The rise of the social enterprise

2018 Deloitte Global Human Capital Trends

Experience Deloitte's
Global Human Capital Trends **like never before. Access the new HC Trends app featuring exclusive content.**

Deloitte's Human Capital professionals leverage research, analytics, and industry insights to help design and execute the HR, talent, leadership, organization, and change programs that enable business performance through people performance. Visit the Human Capital area of www.deloitte.com to learn more.

COVER AND CHAPTER ILLUSTRATIONS BY TRACI DABERKO

People data

How far is too far?

The domain of people analytics is growing rapidly, offering new opportunities to better hire, manage, retain, and optimize the workforce. As organizations collect more personal and business data about their employees, however, they raise growing risks and ethical questions about data security, transparency, and the need to ask permission. Organizations now need robust security safeguards, transparency measures, and clear communication around their people data efforts—or they could trigger employee privacy concerns and backlash over data abuse.

THE use of workforce data to analyze, predict, and improve performance has exploded in practice and importance over the last few years, with more growth on the horizon. In our 2018 *Global Human Capital Trends* survey, 84 percent of respondents viewed people analytics as important or very important, making it the second-highest-ranked trend in terms of importance.

What explains this surge? We see three converging forces driving people analytics:

- A growing emphasis on critical workforce issues such as productivity and employee engagement, as well as on social issues such as diversity and gender pay equity, is raising CEO-level questions about the best way to lead and manage people.
- Big HR investments in people analytics are yielding many new sources of data. Our research shows that more than 70 percent of respondents are in the midst of major projects to analyze and integrate data into their decision-making.

- Organizations are growing more anxious about their ability to protect employee data—and for good reason. This year, only 10 percent of our respondents felt that their companies were "very ready" to deal with this challenge.

The growing power of people data

The people data revolution, predicted for years, has finally arrived. Sixty-nine percent of organizations are building integrated systems to analyze worker-related data, and 17 percent already have real-time dashboards to crunch the avalanche of numbers in new and useful ways.[1] Among companies at level 3 and 4 in Bersin's people analytics maturity model,[2] 90 percent have accurate, timely data, and 95 percent have data security policies in place. These leading companies are monitoring people data from

many sources, including social media (17 percent), surveys (76 percent), and integrated data from HR and financial systems (87 percent).[3] Creative organizations are mining this rich variety of sources to create a comprehensive "employee listening architecture," providing new insights about the entire employee experience as well as data on job progression, career mobility, and performance.

Advanced analytics can now track and analyze a dizzying amount of employee data, including data harvested from voice communications, personal interactions, and video interviews. Even the sentiment of employee emails can now be measured and monitored.[4] Several vendors now offer organizational network analysis (ONA) software that interprets email traffic to monitor employees' stress levels and help spot fraud, abuse, and poor management. Other ONA tools can analyze employee feedback and performance to identify management challenges, send coaching tips to different leaders, and identify key knowledge management resources, subject-matter experts, and organizational influencers based on their interactions and relationships—not necessarily their titles and roles.[5]

Heightened rewards, heightened risks

Analytics tools offer tremendous opportunities. But in the face of the obvious benefits, many executives may be slow—or perhaps reluctant—to recognize the significant potential risks. Organizations are approaching a tipping point around the use of people data, and those that tilt too far could suffer severe employee, customer, and public backlash.

Indeed, some organizations are now considering the mere existence of data to be a risk. This is the premise behind requirements in the European Union (EU) and elsewhere that one must delete a data element immediately when it is no longer relevant to the processing need, or else face a variety of consequences due to the risk that retaining it presents. Europe's new General Data Protection Regulation (GDPR), slated to come into effect in spring 2018, expands upon this concept by defining high-risk data as that which is "likely to result in a high risk for the rights and freedoms of individuals," and that, therefore, requires greater protection.[6] Private sector actions should keep pace with forward-looking efforts that are designed to strengthen data privacy regulations. Companies that break the new GDPR rules will face penalties as high as €20 million, creating strong incentives for organizations to take data protection seriously.[7]

What risks are most pressing? Our 2018 survey yields some important insights. This year, 64 percent of respondents reported that they are actively managing legal liability related to their organizations' people data. Six out of ten said that they were concerned about employee perceptions of how their data is being used. However, only a quarter reported that their organizations were managing the impact of these risks on their consumer brand.
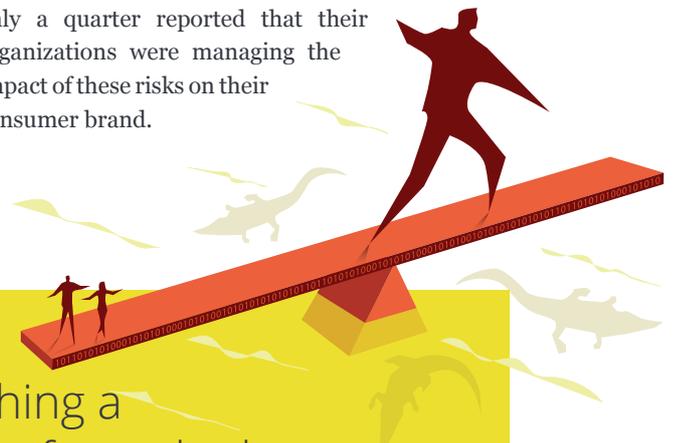
Organizations are approaching a tipping point around the use of people data, and those that tilt too far could suffer severe employee, customer, and public backlash.

PEOPLE DATA'S RISKS TO CONSUMER BRAND: A POTENTIAL BLIND SPOT?

When it comes to using people data, organizations are actively managing risks around employee perceptions and legal liability, but only a quarter are managing the potential impact on their consumer brand.

Figure 1. Management of HR data risk levers

PERCENT OF ORGANIZATIONS ACTIVELY MANAGING IMPACTS TO EACH AREA THAT COULD ARISE FROM AN HR DATA BREACH
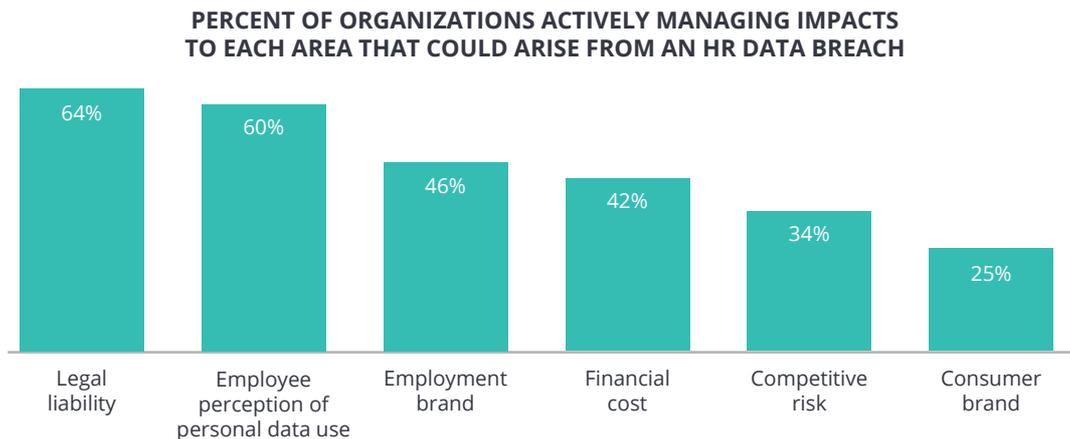
n = 11,069
Source: Deloitte *Global Human Capital Trends* survey, 2018.

Deloitte Insights | deloitte.com/insights

Explore the data further in the **Global Human Capital Trends app**.

Fears over employee privacy appear justified. Beyond the sheer quantity of data some organizations have amassed, the mere existence and possession of sensitive data creates risk, regardless of volume. One employer, for instance, installed body heat detectors at desks to track how many hours people spent in the office. Employees reacted with outrage, swamping managers with complaints and leaking unflattering stories to the media.

Many employees fear that sensitive data may be vulnerable to high-profile cyberattacks—again with good reason. While 75 percent of companies understand the need for data security, only 22 percent have excellent safeguards to protect employee data.[8] Research also shows that the 30 percent of companies that do not consider people data worth the exposure to data risk have no strong data governance structures at all.[9]

Emerging concerns about AI, algorithms, and machine-driven decisions

Data security is a long-standing risk, but there are new risks as well. Some experts worry that algorithms and machine-based decisions could actually perpetuate bias due to flaws in the underlying data or the algorithm itself. Understanding the potential for this type of risk is critical to preventing a new source of bias from seeping into an organization's hiring or promotion processes.

The marriage of people data and algorithm-based artificial intelligence (AI) raises such concerns to a new level. Just as people may never know why a certain advertisement pops up on their Web browser, business leaders are beginning to realize that "data-driven decisions" are not guaranteed to be understandable, accurate, or good.

Even advanced technology companies like Facebook and Twitter have discovered that AI without humans can be "stupid."[10] In response, they are hiring thousands of people to monitor their AI-based social networking and advertising algorithms.[11] HR organizations must be rigorous in monitoring "machine-related" decisions to make sure they are reasonable and unbiased.

Tech leaders are beginning to invest more resources in solving these problems. A consortium of data experts recently formed the Partnership on AI to Benefit People and Society, a group funded by Amazon, Apple,[12] Facebook, Google, IBM, and Microsoft. This group was established specifically to study and formulate leading practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society.[13] Ginny Rometti, the CEO of IBM, has also laid out a set of ethical principles for the use of data and AI.[14]

Staying on the right side of the tipping point

Despite the potential risks, the promise of people analytics remains too valuable for organizations to pass up. For example, GE, Visa, IBM, and others are developing a suite of analytics tools that find "non-obvious" job candidates and recommend training.[15] GE's HR analytics team is using data that tracks the "historical movement of employees and relatedness of jobs" to help employees identify potential new opportunities across the company—regardless of business unit or geography.[16] To boost productivity, Hitachi Data Systems uses smart badges to identify behaviors that contribute to employee happiness and performance, leveraging this data to rearrange workspaces and teams.[17]

We predict explosive growth in the coming year for smart products that leverage employee data. The spectrum of risks associated with the collection, storage and use of this data can and should be effectively managed. Strategies such as anonymization and encryption can allow organizations to make effective use of people data while managing the risks associated with storing and processing various kinds of personal information.

Creating a secure organizational context

It is now clear that companies using people data and analytics, as well as vendors that provide these services, need robust policies, security, transparency, and open communication to address the associated risks. These elements should work together to create a secure organizational context for the use of people data—one that reduces the likelihood of leakage, error, and abuse.

One important aspect of managing the risk of people data analytics is to know all of the places where personal data resides. Mapping the flow of personal data to and from systems, especially when those systems are connected to analytics engines, is essential for creating transparency and installing proper protections. The use of discovery, mapping, and classification tools can help organizations classify both structured and unstructured data.

The IT, HR, and legal departments at leading organizations are collaborating to make recommendations about data risks and organizational responses. These companies have clear policies and communications that explain to employees what data is being collected and how it is being used. This helps to engage employees as informed stakeholders who understand and support the benefits of people analytics for their work and their careers.

THE BOTTOM LINE

Organizations need to understand the trade-offs involved in the accelerating collection and use of employee and workforce data. Most have good intentions in collecting and using this data, but these troves of data also raise significant risks. Companies must be vigilant about data quality, data security, and the accuracy of machine-driven decisions. While this is a relatively new challenge for HR, it is rapidly, and rightly, becoming a top priority.

Table 1. What role does the C-suite play in capitalizing on people data? How can individuals adjust?

CHRO	Tighten collaboration between HR, IT, and risk to develop and communicate a useful, secure, and transparent people data strategy. That strategy should both push the envelope in leveraging data to gain greater insight into the workforce, and effectively manage the associated risks to guard against brand damage or legal consequences. If there is not one already in place, consider using a people data contract with workers to establish clear expectations of how data will be used.
CIO	Understand the flow of people data internal and external to the organization, and put the right security and IT controls in place to effectively manage the risk of the data falling into the wrong hands. Given how rapidly cyber risk is evolving, this is an area where ongoing monitoring and constant innovation is key.
Chief operations officer	Proactively review where automation is driving decision-making, and consider ways to put "humans in the loop" to help make sure that the right decisions are being made—especially as they relate to key operational processes.
Chief risk officer	Get and stay involved. You play a critical role in protecting your organization from people data-related risks, from implementing appropriate protections to tracking regulatory changes to identifying potential privacy issues.
Chief marketing officer	Constantly monitor both employee and consumer sentiment about how your organization is handling data. Because of people data's potential negative impact on brand, it's important for you to provide insights on where policies or actions should change to help avoid brand damage.
Individuals	Decide what kinds of data you are comfortable sharing with your employer, considering both potential benefits and privacy concerns. Protect your personal data by monitoring your social media profiles so that your data is being presented the way in which you want it to be.

Source: Deloitte analysis.

ENDNOTES

1. Bersin, Deloitte Consulting LLP, High-impact people analytics research, 2017.

2. Madhura Chakrabarti, *The people analytics maturity model*, Bersin, Deloitte Consulting LLP, 2017.

3. Madhura Chakrabarti, *Seven top findings for driving high-impact people analytics,* Bersin, Deloitte Consulting LLP, 2017.

4. Bersin, Deloitte Consulting LLP, *Predictions for 2018: Embracing radical transparency*, 2018.

5. Josh Bersin, conversations with vendor executives.

6. The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. EU Publications, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," accessed March 8, 2018.

7. Cheryl O'Neill, "GDPR Series, part 4: The penalties for non-compliance," Imperva, March 14, 2017.

8. Bersin, Deloitte Consulting LLP, High-impact people analytics research, 2017.

9. Mary Young and Patti Phillips, *Big data doesn't mean 'Big Brother': Employee trust and the next generation of human capital analytics*, The Conference Board, 2016.

10. Christopher Mims, "Without humans, artificial intelligence is still pretty stupid," *Wall Street Journal*, November 12, 2017.

11. Ibid.; Todd Spangler, "Mark Zuckerberg: Facebook will hire 3,000 staffers to review violent content, hate speech," *Variety*, May 3, 2017; Benjamin Mullen, "Twitter is hiring people with 'newsroom backgrounds' as real-time curators," Poynter, June 18, 2015.

12. *Global Human Capital Trends 2018* is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc.

13. Partnership on AI to Benefit People and Society, "Goals," accessed March 8, 2018.

14. Larry Dignan, "IBM's Rometty lays out AI considerations, ethical principles," ZDNet, January 17, 2017.

15. Andrew McIlvaine, "GE is reinventing talent management," *Human Resource Executive*, September 14, 2017.

16. Josh Bersin, conversations with GE executives, November 2017.

17. Josh Bersin, conversations with Hitachi executives; AI Business, "Hitachi developing AI to improve workforce efficiencies," September 28, 2015.

Deloitte. Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Junko Kaji, Karen Edelman, Abrar Khan, Nikita Garia, Matthew Budman, Rithu Thomas, Preetha Devan
Creative: Sonya Vasilieff, Molly Woodworth
Promotion: Amy Bergstrom, Alex Kawecki
Artwork: Traci Daberko

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.