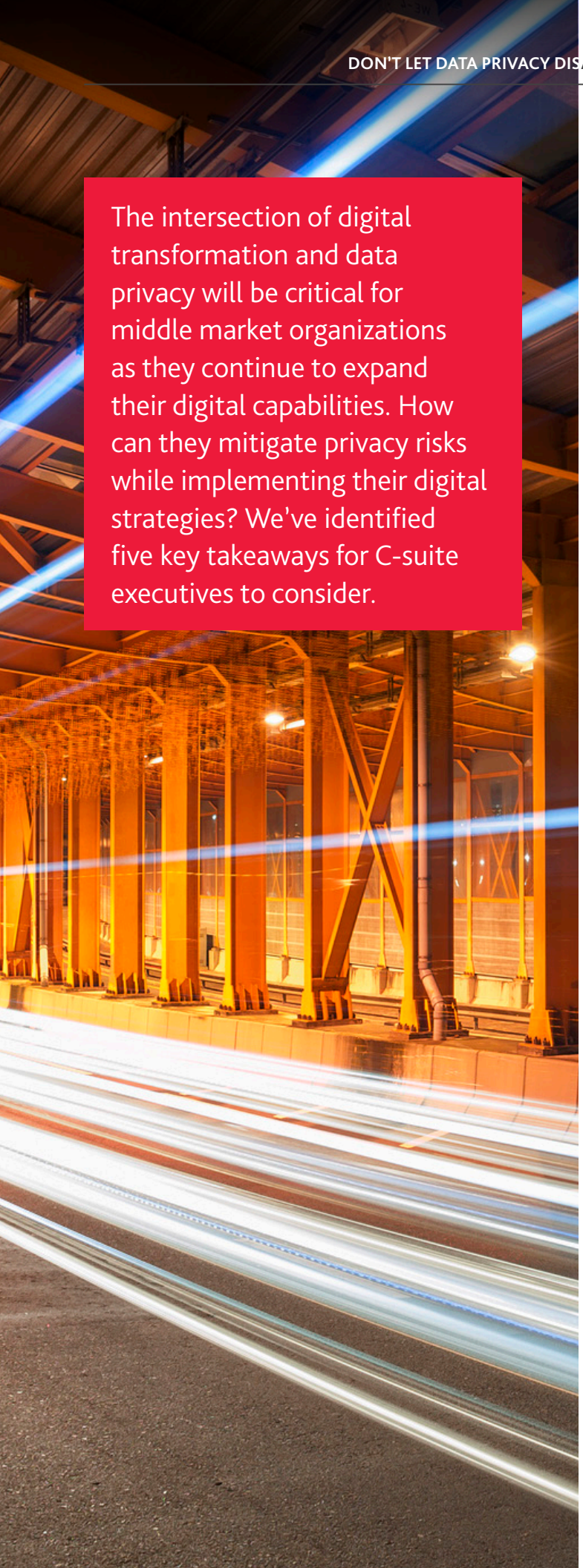
Imagine waking up to see your company's name strewn across the headlines at the center of a massive privacy breach—a mistake that could put all or most of your customers at risk. It sounds like a nightmare, but it's a real danger that companies face every day. If you don't have robust controls and threat-based data protection practices in place, your company data is vulnerable to cyberattacks and insider threats at all times.

The role of data privacy for companies of all sizes is rapidly evolving, and it should be at the forefront of every C-suite executive's mind. Data privacy is no longer an amorphous concept or aspirational goal – it is a firm legal obligation with compliance requirements set out in current legislation, such as the California Consumer Privacy Act (CCPA) and the EU's General Data Protection Regulation (GDPR). Privacy continues to be a focus in future legislation, especially as new technology for contact tracing and wellness apps is leveraged in the fight against COVID-19.

What does that mean for middle market organizations? BDO tackled this question in the **2020 Digital Transformation Survey**, which surveyed 600 middle market C-suite executives at organizations with annual revenues between $250 million and $3 billion. The survey found that 100% of respondents had already developed or were planning to develop a digital transformation strategy, but practices for data privacy varied.

In addition, the survey revealed that data privacy risks are at the forefront of middle market executives' minds: 39% of respondents cited cyberattacks as their #1 digital threat, and 59% said bolstering cybersecurity is one of their top three short-term goals (in the next 12 to 18 months). Forty percent said bolstering cybersecurity is among their long-term business goals (18 months to three years). As COVID-19 continues to impact cybersecurity, it's likely that these goals will continue to rise in importance for many organizations. Clearly, protecting personal data is an urgent need that cannot be ignored, and many companies are focused on addressing it now and prioritizing it in the future. However, there is still plenty of work to be done to mitigate data protection risks.





The intersection of digital transformation and data privacy will be critical for middle market organizations as they continue to expand their digital capabilities. How can they mitigate privacy risks while implementing their digital strategies? We've identified five key takeaways for C-suite executives to consider.

1. HANDLE INNOVATION WITH CARE—CAUTION IS KEY

When leveraging the latest technology solutions or implementing new processes for your organization, you must also remain compliant with an expanding web of data privacy regulations. Innovation must be balanced with conscientious business practices.

In a climate of intense public scrutiny around data privacy, business leaders face unprecedented pressure to demonstrate responsible data stewardship. With companies awash in an ever-expanding sea of data, implementing a data privacy program is crucial to staying afloat.

A key element of innovation with intent is to incorporate "Privacy By Design"—a concept that prioritizes consumer privacy in the systems that collect and store personal data—at the outset of all new digital initiatives. An effective privacy program requires a clearly articulated vision and mission for internal and external distribution. Business leaders who take the "how would I feel?" approach to their privacy initiatives are more likely to provide consumers with reasonable expectations of how their data will be used, processed and shared.

2. FROM ROADBLOCK TO ROADMAP—ENABLING SECURE INNOVATION

Thirty-one percent of survey respondents cited concerns about cybersecurity as the biggest challenge in moving forward with a new digital initiative. Retail, tech and manufacturing companies were particularly concerned about cybersecurity threats, weighing in at 34%, 35% and 39%, respectively. And that's no surprise—while emerging technologies streamline and optimize processes, they also expose businesses to significant privacy risks.

That doesn't mean data privacy concerns must halt innovation. Digital resilience is the key to overcoming these challenges. Investing in proactive threat intelligence, detection and rapid response, in addition to implementing administrative, technical and operational controls, can keep your business safe while pursuing your digital initiatives. At the same time, business leaders need to ensure that data protection measures don't become too cumbersome and impact usability. Data protection measures should not be redundant or overly complex—they should be user-friendly and designed to facilitate safe and secure innovation. The key lies in Privacy By Design—weaving Privacy By Design into digital initiatives enables secure, agile, and impactful solutions.

Learn more about CCPA and whether it applies to your organization ▶

3. CCPA IS ONLY THE BEGINNING—KEEP YOUR EYE OUT FOR MORE LEGISLATION ON THE HORIZON

From the new California Consumer Privacy Act (CCPA) that went into effect in January 2020 to the European Union's two-year-old General Data Protection Regulation (GDPR), more and more companies must comply with privacy regulations or risk the consequences, which could include losing the trust of investors and the public. As of 2020, all 50 states have some type of data privacy law, from basic data privacy notification obligations to more rigorous data protection and monitoring obligations for companies. This is just the beginning—more regulation is coming as both legislators and the public better understand the persistent nature of threats to personal data.

COVID-19 has played a critical role in public awareness of threats to privacy. Along with the increase of cyberattacks carried out during the crisis, contact-tracing technology has become a hot-button issue in efforts to track the spread of the virus. Contact-tracing apps are distinct from other apps in that they track and collect health information. They monitor individuals that exhibit symptoms or contract the virus, and while this may not violate the Health Insurance Portability and Accountability Act (HIPAA), this is still sensitive data and its collection brings a host of pressing questions regarding data privacy. As the use of contact-tracing technologies becomes more widespread, concerns regarding the security of these apps will continue to rise and bring data privacy to the forefront of consumers' minds.

The variety of data privacy legislation brings unique challenges to data governance and management. Companies must be aware of which regulations apply to them, then design compliance processes according to the company's risk profile. Implementing these processes is not easy or simple. According to BDO's Technology CFO Outlook Survey, CFOs see data privacy as a triple threat: as the top regulatory concern, business risk and main priority.

In general, C-suite executives are focused on data privacy regulation compliance as well. BDO's **2020 Digital Transformation Survey** found that 95% of respondents have either already begun providing training for employees in data privacy or planned to in the next 12 months. Respondents are also planning on or, already in the process of, revising privacy policies and processes (89%), updating privacy disclosures (87%), automating compliance processes (91%), performing readiness assessments (84%), performing data mapping exercises (86%) and reviewing third-party agreements (86%).

Benchmarking / Data Privacy Compliance

	All Respondents		Lower Middle Market		Upper Middle Market	
	Currently	Next 12 Months	Currently	Next 12 Months	Currently	Next 12 Months
Providing Training for Employees	55%	40%	53%	38%	57%	41%
	95%		**91%**		**98%**	
Revising Privacy Policies and Processes	53%	36%	55%	36%	52%	35%
	89%		**91%**		**87%**	
Updating Privacy Disclosures	52%	35%	58%	34%	48%	36%
	87%		**92%**		**84%**	
Performing a Readiness Assessment	49%	35%	54%	30%	46%	30%
	84%		**84%**		**76%**	
Automating Compliance Processes	48%	43%	46%	44%	49%	42%
	91%		**90%**		**91%**	
Performing a Data Mapping Exercise	47%	39%	51%	35%	44%	41%
	86%		**86%**		**85%**	
Reviewing Third-Party Agreements	46%	40%	40%	44%	50%	37%
	86%		**84%**		**87%**	

The cumulative nature of data privacy regulations means that executives can't simply check the box once solutions are implemented—governance of data privacy is an ongoing process that requires continual engagement and revision based on a commitment to safeguarding sensitive data the organization collects, processes, transfers and stores.

4. UNDERSTANDING DATA ETHICS—THE FOUNDATION OF GOOD DATA PRIVACY

Data ethics is the guiding force that to helps navigate the minefield of potential data privacy missteps. Data ethics enables businesses to go beyond compliance when planning and executing projects. A mature data ethics framework will include several requirements on data project management, including: clearly defining the project and it's benefits, developing a transparent program that keeps a company accountable, using data that is compatible with the project, and understanding the limits of the data.

Unfortunately, many companies have not sufficiently developed their data ethics practices. The **2020 Digital Transformation Survey** shows that 30% of middle market organizations have no formal data ethics program or policy in place. In particular, healthcare (37%) and manufacturing (34%) companies were less likely to have such programs or policies in place compared to other industries.

Integrating a data ethics program into your digital transformation strategy helps minimize the risks of collecting consumer data and builds trust with consumers and investors alike. Companies that prioritize the protection of their customers' data can gain market share on trust alone. Data ethics can also guide business leaders through the appropriate management and use of data even before starting a new project, introducing a new process or releasing a new technology.

5. DATA PRIVACY MANAGED SERVICES—BRINGING YOUR ORGANIZATION UP TO SPEED

Understanding compliance with data privacy regulations can seem like an insurmountable task. Combined with constructing a data ethics program and spearheading digital transformation initiatives, companies can understandably become overwhelmed. As a result, many organizations are turning to outsourced solutions to help manage their data privacy programs and help them ensure they're complying with all applicable regulations. In the **2020 Digital Transformation Survey**, 34% of respondents say they are using outsourcing to ensure employee adoption of technology advances.

Leveraging a managed services provider to build a robust data privacy program has many benefits. These services can focus on immediate privacy concerns while maintaining operational readiness, helping your organization understand your compliance obligations and helping manage risk. These services can include data flow diagramming, Privacy Impact Assessments (PIA) privacy maturity assessments, privacy training and awareness,, privacy strategy and framework development, and more. Contracting a third party to manage your data privacy program can be cost-effective in the long run by reducing redundancy in your operations, ensuring compliance and helping you win consumer trust.

Data privacy is only growing in importance as the COVID-19 situation continues to evolve and breaches to personal data become common place.. Even in a post-pandemic world, the implications of data privacy will spur new regulations and heighten consumer concerns. Missteps can have grave consequences—C-suite executives need to make addressing data privacy a top priority for their business.

BDO Digital's Data Protection Managed Services offer a proven, scalable approach to data protection for middle market organizations and delivers enterprise risk management, data privacy, governance and digital enablement. These services include:

Personal Information (PI) inventory and processing registers

Individual rights response management

On-call privacy operations

Outsourced privacy management

Outsourced Data Protection Officer (DPO)

Learn more about how BDO can address your organization's data privacy needs and help accelerate your business transformation ▶

CONTACTS:

KAREN SCHULER
Principal
Governance, Risk & Compliance Leader
301-354-2581 / kschuler@bdo.com

MARK ANTALIK
Managing Director
Information Governance and Privacy Leader
617-378-3653 / mantalik@bdo.com