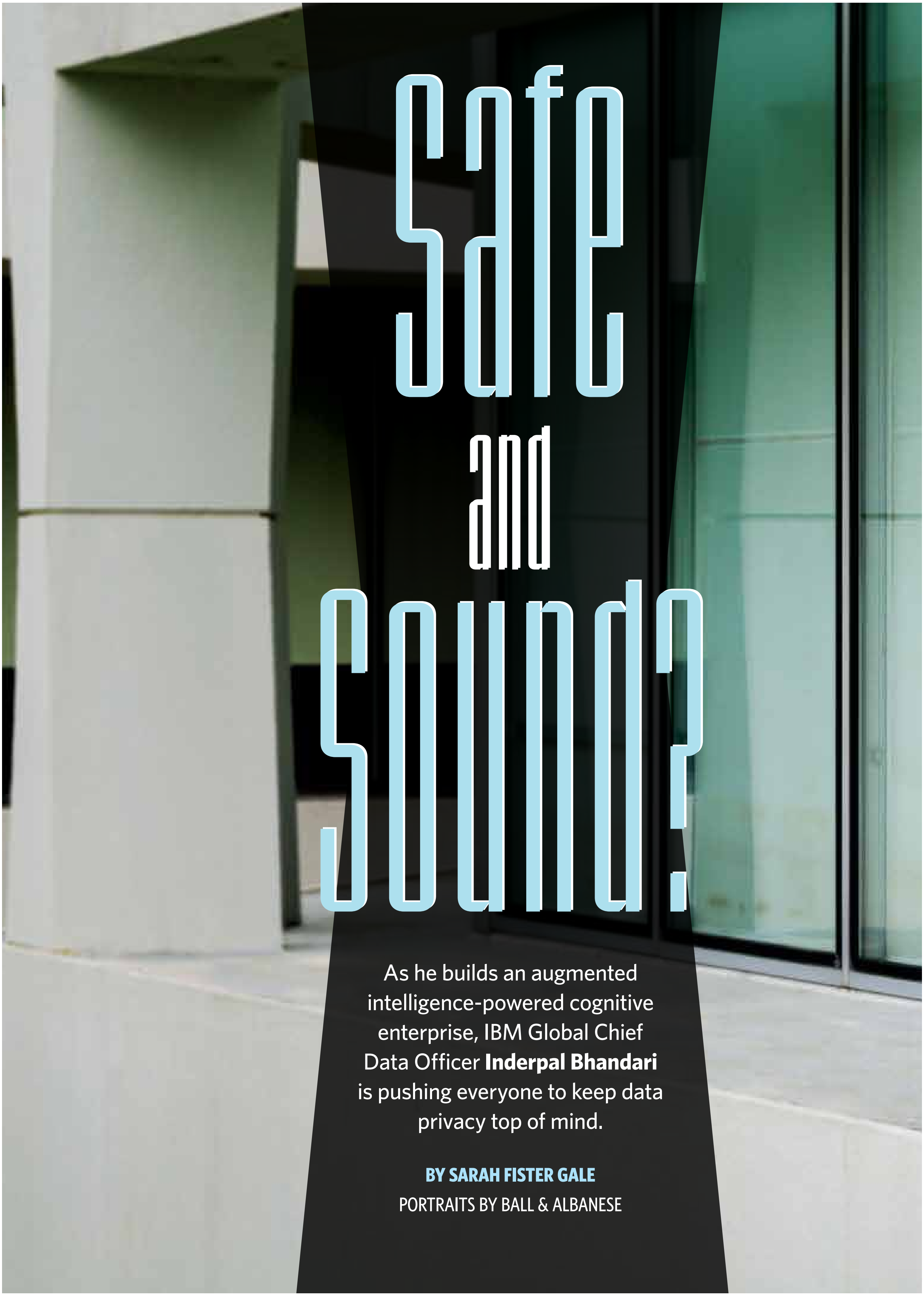


Safe and Sound?

As he builds an augmented intelligence-powered cognitive enterprise, IBM Global Chief Data Officer **Inderpal Bhandari** is pushing everyone to keep data privacy top of mind.

BY SARAH FISTER GALE

PORTRAITS BY BALL & ALBANESE

Data is sparking a major corporate crisis.

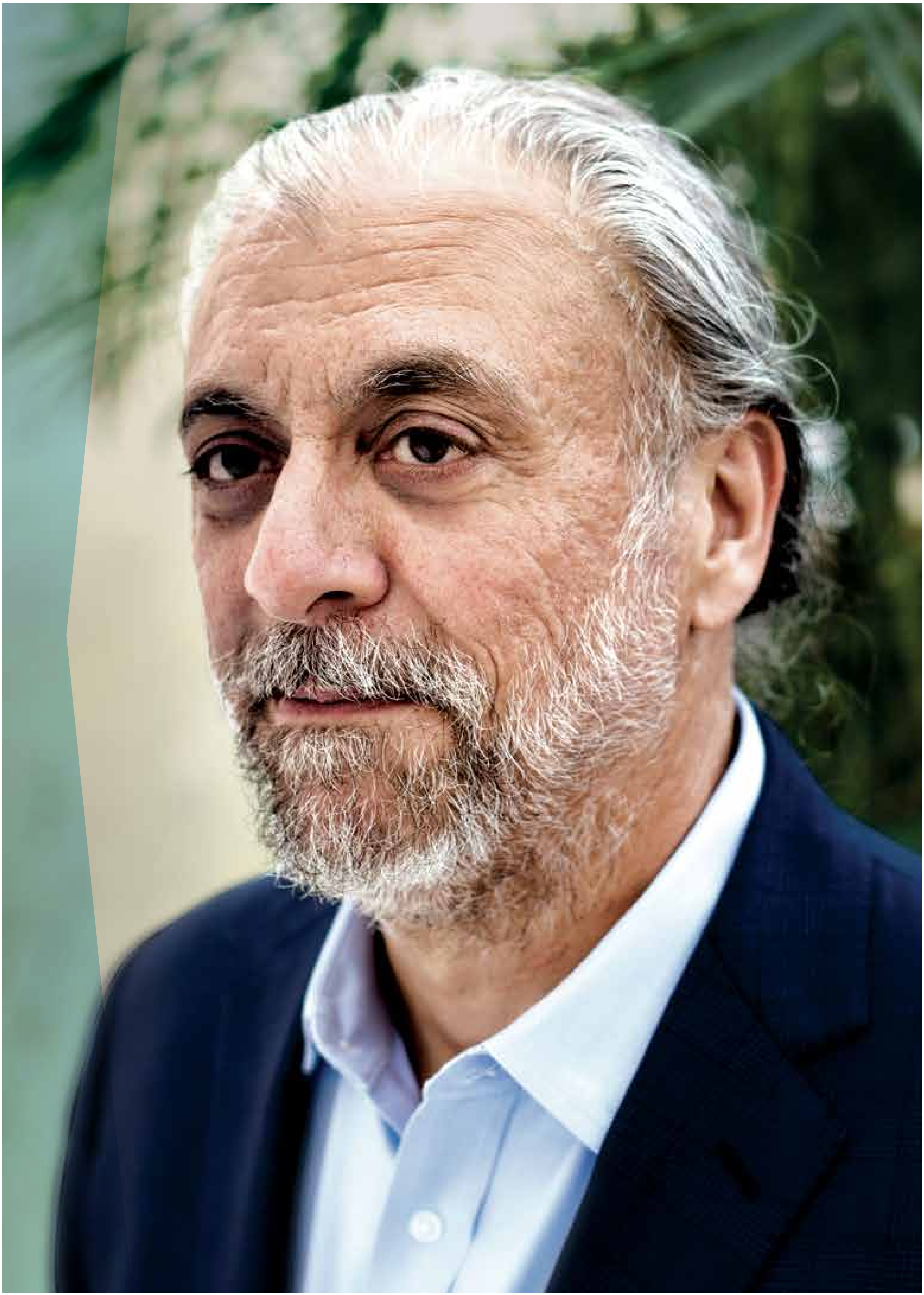
Executives are being held to account for security vulnerabilities leading to the theft of sensitive customer information—top leaders at Equifax, Yahoo, Target and other companies have been shown the door in the wake of major breaches. Entire companies are seeing their fortunes wane if customers turn away from how their personal data is being used. The Cambridge Analytica scandal, for example, put major dents in Facebook's brand and raised questions about the company's business model. In a digital world, data is both an asset to be leveraged and a liability to be protected.

"Executives are not only becoming more aware of the importance of data security, they are also increasingly being held accountable after data breaches," says Inderpal Bhandari, global chief data officer (CDO) of IBM, the $80 billion global technology organization headquartered in Armonk, New York, USA.

No surprise, then, that CDOs are now among the most important leaders in many of the world's top companies. Ten years ago, this C-suite role was virtually unheard of. But today CDOs act as transformation leaders, charting a company's digital course, finding new ways to leverage data, and safeguarding customer and company data. As data breaches become commonplace and complex data privacy regulations are implemented, executives are looking to their CDO for security guidance and guarantees.

Mr. Bhandari is up to the challenge. He began his career with IBM in 1990 studying data mining at the Watson Research Center and became one of the first executives to earn the title of CDO in 2006 while at Medco Health Solutions. Over the years, he helped to define the role as it evolved from "king of the data warehouse" to transformation

> "Executives are not only becoming more aware of the importance of data security, they are also increasingly being held accountable after data breaches."
>
> **—Inderpal Bhandari,**
> global chief data officer, IBM



“We made the decision early on that building a relat customers makes perfect strategic business sense.

—Inderpal Bhandari

leader. Since returning to IBM as CDO in 2015, Mr. Bhandari has been redefining the company’s data strategy based on the vision of a “cognitive enterprise” that is powered by augmented intelligence and has data protection at its core. “We made the decision early on that building a relationship of trust between us and our clients and customers makes perfect strategic business sense,” he says. “It is the direction the market will go.”

The Promise and the Perils

The vision Mr. Bhandari is in the process of implementing at IBM underscores both the promise and perils of data-centric enterprises. Here is how the IBM cognitive enterprise works: Advanced augmented intelligence systems and analytics powers can instantly merge multiple vast datasets to generate new insights on demand. In Mr. Bhandari’s vision, augmented intelligence allows IBM’s subject matter experts to submit a query and instantly receive all of the information they need to solve a problem, regardless of where that data resides and what format it takes.

“The cognitive enterprise system helps them answer questions more effectively, rapidly and accurately because they’re able to harness all of this information, which previously they wouldn’t have been able to use,” he says.

This makes IBM’s data more valuable and efficient, but it also makes data security a lot more challenging. In an era where the number and scale of data breaches continues to grow, data security is now a C-suite imperative.

“The C-suite must make data privacy and security a top priority for the company, recognizing that a lapse can put the enterprise itself at risk,” Mr. Bhandari says. “Seventy-five percent of consumers say they will not buy a product from a company—no matter how great it is—if they don’t trust the company to protect their data.”

With this in mind, Mr. Bhandari has broadened IBM’s security practices to encompass data privacy. This necessitates additional security barriers in everything IBM designs. “It’s evident that you have to protect the privacy of the subject whose data you are carrying,” he says.

Mr. Bhandari notes that as augmented intelligence capabilities advance, it can lead to unexpected data privacy risks. He points to the classic example of a major retailer analyzing data for marketing purposes about a consumer

IBM researchers celebrate a patent for a system that detects and counteracts cyberattacks.

PHOTO COURTESY OF IBM

ionship of trust between us and our clients and It is the direction the market will go."

buying prenatal vitamins and other products. The company inferred she was pregnant and then sent her marketing materials for baby clothes and other products—only to discover that she was in high school and her parents were unaware of her pregnancy. "Each data element by itself was OK, but the conclusion clearly violated her privacy," he says. "This is the nature of analytics. It is what makes it so powerful, but it also makes it hard from a regulatory standpoint to perfectly protect everybody."

A Culture of Trust

For Mr. Bhandari, this kind of scenario reinforces his commitment to building trust into every element of IBM's product design process. "In this environment, the only thing that a customer can lean on is 'Can I really trust this organization to look after my interests?'" he says. "That's why it has to be part of our data privacy culture."

As a global organization that processes, stores and analyzes millions of bits of data from customers and clients, IBM is obligated to be sure every action it takes directly benefits the owner of that data and any related vendor. "That is what is required today. I believe companies that have acted otherwise will face significant challenges."

The constant threat of security breaches makes it difficult to deliver on a promise of trust to customers. In the first half of 2017, more than 6 billion records were exposed through 2,227 publicly disclosed data breaches, according to a report from Risk Based Security. That number of records was an all-time high, putting executives like Mr. Bhandari on alert.

"There is the risk that powerful technologies like artificial intelligence and the internet of things can be misused by bad actors, which makes it very difficult to protect data," he says. One of the biggest risks today, according to Mr. Bhandari, are botnets: malware that causes a collection of connected devices to be controlled by a hacker without the owner's knowledge. Hackers "are able to harness botnets at a scale never before possible and use them against companies, individuals and even governments," he says. "That is a major technology challenge."

Building a culture of trust amid such malicious threats is a key leadership challenge Mr. Bhandari faces as he works to build a data-driven cognitive enterprise. To create secure products and infrastructure, trust must be embedded in everything IBM does. As an example, he cites IBM's cloud computing platform. It was architected from the ground up so that even in a multi-tenant, multi-cloud environment, the company can guarantee every client that their data—and any insights drawn from it—is controlled by them, unless they choose to let it be shared.

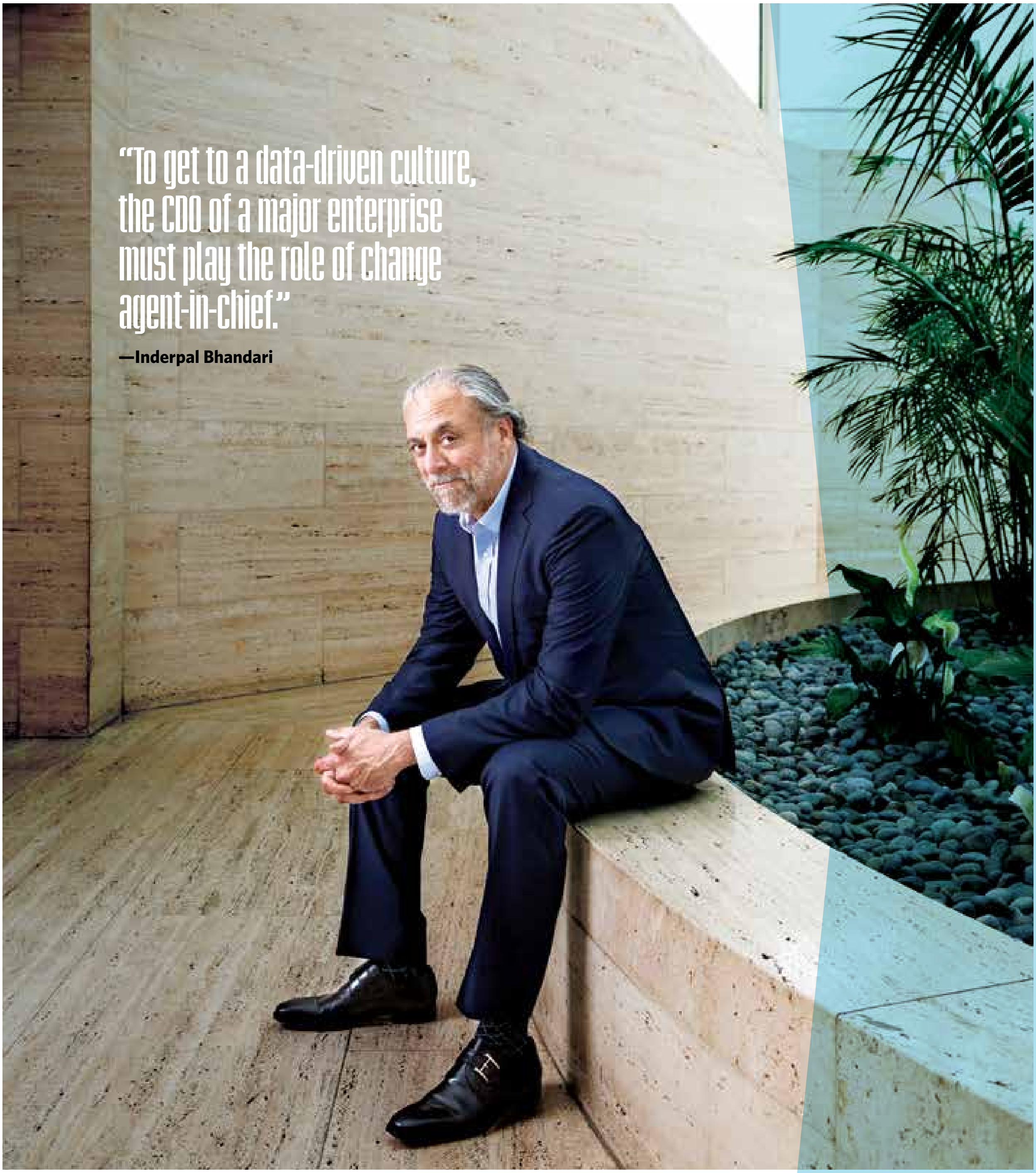
But the company's data privacy strategies cannot be limited to the internal IBM infrastructure. "Trust needs to extend through the supply chain, because if the enterprise can't trust a vendor it makes them vulnerable to being breached," he says. Sixty percent of organizations now say they are more concerned about a data breach from a third party, such as a partner or vendor, than from within their own company, according to a 2017 survey by Ponemon Institute and Opus.

From a leadership perspective, embedding sound data privacy practices through an organization—and building new data-driven enterprise tools—is fundamentally a change management challenge. "To get to a data-driven culture, the CDO of a major enterprise must play the role of change agent-in-chief," Mr. Bhandari says. "Having recognized this over my career as a four-time CDO, my leadership style has evolved to 'fail fast' by

60%

of organizations say they are more concerned about a data breach from a third party, such as a partner or vendor, than from within their own company.

Source: Ponemon Institute and Opus



"To get to a data-driven culture, the CDO of a major enterprise must play the role of change agent-in-chief."

—Inderpal Bhandari

design. One learns by making a series of missteps that are all but inevitable as one pushes the envelope to effect change."

High-level relationships matter. He credits his close working relationship with IBM's Chief Information Security Officer David Cass and Chief Privacy Officer Cristina Cabella for promoting the strategic vision of the cognitive enterprise to every business unit leader and project team. Building these relationships is the best way for a CDO to promote a culture of trust and ensure teams prioritize data security and privacy. Executives need to "make employees aware of the consequences of data breaches and poor data privacy practices," he says, adding that even if it adds time or cost to a project, it is worth it. "A culture of trust does impart additional constraints on the setup, and it does make the engineering process more complicated. But making sure clients and customers can trust us with their data is the only way to make use of these new technologies for their benefit." **IQ**

The Evolution Starts Now

The European Union's new GDPR data privacy regime is a big deal—but not in the way many people think. *By Novid Parsi*

European Parliament President Antonio Tajani greets Facebook CEO Mark Zuckerberg, left, in Brussels in May.

PHOTO BY JOHN THYS/AFP/GETTY IMAGES

Suddenly, "privacy policy" emails flooded everyone's inbox. In May, those emails were the most obvious indication that the European Union's new General Data Protection Regulation (GDPR) had gone into effect. It felt like a whole new day for data privacy—but contrary to popular perception, the GDPR does not fundamentally change the rules for how companies handle data, says Jack Carvel, general counsel for London, England-based Qubit, which provides personalization software. But the new regulation does mark a shift in the balance of power between companies and customers, Mr. Carvel says.

As before, companies still have to be transparent about how they use an individual's data. They have to be upfront about what they are collecting, why they are collecting it and how long they will keep it, Mr. Carvel notes. They also still have to be fair in their use of data, and they cannot collect more information than they actually need. That is why the Information Commissioner's Office—the U.K. regulatory body that upholds information rights—called the GDPR an evolution in data protection, not a revolution.

But new stiff fines are now in the mix. The maximum fine for noncompliance with the GDPR is €20 million or 4 percent of a company's global annual revenue—whichever is greater. (For Facebook, that could be $1.6 billion.) Little surprise, then, that companies are taking the GDPR more seriously.

Another significant change brought on by the GDPR, which applies to any company processing the data of EU citizens, involves implied consent. "The internet had worked on the basis of implied consent: 'By using this site, you comply with this long policy,'" Mr. Carvel says. "Under the GDPR, companies can't rely on implied consent anymore." Now, businesses must receive an individual's explicit, informed consent, and this must be evidenced by an affirmative action. The GDPR also clarifies accountability: Companies have to document their compliance. For example, when someone asks a company to provide or delete all their personal information, the company has to document that it has done so.

The GDPR's basic guiding principle of fairness and transparency should limit what Mr. Carvel calls creepy uses of data—in particular, the ways that some companies use a slew of information to target ads and products to individuals or to make decisions affecting their lives.

Inderpal Bhandari, chief data officer (CDO) at IBM, says the GDPR has informed his company's data security strategy as much as the risk of data breaches. That strategy is about building relationships with customers that are built around trust. "The movement around data sovereignty obviously informs our thinking."

Complying with the regulation was a "massive challenge," he says. It was also the occasion for one of his leadership missteps since becoming IBM's CDO in 2015. Initially Mr. Bhandari thought IBM could achieve compliance by focusing only on internal data management systems where the company had 100 percent control. "But then I learned that the major work was in how we worked with suppliers and clients—the best result would only occur if we were all on the same page."

IBM has tens of thousands of supply relationships, and the data security team had to be sure any solution they brought forward was compliant. "So collaboration was a key aspect of what we had to do," he says. The team spent months collaborating with every vendor to be sure the way they captured, used and stored data was GDPR-compliant at every step.

It was not merely a "check the box" activity. "Through the compliance process we found that everybody had different levels of preparedness, but also different interpretations of the GDPR." That required some unavoidable debate. "Given the yardstick by which we judge ourselves regarding trust, security and privacy, we knew we had to go the extra mile," Mr. Bhandari says. "It was a massive effort across the board, but I think differentiates us in terms of our commitment to data privacy."