Harvard Business Review
ANALYTIC SERVICES

Pulse Survey

DIGITAL DILEMMA

Turning Data Security and Privacy Concerns Into Opportunities

Sponsored by

Cognizant

Customer Data Protection: Burden or Competitive Advantage?

SCOTT SCHLESINGER
CHIEF ANALYTICS OFFICER
COGNIZANT DIGITAL BUSINESS

We reveal personal information with every click, social media post, online check-in—possibly even when we start the car or apply the brakes. For merchants and service providers, customer data is a valuable asset for product planning and personalized marketing. Some companies also monetize customer data by selling it to third parties.

As consumers, however, we worry about data privacy. Our personal information is scattered around in databases, emails, documents, and web chat transcripts. We fear identity theft. We're annoyed when we open our mail and realize that our personal information has been sold without our permission. We wonder which merchants we can trust to look out for our privacy.

What's the optimum balance between monetizing customer data and protecting privacy? To find out, we asked Harvard Business Review Analytic Services to survey companies around the world about the importance of data privacy in their business. In the next one to three years, 95% of the survey respondents will adopt big data analytics, 87% will implement data-driven marketing, and 65% will sell or purchase customer records.

An organization's approach to data protection depends on the relative value it assigns to short-term profits versus customer goodwill and loyalty. A company focused on short-term profits may be tempted to extract as much personal data as customers will tolerate, sell the data, and take the minimum precautions to comply with data privacy regulations such as the EU's General Data Protection Regulation (GDPR). The downside is increased risk exposure. A patchwork of point solutions leaves the company vulnerable to breaches—potentially leading to fines, reputational damage, costly redevelopment efforts, and a battered share price. What's more, customers who perceive a cavalier attitude about privacy feel justified in defecting to a competitor.

Companies that place a priority on goodwill, in contrast, view data privacy as a competitive advantage. They aim to collect enough data to engage customers—but not enough to alienate them. They clearly convey their commitment to privacy and back it up with technology, processes, and employee education. The obvious reward for investing in privacy is stronger protection against cyber attacks. But companies in this camp also gain a competitive advantage. Customers who trust your company to not sell or misuse their data are more likely to remain loyal. They also may be willing to share more data, giving you an edge for new product development and marketing.

What does a comprehensive data-protection strategy look like? No two organizations' strategies are identical, and the approach that each one takes (personnel, processes, and technology) will evolve over time. That said, survey respondents highlighted the following elements: identifying potential threats; strengthening compliance; integrating data privacy into core systems; developing standard procedures for gathering, identifying, classifying, and discarding customer data; and employee training. Phishing, for example, is a big problem.

In summary, organizations stand to gain a competitive advantage by viewing regulations like GDPR as an opportunity rather than a burden. Protecting customers' personal data helps to build trust and loyalty, ultimately increasing market share and wallet share.

DIGITAL DILEMMA

Turning Data Security and Privacy Concerns Into Opportunities

INTRODUCTION

The data economy is evolving rapidly in new directions as artificial intelligence, big-data analytics, and data-driven business and supply chain management become embedded in countless new products and services. With a more data-centric economy, consumer confidence in companies' ability to protect personal data becomes paramount. The digital future, as a result, will be defined not just by disruption, innovation, and product breakthroughs, but also by consumer awareness, legislation, regulation, and commercial adaptation.

Data today, however personal, is an asset; how it is used, or abused, will be critical to the success of the digital economy. One has to think only of the 2017 breach at Equifax, which exposed 143 million Americans' Social Security numbers, credit card information, and other personal data, or the 2015 hack of Talk Talk that affected almost 157,000 customers of the telecom company—resulting in a record £400,000 fine; the halving of the company's stock price; and the loss of 101,000 customers, £60 million in revenue, and the CEO's job. Companies that collect and benefit from the vast stream of client data therefore must adapt to an environment defined by government-mandated consumer protections nearly as much as by economic opportunity—or pay the cost of failing to do so.

Consumer confidence is a priority for the EU, which valued its data economy at €272 billion in 2015, with annual growth of 5.6%, and projects that it could employ as many as 7.4 million people by 2020.[1] The EU's new General Data Protection Regulation (GDPR) includes stringent data privacy rules and imposes sanctions for noncompliance. Any company doing business in the EU will be subject to GDPR, marking its implementation date of May 25, 2018, as a pivot point in the development of global data security and privacy regulation. Most organizations expect to experience at least some impact from the new regulation. FIGURE 1

GDPR compliance "is about telegraphing to customers, prospects, and employees that you take data privacy seriously," says Ardi Kolah, executive fellow and codirector of Henley Business School's GDPR Transition Programme, and editor-in-chief of the *Journal of Data Protection and Privacy.*

HIGHLIGHTS

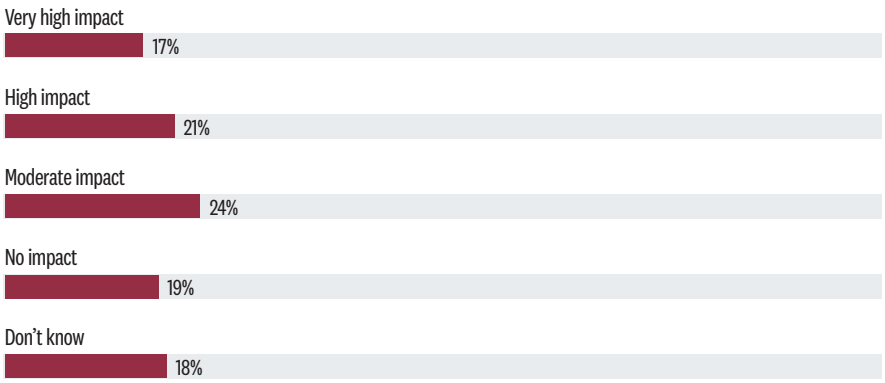
42%
OF RESPONDENTS EXPECT RULE CHANGES TO AFFECT THEM SIGNIFICANTLY OR VERY SIGNIFICANTLY OVER THE NEXT ONE TO THREE YEARS

85%
EXPECT TO BE AFFECTED AT LEAST MODERATELY

FIGURE 1

ANTICIPATED IMPACT FROM GDPR

What impact does your organization expect from the EU's General Data Protection Regulation (GDPR)?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

Perhaps most important, the GDPR is part of a matrix of EU data initiatives geared to remove restrictions on the free flow of data within the economic union and eliminate uncertainties created by the patchwork of legal regimes among European states. The EU's Digital Single Market Strategy includes eliminating data localization requirements, for example, and sponsoring projects such as connecting motor vehicles with each other and with roadside services to make travel more efficient. Meanwhile, industry-centric working parties are being encouraged to meet and agree on standards and policies.

Organizations that focus too narrowly on the task of compliance therefore miss the larger picture of the digital future now approaching, and the opportunities that come with it. The heightened profile of data security and privacy is creating a new world where data privacy features will have to be embedded in every product and service and where they can even create new needs that companies can then meet with new offerings, resulting in new competitive advantages for companies that approach this new world effectively.

Making Data Privacy a Priority

"Your relationship with your customer is only as strong as the weakest link in the chain," says Joanne Bennett, vice president and associate general counsel, commercial and global compliance at Hitachi Consulting.

How are companies changing their processes, practices, and even their business model to meet this reality? To find out, Harvard Business Review Analytic Services surveyed 331 organizations and conducted a series of one-on-one interviews with executives and thought leaders around the world and in a wide variety of industries about their data security and privacy perspectives. They were asked about the impact they expect from new rules and regulations and rising client and consumer demand for data privacy in coming years, and the opportunities that the new world of heightened data security concern may offer. (See methodology, page 16.)

The survey revealed widespread agreement that data will be critically important in the years ahead. Large majorities said that artificial intelligence (72%), big data/data analytics (95%), sales and purchase of client and customer records (65%), and data-driven marketing and customer tracking (87%) will be important or very important to their business in the next one to three years. FIGURE 2

Furthermore, most respondents expect new data privacy laws, regulations, and directives to have at least some impact on their role. Almost half (42%) expect rule changes to affect them significantly or very significantly over the next one to three years, and 85% expect to be affected at least moderately.

Client/customer concerns about data privacy and security are central to the heightened attention that organizations are devoting to data security and privacy, the survey found. "Our company's key strategic focus is based on providing products and services for the growth of data in a connected world," said one respondent. "Data privacy and excellence in managing data are critical to that strategy."

Respondents said their clients are increasingly concerned about how well the security and privacy of their data is maintained (90% agree or strongly agree). Clients are increasingly concerned about having access to their data when and how they want it (81%), whether it is being shared with or sold to other organizations (81%), and whether it is deleted when it is no longer needed (66%). FIGURE 3

Beyond legal and regulatory concerns, organizations are propelled by the risk to their reputation, not to mention the resulting costs, from data attacks and breaches. "The concern is data- and use-specific," says Viktor Mayer-Schönberger, professor of internet governance and regulation at Oxford University. "It's no problem if one's health data is used in health research to come up with a diagnosis, but if it's given to an insurance company, say, that's another thing."

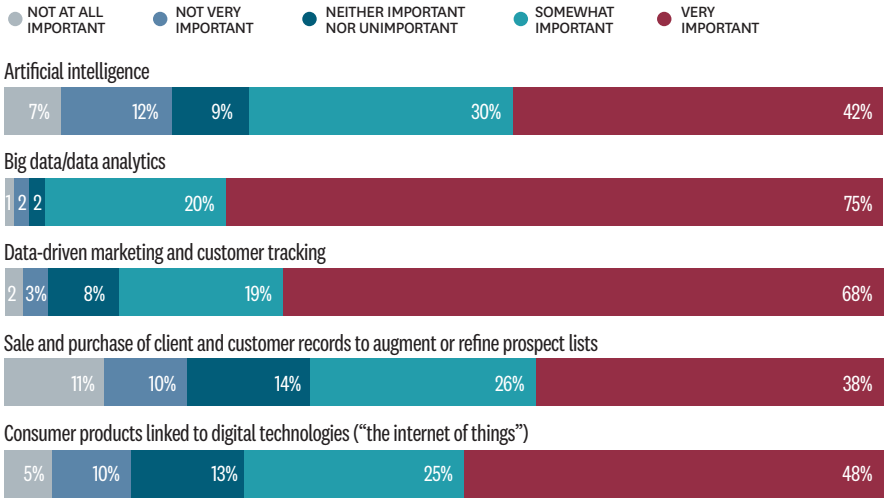
Boards, accordingly, are not focused only on fines, Bennett says. They are also concerned about the impact that highly publicized failures could have on their reputation with clients, the cost of mitigating and cleaning up after a major breach, and the potential impact, in the case of public companies, on their share price. "It's better to have the right measures in place and to think it through so it doesn't happen again," she says.

Accordingly, 81% of respondents agreed that their organization is making data privacy and security a high priority. This includes ensuring that all functional and business units in contact with or in control of client data are applying the organization's data privacy policy (82%), devoting adequate budget and resources to maintaining privacy procedures (73%), and taking a role in crafting industry-wide or government-enforced standards for client and customer data collection (61%).

FIGURE 2

GAME CHANGERS

How important will these data-driven technologies and applications be to your organization's business plan over the next one to three years?

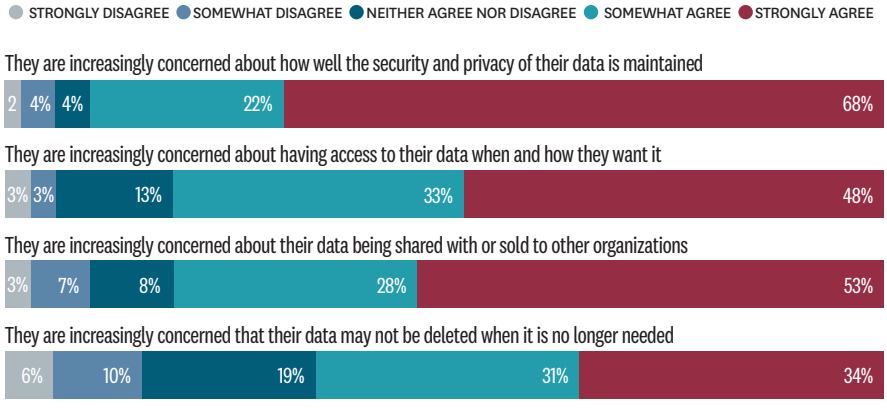


SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

FIGURE 3

CLIENT CONCERNS

How strongly do you agree or disagree with the following statements about your organization's clients and customers?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

Respondents with a variety of profiles agreed on these points: For those at larger organizations with 10,000 or more employees and at smaller ones, regional and national as well as multinational organizations, C-suite level and below, the results were largely the same.

GDPR is a strong motivator for many if not most. "GDPR will affect all our global databases," said one respondent. "Compliance there is a requirement and should be used globally as a template."

A little more than half of respondents (58%) said their organization had made GDPR preparation a high or very high priority. More than one-third (38%) expect their organization to experience a high or very high impact from the regulation, and 63% anticipate at least a moderate impact. More than half (57%) are implementing an organization-wide compliance plan.

Most are moving slowly, however, despite the fact that the implementation date for GDPR is barely half a year away. Only 30% are communicating regularly with employees at all levels about the new regulation, although 55% say they are planning to do so. Only 23% are communicating regularly with clients/customers, with 55% planning to do so. And while more than two out of five (41%) are working with regulators to clarify aspects of the rule, only 30% more are planning to do so—and 14% have no such plans. FIGURE 4

Size accounts for some of these differences. While large and small organizations are comparable in giving GDPR preparation high or very high priority (61% vs. 53%), larger organizations are more likely to expect a high or very high impact from GDPR (40% vs. 24%). This suggests why larger organizations are more likely to be currently taking steps to implement an organization-wide compliance plan (61% vs. 33%) and communicating regularly with employees at all levels about the new rules (34% vs. zero), although respondents at smaller organizations say they are planning to catch up.

Seizing the Competitive Advantage

Regulation, done right, can create advantages.

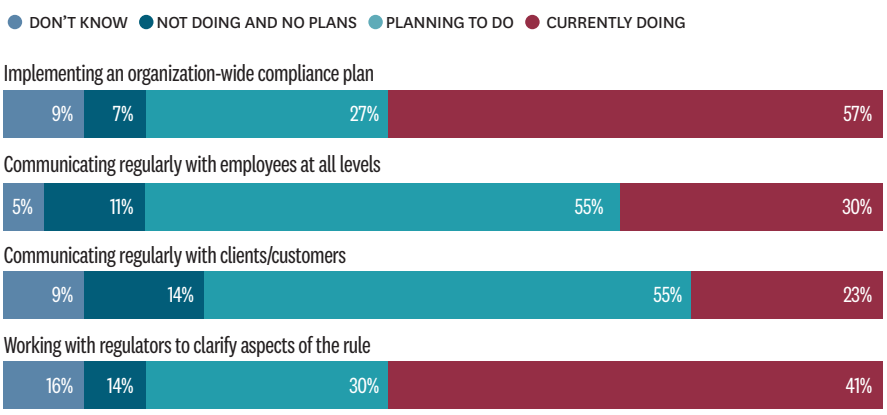
"The big challenge for a global organization like ours," said one respondent, "is that we have to comply with a disjointed set of regulatory frameworks where each country has its own say and their regulations are in some cases at odds with each other. That makes any global company's work more complex."

But while data privacy standards will be tighter, initiatives like the GDPR will help data to flow more freely, with fewer variations across markets and jurisdictions. Companies' risk management processes will improve as the regulatory road map becomes clearer and they acquire greater control of their own data. And adeptness at privacy and security will itself become a significant competitive advantage and even a source of new business for companies that can integrate it into their culture and processes.

FIGURE 4

PREPARING FOR GDPR

Which of the following initiatives has your organization undertaken in advance of GDPR's implementation?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

While **data privacy standards** will be tighter, initiatives like the GDPR will help data to flow more freely, **with fewer variations** across markets and jurisdictions.

The more ways that data can be repurposed for more differentiated products and services, the more valuable it becomes—and the more integral data privacy features will be to its value. "Companies need to make arrangements with the individual that assure them their data is not being misused," says Mayer-Schönberger. "These arrangements enable the reuse of that data."

Survey respondents said new data privacy laws, regulations, and directives afford their organization some or significant competitive advantage by:

- Facilitating freer flow of data across borders (e.g., in the EU) by eliminating multijurisdictional regulatory uncertainties (some or significant advantage, 60%),
- Creating greater confidence in all companies that receive and control client and customer data (65%),
- Instituting certification processes and providing a third-party credential of the strength of the organization's data privacy policy and processes (63%),
- Making optimization of the organization's data-handling practices easier (60%),
- Enabling the organization to develop data-driven marketing strategies and products (e.g., connecting motor vehicles with each other) with confidence by clarifying the guidelines around them (61%), and
- Leveling the playing field between the organization and its competitors (49%).

Certification and credentialing are especially important, says Bennett, because they assure suppliers that the products they sell and the work done by their third-party providers meet a specific data privacy standard. "If you have two providers," she says, "both using the tools and services of a third-party provider, and one is validated by independent accreditors while the other isn't, most people would lean toward the party that has the accreditations."

Established companies will also benefit from the assurance that their competitors are following the rules. "New regulation will in fact help our organization," said a respondent, "as it will regulate most of the new, smaller companies that sometimes choose to cut the corners to get the extra edge."

Establishing a uniform standard for data privacy and security fits into the framework of facilitating free flow of data because it gives consumers greater certainty that their data is secure across borders and greater confidence in their commercial counterparts. GDPR creates a "data protection seal" notifying consumers that a firm complies with the supervisory authority and can transfer data to third parties lawfully—a designation that could become a significant competitive advantage for organizations that earn it. (Larger European economies like Germany, France, and the UK already include some of GDPR's provisions in their own laws.)

These changes could have a dramatic economic effect. Removing localization restrictions could generate up to an additional €8 billion in GDP a year, it is estimated.[2]

78%

SEE A STRONG DATA PRIVACY STRUCTURE AS HELPING TO ENHANCE AND DIFFERENTIATE THEIR BRAND

"There's a good business opportunity if you can demonstrate that you can manage data privacy very transparently and accountably. Then, your customers are likely to share more personal data with you," says Kolah.

Most respondents see a strong data privacy structure as helping to enhance and differentiate their brand, with 78% citing some or a significant advantage. Current clients will be more forgiving of a data breach if the organization has a strong data privacy structure and as long as the breach is quickly addressed (58%), and strong data privacy enables their organization to implement efficiencies that lower costs (68%). Potential clients and customers will be more likely to choose the organization's services or products (72%). FIGURE 5

Over half of respondents (56%) said that potential clients and customers might be more likely to pay a premium for their organization's services or products as well. As one respondent noted, "We don't sell privacy as a premium, but it still does bring you to contract."

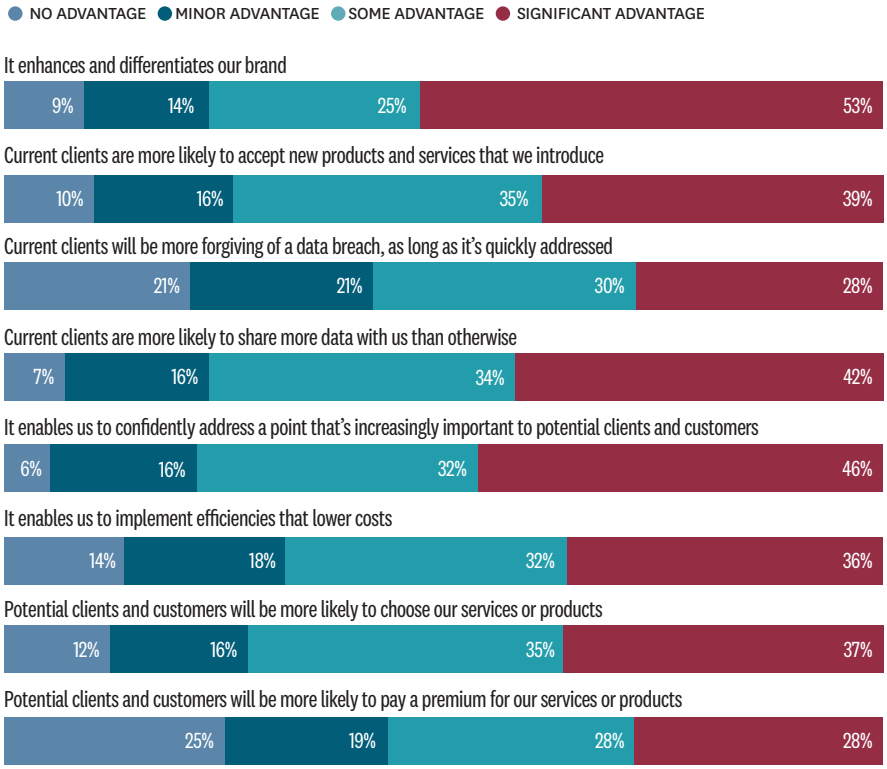
Larger organizations are somewhat more likely than smaller ones to see strong data privacy as generating a competitive advantage for them—for example, by enhancing their brand (54% vs. 46%). The same is true for multinationals as opposed to companies with a national focus (58% vs. 47%). Larger organizations are also more likely to anticipate that strong data privacy will encourage current clients to share more data with them (43% vs. 35%). Multinational organizations are more likely than nationally focused ones to feel the same (45% vs. 35%).

Perhaps most significant for companies in the future digital economy, a stronger data privacy structure can open up opportunities to create new product offerings. Current clients are more likely to accept new products and services (74%), respondents said. Current clients are more likely to share more data with the organization than otherwise (76%), which can enable it to generate new products and services. Over half of respondents (54%) said a strong data privacy structure can facilitate innovation by embedding data privacy

FIGURE 5

BENEFITS OF A STRONG DATA PRIVACY STRUCTURE

What are the future benefits and advantages for your organization of a strong data privacy policy?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

A STRONGER DATA PRIVACY STRUCTURE CAN OPEN UP OPPORTUNITIES TO CREATE NEW PRODUCT OFFERINGS.

DATA PRIVACY AND SECURITY CAN NO LONGER BE SIMPLY THE JOB OF IT OR THE CIO.

features in new products and services, and 60% agreed that it enables the organization to offer expanded analytic capabilities to clients, built on their personal data.

"Regulations on consumer protection will drive innovation on anonymized insight collection rather than raw data collection," said one respondent from a leading technology company, "which our company thrives on. It is an opportunity for us to differentiate and enhance the brand."

Controlling Data and Serving Clients

Positioning themselves to take advantage of the opportunities created by the new digital economy and its focus on data privacy places a new set of demands on organizations. "The way to do it is to push it deep into the structure of the company, into the product units where the repurposing of data is actually being discussed and so where sensitivity needs developing," says Mayer-Schönberger.

Larger organizations may be more inclined to go deep, the survey indicates. While it found that organizations of all sizes are making data privacy and security a high priority, respondents from large organizations were far more likely than those from smaller ones to strongly agree that their employer ensures that all functional and business units in contact with or in control of client data are applying the organization's data privacy policies and procedures (51% vs. 33%).

All companies, however, will need to develop clear internal processes and networks of control and responsibility extending throughout the organization; data privacy and security can no longer be simply the job of IT or the CIO. Most companies are not their own data systems designers, and so will have to renegotiate contracts with their technology partners. New business models, new product groups, and new audiences will have to integrate data privacy provisions from the outset. The stakes are high: Breaches of the GDPR rules could trigger fines of up to 4% of a company's global turnover or €20 million, whichever is higher.

"Regs will drive increased investment in data management and systems," said one survey respondent, suggesting that data management and systems will increasingly reflect regulatory demands for enhanced data privacy. Failing to keep privacy policies and procedures up to date with new laws, regulations, and directives emerged as one of the top five obstacles to client and customer data privacy in coming years, cited by almost one-third (31%) of respondents.

The good news is that most organizations understand the need to prioritize adherence to data security and privacy rules. Almost three-quarters (73%) now include top management in all aspects of privacy policy development, and nine out of 10 respondents either strongly or very strongly agreed that their organization keeps current with all pertinent laws and regulations.

Keeping up with evolving digital rule-making is not enough, however; "data security must be embraced by the organization as a whole, so that everything's transparent and everyone's accountable," says Kolah. "You can create amazing policies," says Bennett, "but if you don't embed them within the business, making it real, then you can wind up with policies-in-a-drawer that are next to useless. That's something that will catch a lot of organizations out" as they prepare for GDPR implementation.

Seventy percent of respondents said their employer is making data privacy policies and procedures clearer and more easily understandable for employees, while 71% are creating programs, tailored to the organization, to educate employees about its data privacy policies. Almost three-quarters

(73%) said they are establishing an organization-wide strategy for responding to breaches. FIGURE 6

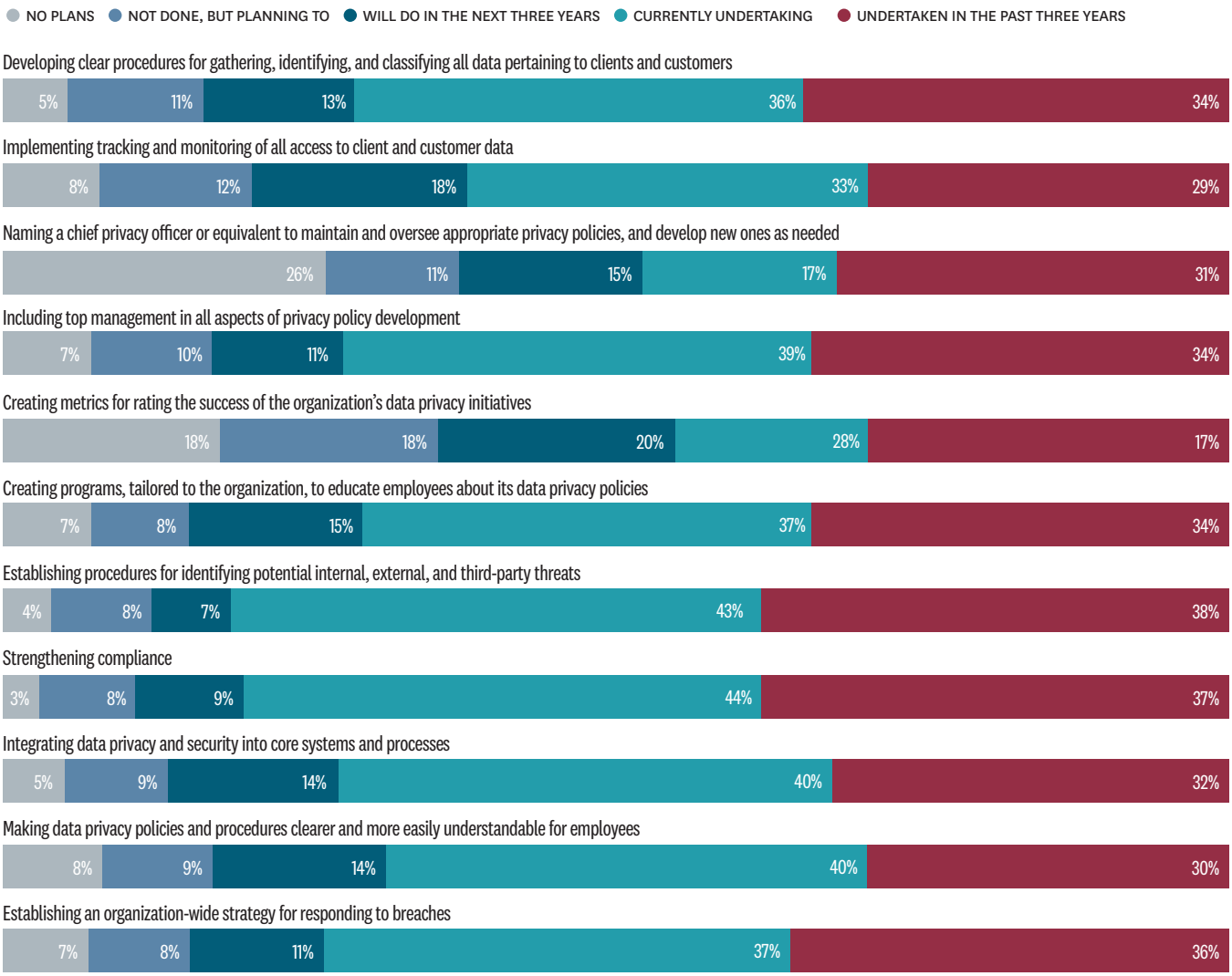
From a corporate perspective, the new-era imperative will be to achieve greater control and awareness of the data the company holds: how it is categorized, where it is located, and what obligations are attached to it. Organizations are challenged both to improve their systems' data privacy and security and to convince clients that, in this respect, they can have confidence in products and services the organization offers.

Most have undertaken at least some initiatives in these areas, because, as the response to numerous recent data breaches and internal bungles demonstrates, consumers and shareholders are becoming less and less tolerant of failure. Measures include developing clear procedures for gathering, identifying, and

FIGURE 6

STRENGTHENING CONTROL OF CLIENT DATA

What initiatives has your organization undertaken to gain better control of client data and ensure data privacy?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

COMPANIES WILL NEED TO KEEP TRACK OF NOT ONLY THE DATA THEY HOLD, BUT ALSO OF HOW AND WHEN THEY GET RID OF IT.

classifying all data pertaining to clients and customers (70%); establishing procedures for identifying potential internal, external, and third-party threats (81%); strengthening compliance (81%); and integrating data privacy and security into core systems and processes (72%).

Preparing for the digital future can also be a catalyst for companies to adopt more sophisticated customer data management techniques. This supports efforts to take a risk-based approach to storing information appropriately. Sixty-two percent of respondents said their organization is building more robust, up-to-date client data management systems, and 62% said it is implementing tracking and monitoring of all access to client and customer data.

Most said their organization is also taking specific steps to reinforce client confidence, including:

- Providing greater control for clients and customers over what data can and cannot be shared (e.g., an opt-in consent requirement, 59%),
- Clarifying data privacy policies and procedures for clients (70%),
- Informing clients and customers how personal data will be used each time it's requested (59%), and
- Establishing clear procedures giving clients and customers access to their data when and how they want it (60%).

Opt-in and informing clients each time their data is used could be especially important for solidifying client trust, says Mayer-Schönberger—far more so than the current practice whereby companies give them a blanket informed-consent agreement to sign at the commencement of the relationship.

Companies will need to keep track of not only the data they hold, but also of how and when they get rid of it—and to ensure they do not contact someone who expressly says they don't want to be contacted. Yet this too underscores the opportunities that accompany the new digital economy, since organizations that can perform such tasks more efficiently and accurately will have a competitive advantage. More than half (55%) of respondents said their organization is establishing clear procedures for disposing of excess or unneeded data, and communicating those procedures clearly to clients and customers.

As this suggests, the basic challenge—how to enhance existing products and create new, tailored offerings using deep analysis of customer data, without being too intrusive—is as much about reputation as it is about regulation and law. This is encapsulated by a respondent at a large law firm: "We are already collecting a significant amount of other people's sensitive data, and the reputational stakes are especially high for our brand if we don't follow best practices and meet regulatory requirements."

To learn how close organizations are to achieving this balance, the survey asked respondents to what extent their organization is meeting the principal tenets of GDPR—which, says Kolah, "are really just a codification of best practices in data privacy." Most, the answers reveal, are on the road to doing so, even if the majority are not there yet. FIGURE 7

- Almost one in five (19%) respondents said clients/customers can request that their data be passed to another processor, and 39% said their organization is planning to add this option.
- Almost one-third (29%) said clients/customers can require that data be deleted when no longer needed (the "right to be forgotten"), and 37% plan to make this possible.

59%

SAY THEIR ORGANIZATION IS PROVIDING GREATER CONTROL FOR CLIENTS AND CUSTOMERS OVER WHAT DATA CAN AND CANNOT BE SHARED (E.G., AN OPT-OUT REQUIREMENT).

More than **one in four** respondents (27%) said clients/customers are **notified of any data breach** within 72 hours.

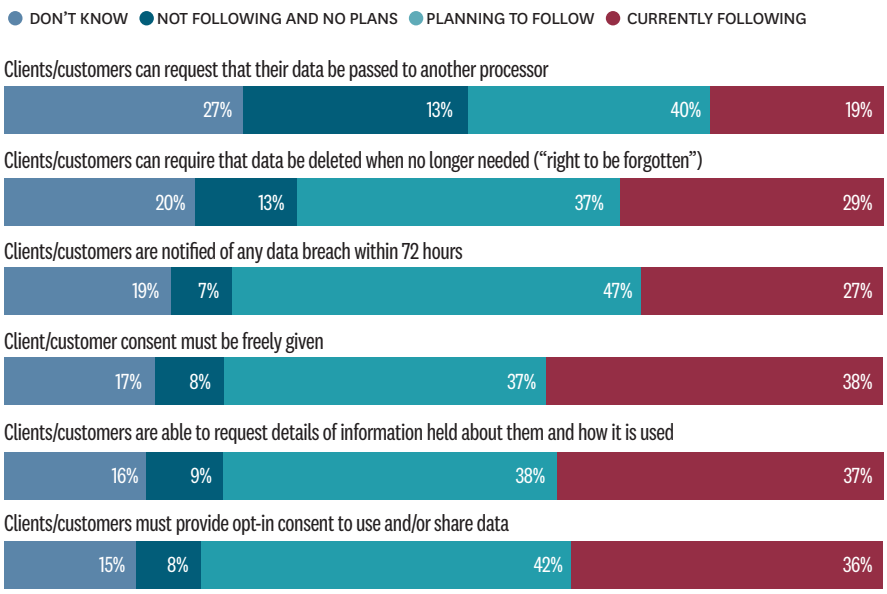
- More than one in four (27%) said clients/customers are notified of any data breach within 72 hours, and 47% said their organization is planning to implement this standard.
- More than one-third (37%) said clients/customers are able to request details of information held on them and how it is used and another 38% said their organization is planning to make this an option.
- More than one-third (38%) said client/customer consent must be freely given to pass on data, while 37% said they will implement this rule.
- More than one-third (36%) said clients/customers must provide opt-in consent to use and/or share data, and 42% said they plan to enforce this.

Strong data protection is a critical enabler for digital commerce and enhanced service offerings, because it ensures consumers can trust data vendors and makes them more likely to trust companies they regard as providing the best protections. Not all organizations understand this in the same way or to the same degree, however. "A lot of financial services companies are probably

FIGURE 7

BEST PRACTICES IN DATA PRIVACY

Which of the following principal tenets of GDPR does your organization follow?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

close to meeting the [GDPR] standard already," says Kolah. "If you're a flower shop, you're processing personal data, but nothing like a bank. So the technological measures you need to put in place are different."

Most companies appear to be taking some steps to earn client confidence, however. "We're taking proactive measures by putting our clients' priorities first," said one respondent. "The new data privacy laws, regulations, and directives will have some profound effects—but we will adjust as appropriate."

Progress Is Not Perfection

Progress doesn't mean perfection, however. Even in areas where most organizations have established or are establishing processes to improve data privacy and increase client confidence, they may not be doing enough, the survey indicates.

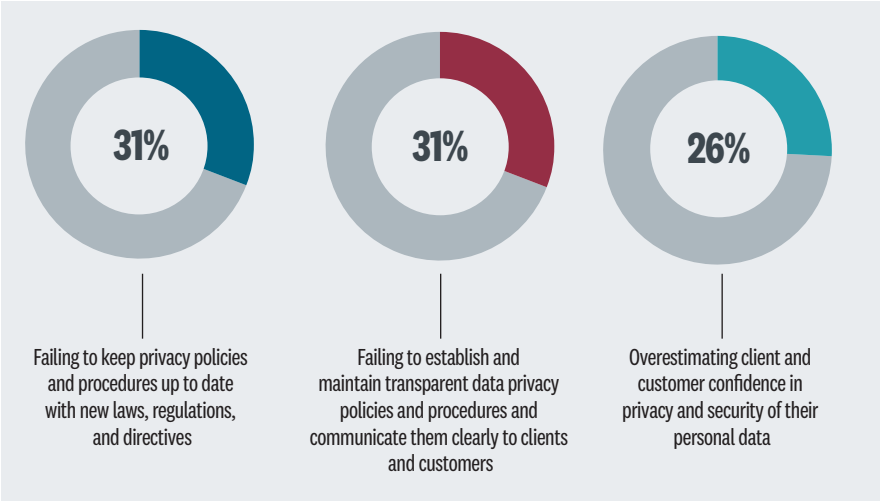
Some concerns relate to the company's grasp of customers' perspective and its efforts to communicate with them. More than one-quarter (26%) of respondents cited overestimating client and customer confidence in the privacy and security of their personal data as one of the greatest obstacles they face to strengthening client and customer data privacy, while 31% named failure to establish and maintain transparent data privacy policies and procedures and communicate them clearly to clients and customers. FIGURE 8

Other concerns focus on resources, controls, and the difficulty of keeping the organization technologically current. Nearly half of respondents mentioned failure to adopt new and preferred technologies to keep privacy policies and procedures up to date (47%) and failure to provide an adequate budget and resources (46%). Nearly as many (41%) cited overdependence on specific functions (e.g., chief privacy officer, CIO, IT, risk management, legal, compliance) to ensure data privacy policies are up to date and observed. "That means data privacy is seen as a cost unit," says Mayer-Schönberger. "The chief privacy officer's job is to achieve regulatory compliance at the lowest possible cost, when the risks to personal data are in the deeper processes of the product or service."

FIGURE 8

OBSTACLES

What are the greatest obstacles your organization faces to strengthening client and customer data privacy?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

Location was no differentiator here: Organizations with a local or single-country focus placed a very similar stress on these pitfalls, as did global and multinational organizations.

One respondent complained of "decentralized and multiple data sources that are not consistently and centrally governed." Another, at a global, multi-industry company, noted that it has failed to create "simple but clear policies that cover all the different industry and national requirements and then ensure good understanding of and adherence to those policies."

Some initiatives that are widely seen as contributing to a more robust data privacy structure are still far from the norm at organizations we surveyed. Less than half (45%) of respondents said their organization has created metrics for rating the success of their data privacy initiatives, and almost one in five (18%) said they have no plans to do so. Less than half (48%) said their organization has named a chief privacy

TO BEST SERVE CUSTOMERS' DATA PRIVACY NEEDS, COMPANIES NEED TO EMPHASIZE EMPLOYEE TRAINING AND AWARENESS.

officer, or equivalent, to maintain and oversee appropriate privacy policies and develop new ones as needed, and more than one in four (26%) said they have no plans to do so.

To best serve customers' data privacy needs, companies need to emphasize employee training and awareness. "Our biggest opportunity is to use data to inform our content (resources, tools, communications, etc.)," said one respondent, "but we could face major issues if we don't improve the average employee's knowledge about data privacy. Phishing is a big problem for us currently and our employees are struggling to remember or put to use their training and our policies."

Some challenges are less subject to organizations' control. While individual governments and supra-national bodies are working to make the rules more uniform across borders through measures like GDPR, increased regulation arising from heightened attention to data privacy and security is expected to create further challenges. Substantial percentages of respondents said that new data privacy laws, regulations, and directives will impose significant or very significant burdens on their organization, including:

- Adding potential liabilities when unclear or ill-defined rules are invoked (52%),
- Requiring new expenses and permanently adding to the resources the organization is required to carry (49%),
- Adding complexity to supplier and third-party relationships (e.g., requiring renegotiation of contracts with outside vendors and technology partners, 49%),
- Making it more challenging to create tailored products without violating privacy rules (40%),
- Disrupting existing business models and networks of responsibility (34%), and
- Disrupting client/customer relationships (27%).

"New laws and regulations could potentially slow innovation, as we would need to adjust to the shifting landscape," said one respondent. FIGURE 9

Conclusion

The era of digital innovation that began a decade and a half ago was typified by a new focus on enhancing the customer experience—through products like the tablet, the smartphone, and digital wearables. Increasingly, this has meant gathering and analyzing a greater and greater volume of customer data. "The value of companies is very much assessed by their ability to exploit intellectual property, including personal data," says Kolah.

As data privacy concerns multiply, the objective in the digital future will remain the same, but embedding data privacy protections into organizations' processes—making them fundamental to how companies do business, not an afterthought or a crisis response—will become the means. Doing so creates the opportunity to develop new products, services, and features that consumers value, and makes the company itself more competitive.

Some survey findings indicate that larger organizations are farther advanced than smaller ones at making the changes needed to enjoy a competitive advantage from better data privacy processes. Larger businesses—particularly those in highly regulated, customer-facing industries that already must comply with strong data privacy rules—may enjoy the greatest potential

"New **data privacy laws will facilitate** the entire process as more customers are likely to **trust the platform and solutions**. They would also be more willing to use the solutions in more creative and innovative ways," said one respondent.

opportunities. "My sense is that large companies, especially U.S. companies, are well on their way to complying with GDPR," Mayer-Schönberger says. "The chasm is between large and small companies."

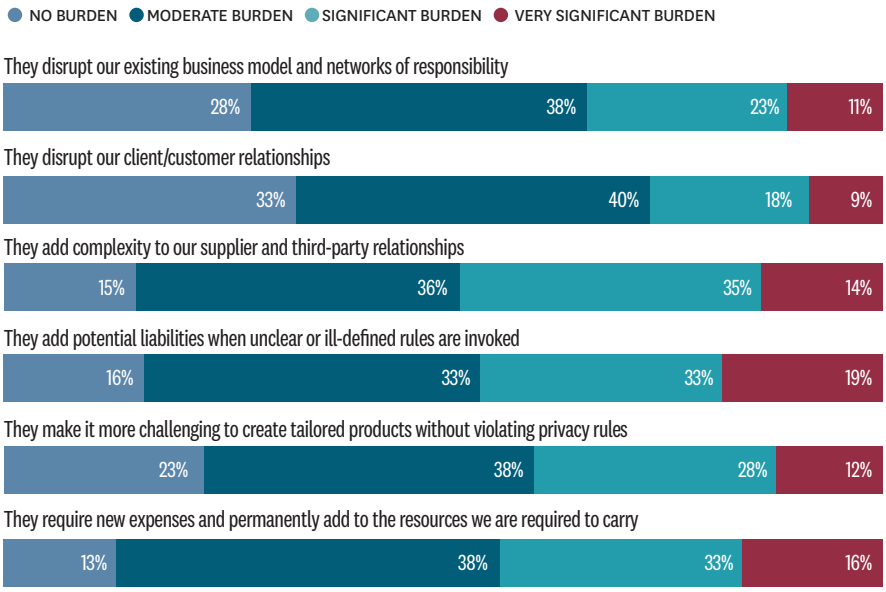
One way to bridge the gap, he suggests, may be to "collectivize" data privacy for smaller companies by creating an organization comparable to Underwriters Laboratories in the consumer products sector that could test, inspect, and certify that their products meet a standard for data security and privacy, and where appropriate, recertify them periodically. "Right now, small companies must do this themselves, at great cost," Mayer-Schönberger says.

The framework of the new digital economy—more rigorous, more regulated, more consumer-conscious—will remain, regardless. "New data privacy laws will facilitate the entire process as more customers are likely to trust the platform and solutions," said one respondent. "They would also be more willing to use the solutions in more creative and innovative ways." While many organizations still lag in implementing better data privacy and security procedures and safeguards, most are moving in the right direction—not least because the opportunities it can help them reap are too great to waste.

FIGURE 9

NEW REGULATORY BURDENS

What level of burden will new data privacy laws, regulations, and directives place on your organization in the next one to three years?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2017

METHODOLOGY AND PARTICIPANT PROFILE

A total of 331 respondents drawn from the *Harvard Business Review* audience of readers (magazine/newsletter readers, customers, HBR.org users) completed the survey.

SIZE OF ORGANIZATION

ALL RESPONDENTS' ORGANIZATIONS HAD 500 EMPLOYEES OR MORE.

41% 10,000 OR MORE EMPLOYEES

12% 5,000–9,999 EMPLOYEES

47% 500–4,999 EMPLOYEES

SENIORITY

19% EXECUTIVE MANAGEMENT OR BOARD MEMBERS

42% SENIOR MANAGEMENT

31% MIDDLE MANAGEMENT

8% OTHER GRADES

KEY INDUSTRY SECTORS

15% FINANCIAL SERVICES

14% TECHNOLOGY

9% GOVERNMENT/ NONPROFIT

9% MANUFACTURING

8% HEALTH CARE/ PHARMA/LIFE SCIENCES

6% OTHER SECTORS WERE EACH REPRESENTED BY 6% OR LESS

JOB FUNCTION

15% GENERAL/EXECUTIVE MANAGEMENT AND IT

7% FINANCE/RISK

7% CONSULTING

7% MARKETING/PR/ COMMUNICATIONS

7% SALES/BUSINESS DEVELOPMENT/ CUSTOMER SERVICE

6% OTHER FUNCTIONS

REGIONS

34% NORTH AMERICA

35% EMEA

24% ASIA/PACIFIC

7% REST OF WORLD

Endnotes

1 "European Data Market SMART 2013/0063: Final Report," prepared for the European Commission (Directorate-General for Communications Networks, Content and Technology) by IDC and Open Evidence. https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1

2 Matthias Bauer, Martina F. Ferracane, Hosuk Lee-Makiyama, and Erik van der Marel, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States," European Centre for International Political Economy, Policy Brief No. 03/2016, December 2016. http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

Harvard Business Review
ANALYTIC SERVICES

hbr.org/hbr-analytic-services