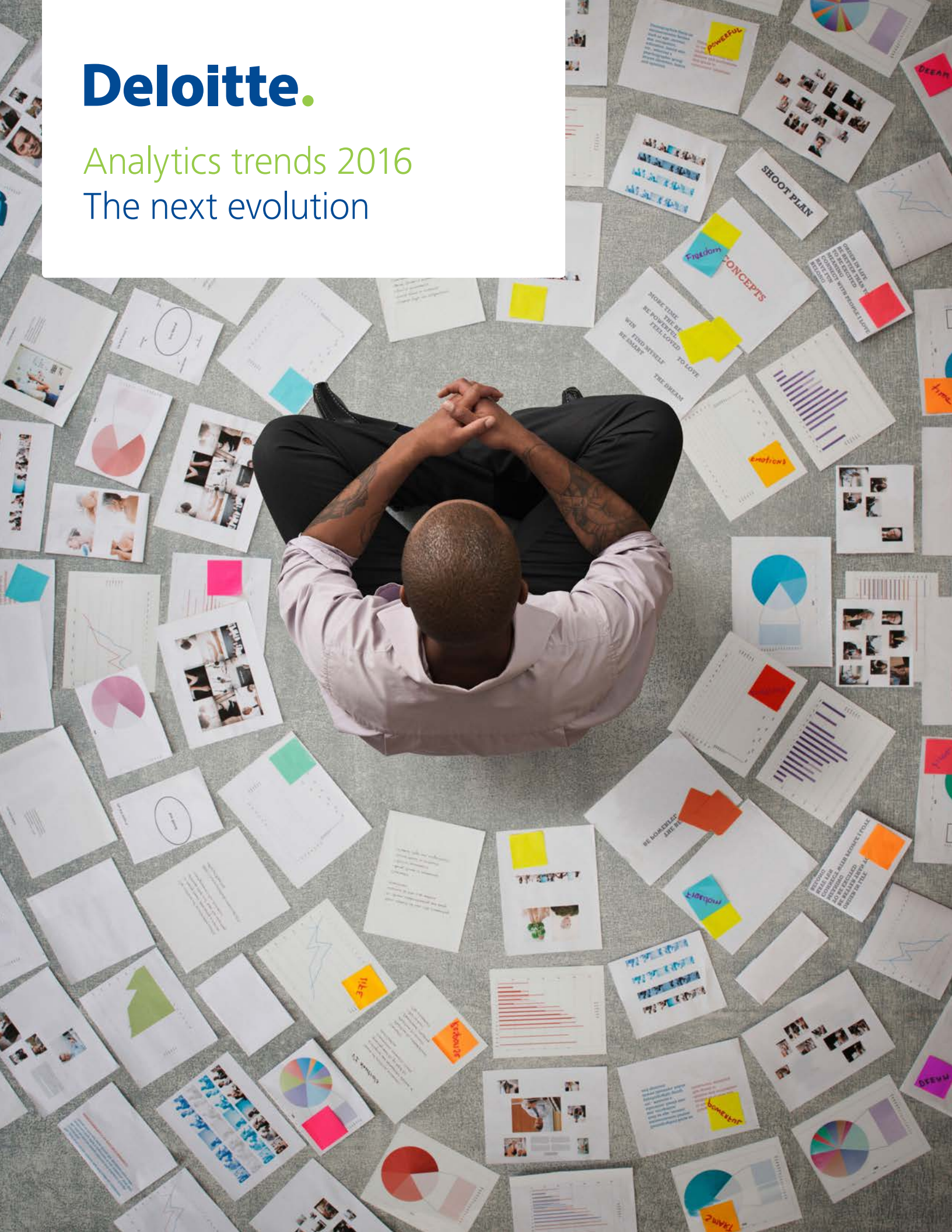
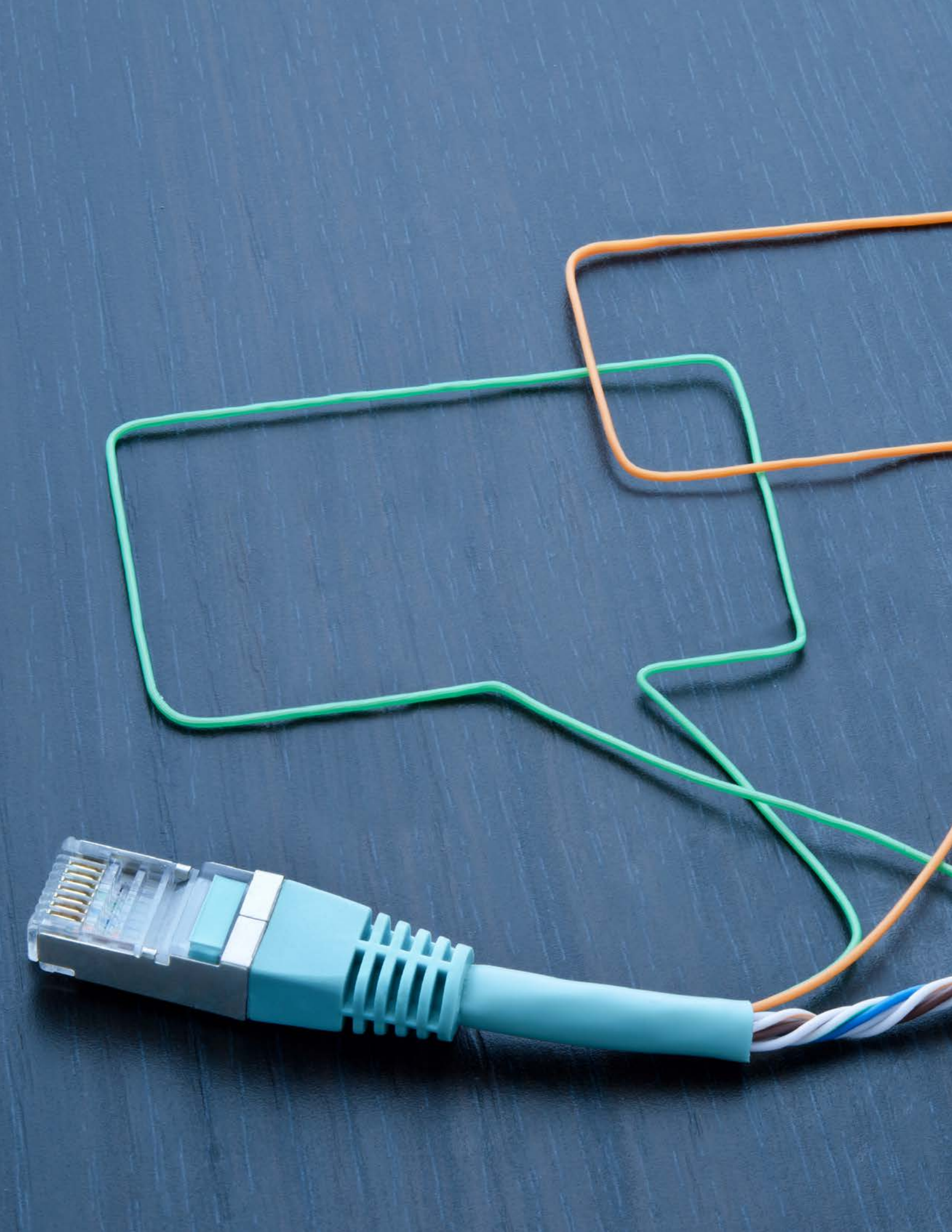
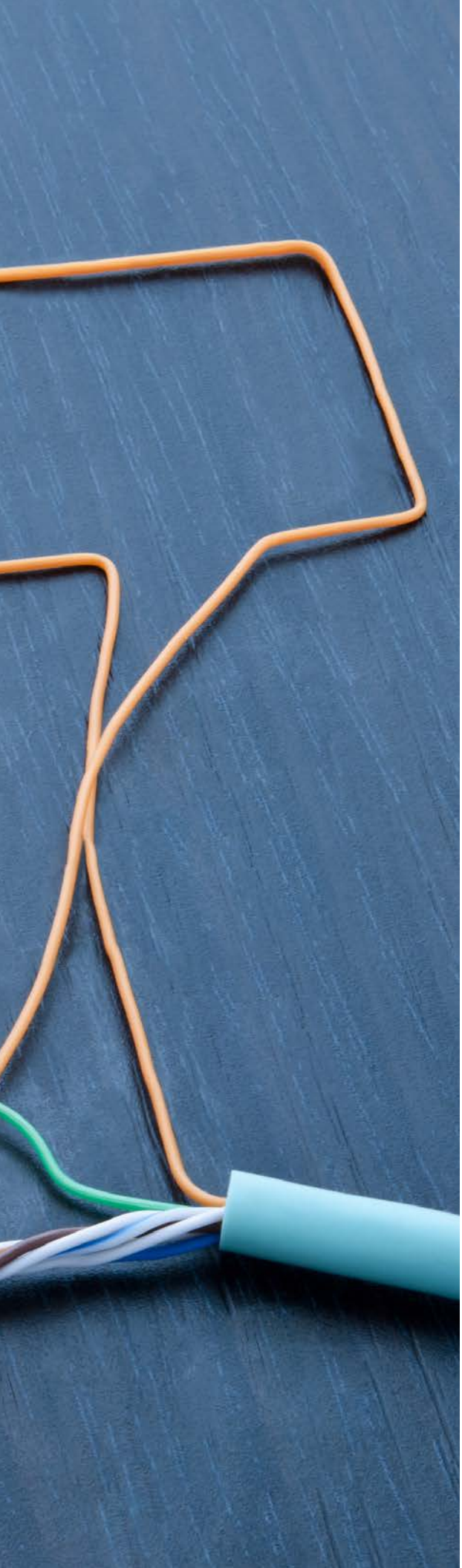
Deloitte.

Analytics trends 2016
The next evolution







Contents

The delights and dangers of data

With each passing year, organizations across Canada grow more reliant on data to set strategy, manage their operations and understand their market. Yet, as data proliferates it also becomes democratized—making it accessible to information gurus and neophytes alike. To be sure, this presents untold opportunities, particularly as employees at every level of an organization begin to rely on insight-driven strategies to make business decisions, engage with customers and employees, and increase revenues.

At the same time, however, this trend introduces new risks. Misuse of data—intentional or not—can expose an organization to legal liability and severe reputational damage. A weak security stance can also make organizations the targets of cyber attackers, putting critical data assets at risk. More significantly, the failure to turn data into reliable insight, or move from insight to action, can derail an organization's analytics progress or commitment—resulting in lost time and money, strategic misdirection and, in some circumstances, disruption and business failure.

To help you maximize the return on your analytics investments, while minimizing risk, Deloitte has identified five key analytics trends set to change the way organizations will compete in the years ahead.

Analytics drives every decision and action

More than data and technology

With the widespread adoption of analytics, many organizations have focused on wrestling their big data into shape and putting a technology infrastructure into place. However, it is becoming clear that a narrow focus on data and technology can stymie an organization's analytics journey. That's because analytics without action tends to generate nothing more than an interesting finding or an expensive latent capability. To gain true value from the analytics journey, organizations are discovering that they must embed data, insight and reasoning into the very fabric of their decision-making processes. This is spurring the rise of the Insight Driven Organization (IDO)—one that turns analytics into a core capability across the organization by promoting a culture of insight-driven decision-making.

Five building blocks

IDOs address five essential building blocks:

They identify executive sponsors to describe the analytics vision and tie it to the organization's overall strategy.

They build 'purple teams' that have the skillsets to drive analytics success, and adopt a culture that empowers people at every level of the organization to rely on the insights their data uncovers.

They adopt an operating model, governance structure and measurement framework capable of not only turning data into insight but turning insight into action.

They create information models to capture the right data, ensure data quality and align their analytics focus with their business objectives.

They bring together the right solution architecture, sandbox, technical resources and delivery model to enable ongoing innovation.

Analytics everywhere

The real differentiator of an IDO, however, is that it approaches analytics as an enterprise-wide competence, rather than as a project confined to an isolated division or operating system. By injecting analytic insight into every decision they make—from the boardroom to the shop floor—IDOs equip their people to deliver targeted in-store experiences, customized product suggestions and stellar customer service. As a result, they gain the ability to increase revenues, reduce costs, mitigate risk and out-compete more often. This may explain why the IDO concept is poised to vastly alter the way in which organizations have traditionally approached analytics.

Analytics, digital and innovation converge

The strategy paradox

Disruptive trends such as digital, mobility, analytics, social networking, cloud computing and big data are fundamentally changing customer expectations. Competition is also reaching unprecedented heights—particularly from online innovators. These combined forces are making it exceptionally challenging for organizations to get strategy right. The strategy paradox is that even good companies will be doomed to mediocrity if their strategies can be easily imitated by others.

Going agile

To achieve true differentiation, then, leading organizations will need to simplify strategy development by unifying their approach to analytics, digital and innovation. Rather than setting up siloed digital labs, innovation centres and analytics programs that operate on the periphery and are isolated from each other, they must converge these capabilities within the heart of their organizations. This should see them using analytics to inform and measure their win strategy, digital to quickly and efficiently engage and connect with stakeholders across multiple channels, and innovation to pivot their strategy in response to real-time data. Rather than setting strategy once and revisiting it every few years, leading organizations will create agile strategies capable of being measured, tested and refined on the go, as market realities change.

Infecting the host

Making convergence work will require a willingness to stop protecting isolated teams of analytics, digital and innovation projects with antibodies. Instead, organizations must infect the host by adopting new capabilities at scale. They can do this by engaging in short, sharp, agile pieces of work rather than making big up-front investments. They need to build a culture capable of getting things done fast and fixing them on the fly—based on insights they glean from their data. And they have to seek out change agents capable of inspiring the organization to create multi-threaded strategies on an ongoing basis. It's a true mindset shift that is focused not on predicting the future, but on developing a process that is sufficiently flexible and fluid to dynamically support a change in strategy as the future unfolds.

Insight informs omnichannel strategies

Walking the talk

It's been a few years since organizations first started talking about the imperative to deliver an integrated customer experience across all their touch points—from brick-and-mortar locations to e-commerce, mobile apps and social media. Now, the time for talking about omnichannel experiences has passed. Instead, it's time for implementation. This requires organizations to better understand how to capture a return on their omnichannel investments. In essence, organizations need to determine how each channel contributes to the success of the others so they can make more intelligent investment decisions and create experiences that drive not only customer loyalty but increased profitability. The challenge? Traditional ways of making these decisions no longer work. In a world where customers vote with their feet and competition continues to intensify, businesses need the ability to both test and build more solid business cases.

Intelligent decisions require intelligence

To overcome these challenges, organizations are increasingly turning to analytics. From the masses of data they collect, they are looking for answers to critical questions that will guide their omnichannel investments. This goes beyond simply determining what products to cross-sell and upsell, and extends to an assessment of the returns they are earning for each channel and the profitability of particular customer sets across various channels. The savviest organizations will ultimately want to use analytics to pre-empt their competitors, particularly as competition continues to come from entirely unexpected quarters. Retailers, banks and telecom companies now compete with each other, mandating businesses to clarify who they are being compared to if they hope to deliver the differentiated experiences their customers expect and define what their brands stand for.

Insight-driven strategies

As organizations begin to act on the insights data delivers to not only ask the right questions but make the right investments, they can begin to refine their omnichannel strategies. To assess whether they need a loyalty program or talking dressing room, for instance, or if they have the right talent to compete against non-traditional competitors, they will need to engage in a data discovery process designed to reconcile their competing versions of the truth and eliminate their data, organizational and functional silos. As experience is rapidly demonstrating, organizations that hope to deliver not only targeted customer experiences but a solid return on their investments must get serious about relying on analytic insights to build out their omnichannel strategies.


Analytics
Audience
Country
City
Status
Sex
Age
Interests
Collaboration
Behavior
Technology
Mobile
Custom 1
Custom 2
Custom 3
Income
Education
Daily Unique Sales by Country
Home
Dashboard
Repoting
Customization
Help
Log Out
Daily Product Sales by Country

Intelligence boosts cybersecurity

The risk of cyber complacency

Most organizations understand that cyber criminals have become exceptionally sophisticated in recent years, exploiting vulnerabilities and weaknesses in IT systems, people and processes to access a huge range of critical data assets. What they don't understand is how exposed they truly are. According to Deloitte Canada's 2015 Cybersecurity Survey—which polled IT leaders at more than 100 major Canadian organizations—60% of respondents said they had not experienced a cyber attack in the past 24 months—and 90% of those said they feel protected against cyber attacks. In other words, those who had not reported being attacked generally felt protected—a potential set-up for developing a false sense of security. It doesn't help that the majority of Canadian businesses rank low on the cybersecurity maturity scale (2.2 out of 5). And maturity matters: this ranking reveals that only about half of businesses use managed security service providers (MSSPs), have a defined cyber resiliency and recovery process, or have documented incident procedures that they follow or test.

The path to maturity

To improve their cybersecurity posture, Canadian businesses need to ensure that their systems are secure, vigilant and resilient. Secure businesses have a security-awareness culture, effective procedures and technologies designed to keep attackers out. Vigilant businesses use people, technologies and partners to monitor the threat landscape, as well as their internal organization. And resilient businesses can do more than repel a variety of attacks. They can also recover effectively from those attacks and learn from them to become more resilient.

Notably, analytics plays a significant role in each of these areas. Beyond using an MSSP, the most secure organizations take intelligence-gathering seriously—with more than 90% monitoring publicly available information about their brand, products, IT, procedures and people. When it comes to vigilance, however, only 33% of organizations have a formal cyber threat intelligence (CTI) process and less than 2% perform global cross-site intelligence sharing. Similarly, while 62% of organizations have defined incidence response procedures—demonstrating their resiliency—just 43% are performing only periodic vulnerability assessments, meaning they aren't capturing the information they need to identify threats before they can spread.

Integrating intelligence with security

As this survey shows, organizations will increasingly need to enhance their CTI capabilities if they hope to bolster their cybersecurity and protect their critical data assets. In truth, most organizations already gather threat intelligence. The issue is that they have too much of it, and don't know what is relevant or what to do with the information that is relevant. By leveraging best in class technology, partnerships and resources, however, they can make the intelligence they gather truly meaningful by building advanced security event monitoring systems that involve innovative analytics and cyber threat management capabilities. In fact, those that have a formal CTI process are 32% more likely to conduct infrastructure, network and system-centric profiling; 16% more likely to engage in user-behaviour analysis and traffic-flow analysis; and 18% more likely to have real-time business risk analytics and decision support. That's because they understand the need to integrate intelligence within security operations, monitoring technologies, analytics capabilities and employee education programs. By relying on automated intelligence sources and industry-leading threat intelligence analysts, organizations that adopt this type of predictive intelligence can better detect threats, understand their impact and make informed decisions to actively strengthen their security capabilities.


Generation Type
OTHER = 12
NUCLEAR = 25
COAL = 400
WIND = 45
Energy Tariff
Generation by Country
CHINA = 400

Data use decisions come under the spotlight

Exploring the boundaries

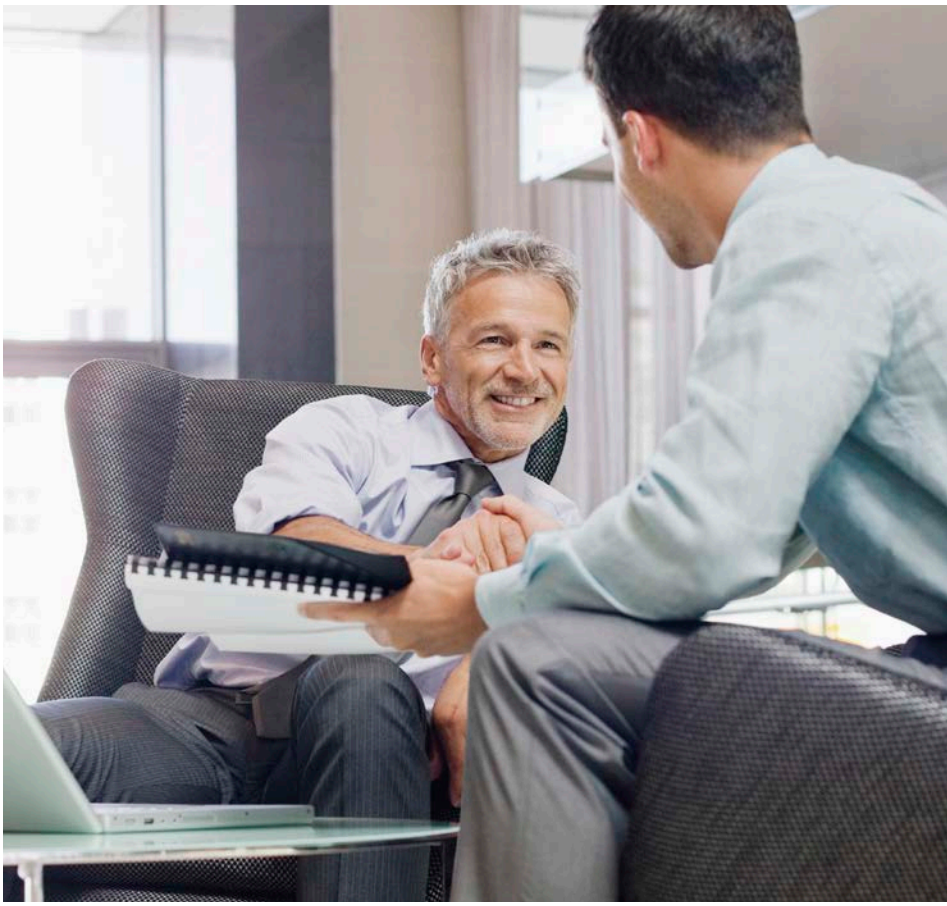
As analytic strategies and implementations become more mature, organizations will gain significantly greater opportunities to work with their data to manage all aspects of their business. For example, analytics will become increasingly pivotal to deliver the one-to-one, real-time, customer-centric immediate service and omnichannel experience that customers will demand. However, in using this data to provide a targeted, individual experience, organizations will still need to be mindful and intentional in how—and how often—they interact with their customers. That's because there are boundaries that go beyond the legal use of data. Although the boundary between the legal and appropriate use of data is often a grey area, executive sponsors, lines of business and purple teams will need to responsibly resolve this conundrum. Ultimately, this isn't just a question about what organizations are legally permitted to do with their data. Instead, it's about what they *should* do with their data to avoid breaching stakeholder trust or damaging their reputation.

Could vs. should

As the boundary around data use changes, the democratization of data increases and one-to-one data use arrangements proliferate, the danger of data misuse rises. That's particularly the case if the organization fails to clearly articulate its principles, beliefs and values around the acceptable use of data. Simply stated, it's eminently possible for internal users to take shortcuts, and misuse information in a way that entirely alienates customers—without ever breaching privacy. Even if the repercussions don't include lawsuits, they can easily create untold harm to a company's brand. This makes it imperative for organizations to define the "should" line they will not cross, particularly as they become more reliant on data to empower their employees and drive their decisions.

With great power comes great responsibility

Beyond securing data privacy and security, organizations have a moral responsibility to treat their customers' data with integrity and respect. That's why it's incumbent upon executive sponsors to implement policies and foster a culture designed to safeguard their information assets. That's also why adherence to these rules is everyone's responsibility. Savvy organizations will find the balance that allows them to connect with their customers in meaningful ways without breaching their trust. As an added benefit, this tacit agreement to uphold client trust will help organizations differentiate themselves in a crowded and competitive marketplace.



To discuss how emerging analytics trends may affect your organization, contact:

Anthony Viel

Managing Partner,
Deloitte Analytics
+1 416 452 8341
anviel@deloitte.ca

deloitte.ca/IDO

Lynette Horton

National Director,
Deloitte Greenhouse
+1 416 436 0535
lhorton@deloitte.ca

greenhouse@deloitte.ca

Deloitte.

www.deloitte.ca

Created by the Deloitte Information Design Lab.