DEMOCRATIZING DATA

BY / ERIC KRELL

Are all companies now technology companies?

It seemed that way this spring as a variety of companies scrambled to comply with the European Union's General Data Protection Regulation (GDPR). The sweeping privacy law equips Europeans with more control over their personal data while significantly altering how companies collect and manage personal data and imposing steep fines—as much as 4 percent of global revenue—on violators. The companies that appeared to suffer most from GDPR compliance—an effort that also happens to cost U.S. companies 4 percent of their global revenue, according to Capgemini—were not Google, Facebook or other tech giants. Instead, business leaders within insurers, airlines and restaurants were more apt to grumble about the millions of dollars and months of work that their GDPR compliance efforts have devoured. The co-founder of a reservation service vented in The Wall Street Journal that 1) "Restaurants are not tech companies;" and 2) Restaurants are now being asked to manage data as if they were tech companies.

His second point is certainly accurate, but the first one will not hold water for much longer. "Every company is a technology company, no matter what product or service it provides," asserts M+W CIO Americas Stephenie Stone on Forbes.com. "The companies that embrace this fact are the ones that shape our world."

"EVERY COMPANY IS A TECHNOLOGY COMPANY, NO MATTER WHAT PRODUCT OR SERVICE IT PROVIDES. THE COMPANIES THAT EMBRACE THIS FACT ARE THE ONES THAT SHAPE

M+W CIO Americas Stephenie Stone

Put another way: if non-tech companies want to survive in the data-driven world, they better rapidly develop data management capabilities on par with Amazon, Google and other Silicon Valley giants already circling, or invading, their industries. This also holds true on a more personal level. Take a glimpse at a manager, director or vice president opening in almost any organizational function—finance and accounting, human resources (HR), sales and marketing, internal audit, risk and compliance, even tax—and you'll be hard-pressed to find a single set of specifications that does not emphasize the need for data analysis, management and/or governance expertise.

NOT EVERY BUSINESS PROFESSIONAL will need to run a SQL query or create a Python script, but professionals should be well-aware of the ways that data analytics and digital transformation are reshaping companies in ways that extend beyond technology capabilities. Addressing the following questions can help clarify this transformation while highlighting increasingly valuable skills:

1. HOW WILL COMPANIES PROTECT THEIR DATA?

When information security professionals speak candidly, their concerns are jaw-dropping. Staggering portions of cybersecurity gaps exist in organizations due to failures to apply basic, readily available software patches. Employees still getting hoodwinked by old-fashioned phishing emails, and many fail to perform the most rudimentary cybersecurity steps (e.g., avoiding unprotected public wireless networks). "We still have machines whose vulnerabilities should have been patched back in the 1990s," *CSO* columnist Roger Grimes noted in 2016. It is impossible to protect all data, but it is imperative to protect the most valuable data. Part of everyone's job should include understanding which data in their domain has the greatest impact on organizational risk. "An alarming number of companies appear unable to confidently identify or locate their most valuable data assets," Protiviti's most recent security and privacy report indicates. "Protecting these 'crown jewels' requires a data classification scheme supported by effective policies in place and adhered to throughout the enterprise."

2. HOW WILL PARTNERS PROTECT YOUR COMPANY'S DATA?

As more companies invest in cloud technology, more data and information assets are stored externally. As a result, organizational cybersecurity effectiveness also hinges on vendors' (or their vendors' vendors') security capabilities. Increasing digital collaboration also extends network access to more external partners. "Enterprises now have an expanding attack surface because of the vast number of third parties that have some degree of access to their network and/or their data," says Marsh Risk Consulting Managing Director Thomas Fuhrman. These risks are reshaping traditional vendor risk management (VRM) programs, which until recently, largely consisted of manual activities, such as having vendors fill out self-assessments or visiting the sites of key vendors. Those types of assessments remain necessary, but they are being enhanced by the addition of real-time monitoring of third parties.

3. HOW WILL YOUR COMPANY'S DATA BE REGULATED?

Global companies are having trouble keeping pace with new laws and regulatory changes related to data privacy and security. PwC Global Cybersecurity and Privacy Co-Leader Grant Waterfall describes the recent surge in cybersecurity laws—including GDPR, New York Department of Financial Service' cybersecurity regulation and China's complex Cyber Security Law (CSL)—as "a bit of a regulatory tsunami, especially for global companies." Organizations, he adds, "are being hit left right and center by these things..." Compliance functions within companies will need to work closely with their colleagues in risk, information security and information technology (IT) functions to understand new requirements and address them in an integrated manner, since different rules cover many of the same processes and internal controls.

4. HOW WILL COMPANIES MANAGE TAX DATA, AND HOW WILL DATA BE TAXED?

Global tax rules are undergoing changes that rival the magnitude of the digital transformations occurring inside companies. These dramatic shifts include The Tax Cuts and Jobs Act of 2017 (TCJA) and the European Commission's value added tax (VAT) proposal ("the biggest reform of EU tax rules in a quarter of a century," according to the commission), separate efforts by the EU and the Organization for Economic Cooperation and Development (OECD) to revamp how digital transactions are taxed, as well as dozens of country-specific "real-time" taxation submission requirements. Combined, these new tax policies are greatly increasing the amount of tax and transactional data that companies need to gather, protect and share with tax authorities. Some proposals have suggested that companies should pay a tax on data assets in countries where they collect that customer data. This ongoing global tax rules upheaval is elevating tax considerations to a strategic issue while making chief tax officers increasingly important participants in strategic planning activities.

5. HOW WILL YOUR COMPANY ACCESS DATA MANAGEMENT SKILLS?

Access to data analytics and cybersecurity skills marks a growing challenge for most companies. This is especially the case at increasingly digital companies outside of the tech industry, notes Stefan Deutscher, a cybersecurity and IT risk management expert with The Boston Consulting Group, "but few of them have the scale or the brand to attract and retain top cyber security [sic] professionals." This talent need will require more human resources functions to develop innovative approaches and partnerships to sourcing talent at a time when U.S. universities are struggling to attract enough educators to groom future data scientists.

All companies may not be tech companies, at least not yet. But all businesses and professionals should be prepared to address the ways that data analytics and digital transformation are reshaping their companies and their careers.

bbr.baylor.edu/questions-beyond-tech