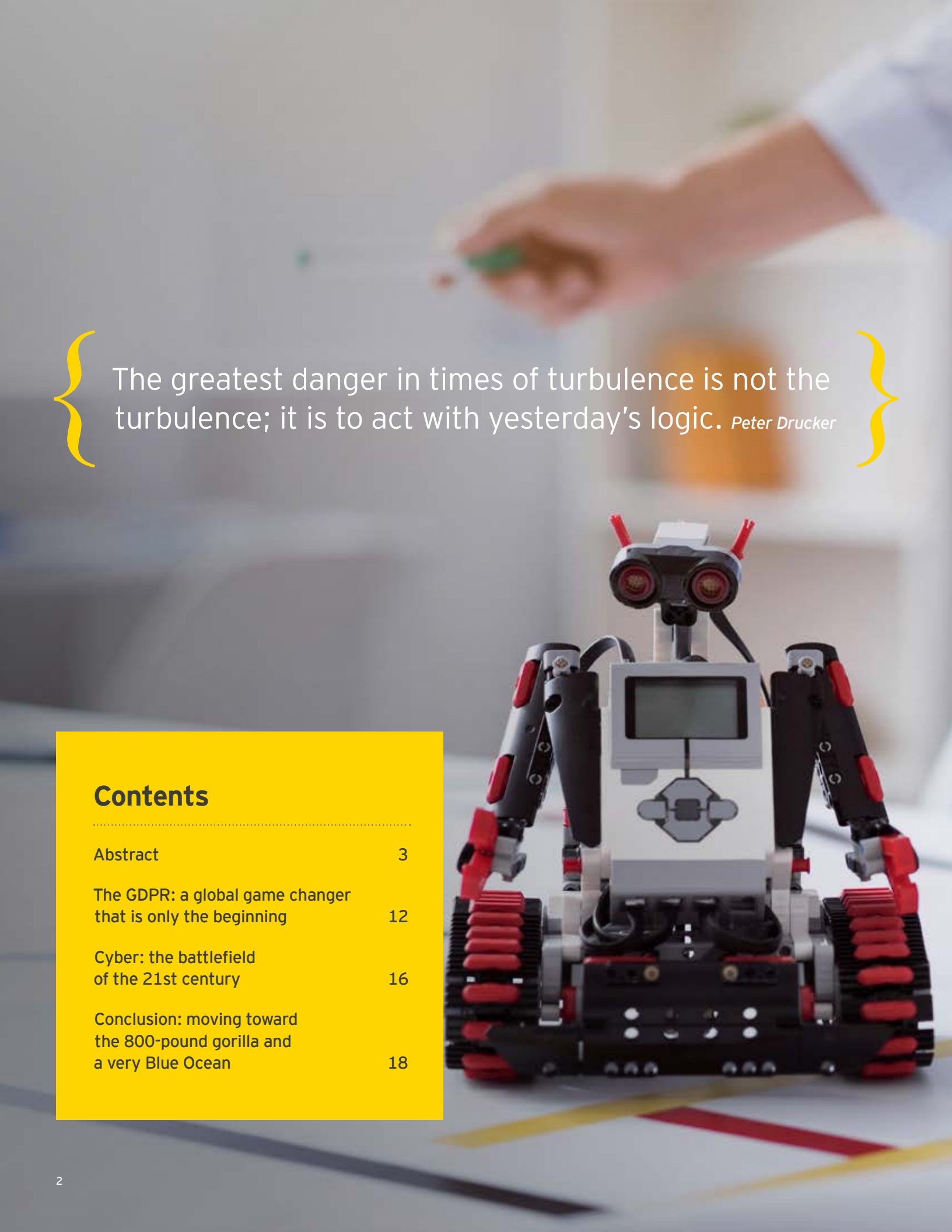
Blockchain in action

Enabling data protection, compliance and workforce growth

Contributors: Tim Aldrich and Jarrett Bunnin

EY
Building a better working world



> The greatest danger in times of turbulence is not the turbulence; it is to act with yesterday's logic. *Peter Drucker*

Contents

Abstract

The 21st century is increasingly proving to be a time of disruption. This disruption spans across different markets and industries, across traditional social and cultural divides, and indeed beyond usual political organization, regulations and bylaws. Technological innovations are at the heart of this, and its pace is staggering, leaving people, companies and governments scrambling to keep up with the change.

The revolutionary concept of big data and the explosion of smartphone technology have created threats to individuals, businesses and states alike. Personal and enterprise data is increasingly susceptible to breach and theft, as mass data breaches in large companies have shown in recent years. Due to this, the way data is managed and stored must be reassessed to safeguard peoples, businesses and states against threats and to prevent similar mass breaches in the future.

This paper argues that an approach implementing a blockchain-enabled data storage and management system is the way forward for companies seeking to combat new-age cyber threats, but also because it can comply with proliferating data protection laws, as well as attract the new generation of workers.

As the 21st century approaches its third decade, it is clear that we are living in a century unlike any before. We have made remarkable advances in technology in the seven decades since the end of World War II. The changes we continue to see across every spectrum of life — technology, industry, the labor force, the climate — are happening at an increasing rate. And they are unparalleled.

Technological innovation and digitization have caused a radical reordering of traditional industry boundaries and have blurred the lines of demarcation between peoples, cultures and economies. Now, we are, and forever will be, living and competing in a world of sectors without borders.[1]

Two of the most pervasive and important advancements contributing significantly to the breaking down of physical and artificial borders have been in the mass production of smart-device technology and in big data analytics and storage.

For individuals, ever faster, smaller and cheaper semiconductor chips have brought an explosion of smartphone technology that has shrunk the world while enabling the seamless transborder flow of information. For private companies, governments and international organizations, the development of big data storage and analytics has meant faster and leaner decision-making, strategic posturing and innovation. It has enabled companies to institute more effective growth initiatives while reducing costs.

While both innovations — smartphone technology and big data storage and analytics — have contributed much to the world, they have also introduced new threats. The data that is captured by personal smart devices and enterprise customer relationship management (CRM) systems for storing B2B-critical and personal employee data is open to breach, theft and manipulation. In recent years, hackers have gained access to information at numerous companies spanning plethora of industries.These attacks, and numerous government breaches as well, make it clear that this type of threat to the protection of our personal data is no longer an anomaly,[2] it is the new normal.

In its year-end report, Eurasia Group, a leading Geopolitical Risk consultancy, recently proclaimed cyber attacks the second-greatest global risk going into 2018.[3] Numerous other technology and management consultancies consider this threat the preeminent one.[4] At this pivotal juncture, the dawn of what Klaus Schwab, and others have called the "Fourth Industrial Revolution," protecting individual, company and government data is critical.

In fact, as the world shifts toward full digitalization across several industries in the coming years, protecting our data will be paramount. Companies that rely on Enterprise Resource Planning (ERP) software for data storage are ill-equipped to confront the vast landscape of cyber threats, which happen with frightening frequency. Recent mass attacks on governments and companies

[1] Venkat Atluri, Miklos Dietz, and Nicolaus Henke, "Competing in a world of sectors without borders," McKinsey Quarterly, July 2017, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/competing-in-a-world-of-sectors-without-borders?cid=other-eml-ttn-mkq-mck-oth-1712.

[2] Taylor Armerding, "The 16 Biggest Data Breaches of the 21st Century," CSO, October 11, 2017, https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html.

[3] Ian Bremmer and Cliff Kupchan, "Top Risks: 2018," Eurasia Group, January 2, 2018, https://www.eurasiagroup.net/files/upload/Top_Risks_2018_Report.pdf.

[4] "Cybersecurity regained: preparing to face cyber attacks: 20th Global Information Security Survey 2017-18," EY, http://www.ey.com/Publication/vwLUAssets/eycybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurityregainedpreparing-to-face-cyber-attacks.pdf and "EY Center for Board Matters: Board Agenda 2018," EY, http://www.ey.com/Publication/vwLUAssets/ey-top-priorities-forusboards-in-2018/$FILE/ey-top-priorities-for-us-boards-in-2018.pdf and Arul Elumalai, Kara Sprague, Sid Tandon, Lareina Yee, "Ten Trend Redefining Enterprise IT Infrastructure," Mckinsey & Company, November, 2017, https://www.mckinsey.com/business-functions/ strategy-andcorporate-finance/our-insights/ten-trends-redefining-enterprise-it-infrastructure.

have ranged from the more sophisticated distributed denial of service (DDoS) to more basic "spear phishing" tactics. DDoS can be said to be the intentional paralyzing of a computer network by flooding it with data. Spear phishing uses scam emails to gain unauthorized access to sensitive information and is by far and away the most common reason for large data breaches.

These omnipresent threats to one's personal data on a social or traditional enterprise level clearly necessitates a shift from ERP/CRM data management to something more individually centered. This will benefit both individuals and employers alike, yet there are significant other variables that come into play when arguing for a transition of this type. Those ranging from the movement to "gig," or freelance, work, to new data protection regulations, to having the ability to attract top talent who want different things than past generations out of their work, to being able to run a lean, agile business. Together, they make a real case to drive systemic change in the ways companies store and manage their employees' data. This paper seeks to elaborate on those areas and in doing so, illustrate the importance of this shift in data storage management.

> "If time heals all, then that is because it changes even more."

As American novelist Ellen Glasgow reminds us, all change is not growth, as all movement is not forward. But if companies move toward an individually focused data management and storage system involving blockchain's decentralized ledger technology, then they will be changing, growing and moving forward all at the same time.[5] A blockchain-enabled data storage solution is arguably the most secure system available, given the immutable nature of blockchain. Such a solution would also be compliant with the EU General Data Protection Regulation (GDPR), which becomes enforceable on May 25, 2018.

Make no mistake, regulatory initiatives like the groundbreaking GDPR will be a global game changer for companies' storage and maintenance of data in the years to come, as traditional ERP/CRM systems will continually be challenged by the concept of personal

[5] "Vision 2020+," EY, September, 2017, pp. 25, https://share.ey.net/sites/vision2020/Toolkit%20One/Vision%202020+%20partner%20overview%20document,%20September%202017.pdf.

data protection and employees who seek right to erasure, notice obligation, rights of access, rectification, right to object, as well as pseudonymization.[6] Moreover, it is without a doubt only the beginning in what will likely be more codified data regulation in the coming years, and undoubtedly further regulation will pose a significant agility problem for companies who are slow to conform to the changing nature of the times. The US is on the list of countries that have not yet enacted a data privacy law, but there have been efforts at forging similar legislation as the GDPR in recent years[7]; indeed, there are similar efforts underway in many countries.

The need for such regulations will only grow, and so will the desire of individuals to manage their own data, largely due to continued technological disruption, cyber threats, workplace innovations and a changing labor force. To be sure, it will not be a facile task to change how a company stores and manages its data, but it will be required of companies if they are to keep up with the pace of disruption and innovation caused by the fourth industrial revolution as well as against cyber risks. This revolution, whether you describe it as the Fourth Industrial Revolution or the "Digitalized Third Industrial Revolution,"[8] has vast potential to disrupt traditional labor markets,[9] while at the same time fundamentally change the way we manage, power, and move economic activity.[10] Duly, "This fundamental technological transformation in the way economic activity is organized and scaled portends a great shift in the flow of economic power from the few to the multitudes and the democratization of economic life."[11] At its very core, this epiphenomenal changing of one era to the next purports that mass job loss for humans will occur thanks to the hybrid fusion of technologies that is blurring the lines between the physical, digital, and biological spheres. It is, when compared with previous industrial revolutions, without precedent and is evolving at an exponential rather than linear pace. Furthermore, it is disrupting almost every industry in every country whilst the breadth of these disruptions announce the transformation of entire systems of production, management, and governance.[12]

Professor Schwab lists four main effects that the revolution has on business: customer expectations, product enhancement, collaborative innovation and organizational forms. While the first three are in and of themselves intriguing, it is the last one that is most relevant to understanding the need for companies to move to a personally managed, blockchain-oriented data storage system for employees and, potentially, areas of the company beyond HR. Companies' transformation to fully digitalized enterprises is well underway, while the modern organizing of labor is not concentric anymore but rather divergent; the gig economy is well and truly upon us. Both of these subtenets of the last of the main effects that the Fourth Industrial Revolution has on business prescribe forward-thinking action by companies, particularly when it comes to managing their data appropriately and safely.

The digitalization reason is perhaps obvious enough as to why organizations need to better safeguard and store their data, yet the gig economy perhaps not as much so. New technologies are changing the way we work. Technology-enabled platforms combine both demand and supply to disrupt existing industry structures, creating entirely new ways of consuming goods and services. In addition, they lower the barriers for businesses and individuals to create and acquire wealth, altering the personal and professional environments of workers. Rendered by things such as smartphones, big data, intangible assets and the improvement of conventional technologies such as MPUs, these platform businesses are rapidly multiplying into many new services, affecting nearly everything we do — from laundry to shopping, from chores to parking, to travel and massages.[13]

---

[6] Cedric Burton, Sarah Cadiot, Laura De Boel, Sára G. Hoffman, Christopher Kuner and Anna Pateraki, "The Final European Union General Data Protection Regulation," Bloomberg Law, February 12, 2016, https://www.bna.com/final-european-union-n57982067329/.

[7] "H.R.3806 – Personal Data Notification and Protection Act of 2017," U.S. House of Representatives, September 18, 2017, https://www.congress.gov/115/bills/hr3806/BILLS-115hr3806ih.pdf.

[8] Jeremy Rifkin, "The 2016 World Economic Forum Misfires With Its Fourth Industrial Revolution Theme," HuffPost, https://www.huffingtonpost.com/jeremy-rifkin/the-2016-world-economic-f_b_8975326.html.

[9] Klaus Schwab, "The Fourth Industrial Revolution," Foreign Affairs, December 12, 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

[10] Jeremy Rifkin, "The 2016 World Economic Forum Misfires With Its Fourth Industrial Revolution Theme," HuffPost, https://www.huffingtonpost.com/jeremy-rifkin/the-2016-world-economic-f_b_8975326.html.

[11] Jeremy Rifkin, "The 2016 World Economic Forum Misfires With Its Fourth Industrial Revolution Theme," HuffPost, https://www.huffingtonpost.com/jeremy-rifkin/the-2016-world-economic-f_b_8975326.html.

[12] Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum, January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[13] Klaus Schwab, "The Fourth Industrial Revolution," Foreign Affairs, December 12, 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

There is much research to support the claim that the labor force as we know it is swiftly transforming. An August 2017 study of nine Fortune 500 firms found that over the previous year, the number of projects sourced via online freelancing platforms increased by 26%.[14] Further back, a 2010 report predicted this shift as well, detailing 20 trends that would shape the coming decade. Listed at number 14 was "Work Shifts from Full-time to Free Agent Employment." The report asserted that, "Over the next decade, the number of contingent employees will increase worldwide. In the U.S alone, contingent workers will exceed 40% of the workforce by 2020 … self-employment, personal and micro business numbers will increase … government will misclassify workers, creating a major issue for companies of all sizes … work classification and work style will emerge as a target of intense political debate."[15]

[14] Mark Weinberger, "3 ways innovation can build a more inclusive world," World Economic Forum Agenda, January 16, 2018, https://www.weforum.org/agenda/2018/01/here-are-3-ways-we-can-use-technology-to-create-jobs.

[15] "Intuit 2020 Report: Twenty Trends That Will Shape The Next Decade," Intuit, October, 2010, http://http-download.intuit.com/http.intuit/CMO/intuit/futureofsmallbusiness/intuit_2020_report.pdf.

The research is proving to be very intuitive, indeed. As of late 2017, there were 57 million freelancers/contractual workers in the US,[16] with total employment numbering 154,430,000,[17] which is 37% of the total workforce. These 57.3 million Americans also contribute a significant amount to the US economy. In 2017, it was $1.4 trillion, nearly 30% higher than in 2016. It is highly likely that the report's prediction will come to fruition. In fact, the 40% dictum is not a finality but rather only the beginning, if we are to believe findings that by 2027 the majority of US workers will be freelance.[18] Work by Alan Krueger and Lawrence Katz has shown similar results in their analysis of the proportion of U.S. workers engaging in what they refer to as 'alternative work'. From 2005 to 2015, the proportion of Americans workers engaged in what they

[16] "Freelancers predicted to become the U.S. workforce majority within a decade, with nearly 50% of millennial workers already freelancing, annual "Freelancing in America" study finds," Upwork, October 17, 2017, https://www.upwork.com/press/2017/10/17/freelancing-in-america-2017/.

[17] "United States Labor Force Statistics Seasonally Adjusted (in thousands) 1978 – Present," Bureau of Labor Statistics, http://www.dlt.ri.gov/lmi/pdf/usadj.pdf.

[18] "Freelancers predicted to become the U.S. workforce majority within a decade, with nearly 50% of millennial workers already freelancing, annual "Freelancing in America" study finds," Upwork, October 17, 2017, https://www.upwork.com/press/2017/10/17/freelancing-in-america-2017/.

refer to as "alternative work" jumped from 10.7% to 15.8%. They found that 94% of net job growth over the past decade was in the alternative work category, and over 60% was due to the rise of independent contractors and freelancers.[19]

To be sure, all of this research was focused on the US labor force, but there is a growing market for digital gig work globally, thereby creating similar freelance opportunities for workers in places like sub-Saharan Africa, India, China and South America.[20] The movement is truly global, and it is here to stay.

What's more, the labor force(s) of the world are shifting to fit the mindset of the dominant generation of the workforce, millennials. They now make up the largest percentage of workers in the US labor force, as they will soon do in many countries around the world, as Gen Xers enter their retirement-eligible years.[21] Companies must adapt and adjust accordingly. Simply put, what matters to millennials, in their lives and careers, differs from what matters to baby boomers or Gen Xers.

These workers present companies with a set of challenges that are different from those of prior generations. A sobering study by Software Advice, detailed by the Society for Human Resource Management, shows that millennials bring a new set of cybersecurity challenges for firms and organizations, because many try to work using their own technology (e.g., smartphones and consumer-grade software solutions). While some employers may find this an admirable attempt to multi-task and be constantly in communication with colleagues and their own personal work projects, doing this can create a cybersecurity threat when questionable applications, devices and tools are used to handle proprietary or otherwise sensitive company data.[22]

While securing remote access through VPNs or other applications may be one method for companies wishing to avoid these perils, having a blockchain-enabled personal data storage system for employees could avoid proprietary loss of information altogether due to the sophisticated mining procedures that are needed to verify and extract data from the ledger, as well as allowing for a more seamless interface between workplace devices and personal devices.

Aside from this strategic challenge, millennials "… want it fast and want it now,"[23] but perhaps even more than instant gratification, they want great experiences.[24] Not only on a vacation that will give them social media fodder to post about but increasingly in the workplace; so how do companies give that to them? One way could be through better management systems, not only for clients (CRMs), but for themselves as well. A 2016 Harvard Business Review report details that millennials are likely to change jobs more often than previous generations. They see quality of management as more important than factors such as compensation, the type of work, the room for growth and advancement, or even having a fun, hospitable working environment.[25] Millennials clearly want an improved consumer-grade experience from their technology at work; almost half of them expect to be able to complete key transactions with their business software from a tablet or mobile device.[26] However, aside from attracting the largest portion of the workforce, there are other tangible realities that firms, organizations, and small businesses must understand. The report emphasized that user experience with business technology is becoming critical not just to recruiting and retaining millennials, but to anyone who expects the software they use at work to be "mobile-friendly, flexible, simple and easy to use."[27]

---

[19] Lawrence F. Katz and Alan B. Krueger, The Rise and Nature of Alternative Work Arrangements in the United States, 1995-2015, Working Paper, Princeton University, pp. 1-47, September, 2016, http://dataspace.princeton.edu/jspui/bitstream/88435/dsp01zs25xb933/3/603.pdf.

[20] Vili Lehdonvirta, "Where are online workers located? The international division of digital gig work," The iLabour Project, July 11, 2017, http://ilabour.oii.ox.ac.uk/where-are-online-workers-located-the-international-division-of-digital-gig-work/.

[21] Richard Fry, "Millennials surpass Gen Xers as the largest generation in U.S labor force," Pew Research Center, May 11, 2015, http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/.

[22] Karl W. Hardy, "Millennials Bring New Workplace Cybersecurity Challenges," July 12, 2016, https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/millennials-bring-new-workplace-cybersecurity-challenges.aspx.

[23] Christine Barton, Chris Egan, and Jeff From, "The Millennial Consumer: Debunking Stereotypes," The Boston Consulting Group, April, 2012, https://www.bcg.com/documents/file103894.pdf.

[24] "Best of Money: Why millennials go on holiday instead of saving," Financial Times, February 12, 2016, https://www.ft.com/content/94e97eee-ce9a-11e5-831d-09f7778e7377.

[25] Amy Adkins and Brandon Rigoni, "What Millennials Want from a New Job," Harvard Business Review, May 11, 2016, https://hbr.org/2016/05/what-millennials-want-from-a-new-job.

[26] Jody Kaminsky, "What Millennials Expect from Workplace Technology and What It Means for Business Software Buyers," Oracle NetSuite, August 31, 2015, http://www.netsuiteblogs.com/what-millennials-expect-from-workplace-technology-and-what-it-means-for-business-software-buyers.

[27] Jody Kaminsky, "What Millennials Expect from Workplace Technology and What It Means for Business Software Buyers," Oracle NetSuite, August 31, 2015, http://www.netsuiteblogs.com/what-millennials-expect-from-workplace-technology-and-what-it-means-for-business-software-buyers.

Employers need to know and act on the factors that make their company appealing to millennials. They have to make it easy for prospects to choose them over the competition.[28] Giving data rights and ownership to the individual would be of significant benefit to companies wishing to stay ahead of the game in this era of seemingly continual disruption, industry convergence, and changing regulations. It could be a key driver of employee retention, and it would appeal to gig workers because it would help them maintain flexibility in their job choices rather than having to stay with any one company for too long. This is because, in theory, giving individual data ownership would simplify HR processes of leaving or joining a company.

On the other hand, it could also potentially be a crucial factor in keeping these contracting employees more accountable, because said protection and maintenance of their own data could be tied to certain benefits while they are with a company, such as bonuses, short-term health coverage, or further professional development opportunities. Particularly, as the GDPR comes into full effect in May 2018, one could argue that companies would see an ERP service giving individual data management to employees a much more attractive thing. This will be explored further in the next section. But aside from the above, having this particular enterprise data storage system could also serve as a competitive advantage toward winning contracts and/or working in emerging markets, due to the gig economy flourishing in these places and employees finding it more attractive than traditional cumbersome ERP software.[29]

Companies that offer Data as a Service (DaaS) could attract new engagements with businesses, organizations and governments, particularly in the developing world, due to the burgeoning growth in digital contractual working. Governments, notably, could see personal data protection tools as a significant driver of growth on a GDP level. Numerous nations that are forward-thinking in emerging markets — e.g., India, China, Kenya, South Africa, Colombia, Mexico and Gulf states such as the UAE — have already implemented policies that enable workers as opposed to limiting them. A DaaS solution such as the one described here would facilitate governments' efforts to reduce difficulties for workers, increasing output in hours worked per employee by eliminating the organizational deficiencies produced by a large employee data management system. Companies that switch to a blockchain-enabled method of data storage and management will ultimately drive commerce and growth in their respective countries. This is because we know that while productivity isn't everything, in the long run it is almost everything.[30]

Additionally, with the new GDPR requirements looming and others sure to follow, having a highly secure data storage solution helps to protect companies from noncompliance penalties, which can hurt not only the companies but the countries in which they reside.

Under the new GDPR requirements, countries that do business with European-based companies must abide by the laws set down by the act, as it is extraterritorial in nature. The regulations will apply to companies of all sizes, while enforcement of the new data privacy regulations will be overseen by the European Data Protection Board. This authority will have sweeping power, abundant resources and an EU secretariat in Brussels to oversee that businesses comply with the new policies.

Organizations of all types and sizes must maintain regulatory compliance while striving to stay agile and lean. Agility is as essential for a 21st century company as it is for athletes of all types and sizes. Agile business transformation is characterized by three elements: responsiveness, insightfulness and efficiency.[31] So, for companies wishing to be at the forefront of functional workforce management, retention and economic growth for the countries within which they reside, creating a modern work experience and enabling employees through technological empowerment so as to be as effective and engaged as possible in their jobs is vital.[32]

---

[28] Amy Adkins and Brandon Rigoni, "What Millennials Want from a New Job," Harvard Business Review, May 11, 2016, https://hbr.org/2016/05/what-millennials-want-from-a-new-job.

[29] Vili Lehdonvirta, "Where are online workers located? The international division of digital gig work," University of Oxford: The iLabour Project, July 11, 2017, http://ilabour.oii.ox.ac.uk/where-are-online-workers-located-the-international-division-of-digital-gig-work/.

[30] Paul Krugman, The Age of Diminished Expectations (Cambridge: MIT Press, 1997), pp. 1 – 232.

[31] "Can agile finance provide fuel to drive your business forward?" EY, http://www.ey.com/Publication/vwLUAssets/ey-agile-finace-2.0/$File/ey-agile-finance-2.0.pdf.

[32] Jacob Morgan, "Forget Enterprise Grade Technology, Consumer Grade Technology is the Future," Inc.com, December 1, 2017, http://www.ey.com/Publication/vwLUAssets/ey-agile-finace-2.0/$File/ey-agile-finance-2.0.pdf.

Consumer technologies are quickly becoming enterprise technologies, and there are several examples of this taking place in the workplace already. G-Suite, consumer-grade CRM systems are becoming normalized in company environments, while business applications mimicking social media platforms that connect employees are ever more popular. These consumer-grade applications that function as business enterprise systems as well are usually more effective, more modern and more user-friendly.[33] Agility, conformity with new policy regulations, lean enterprise systems — all of this necessitates a shift toward an individualized data management and storage system. However, from a legal perspective, the new regulations set forth by the GDPR requirements will influence companies in a much more direct manner in terms of pushing them toward new systems, strategies and methods of enterprise management in order to avoid the penalties that come with noncompliance. The next section will review the new GDPR data privacy requirements and discuss how this pertains to companies needing to shift their data storage and management systems to a format that is more compatible with the macro trends that the 21st century are moving toward.

[33] Jacob Morgan, "Forget Enterprise Grade Technology, Consumer Grade Technology is the Future," Inc.com, December 1, 2017, http://www.ey.com/Publication/vwLUAssets/ey-agile-finace-2.0/$File/ey-agile-finance-2.0.pdf.

The GDPR: a global game changer that is only the beginning

Much of the key debate surrounding what implementation of the GDPR will mean for companies and their organizational goals/strategies has been focused on data security and data privacy. Yet, businesses and consumers alike will soon come to realize that the complex issue of *data ownership* is at least as important if not more so than this.[34] The French have had a law protecting the rights of individuals to own their data and to use it as they please since 1978. In fact, it was the precursor to the first EU-wide law protecting individuals' data rights, the 1995 European Union Directive 95/46/EC on personal data protection, which is in turn, the precursor to the GDPR. The French law stipulates that personal data must be collected and processed fairly and lawfully for specified, explicit and legitimate purposes, and with the consent of the data subject. Additional rights given to data subjects are: the right to be informed, the right of access, the right to object, the right to be forgotten and the right to correct and delete information.[35]

The French law has had much success in safeguarding the data rights of individuals over the years (though, curiously, not for children), with the most recent adjudication for breach of privacy rights coming in 2014.[36] France has attempted to lead the way for countries in the domain of privacy rights vs. protecting state security, and sometimes the lines of demarcation between them are not so clear, which has attracted scrutiny and criticism. The 2015 passing of France's draft law on sweeping surveillance measures for international electronic communications, which was enacted shortly after the Paris terrorist attacks on the Bataclan theater and other places around the city, was one of these heavily scrutinized bills. It will likely be overturned by the European Court of Justice in a case pitting it against the new EU-wide GDPR.

The GDPR is expected to be so sweeping that soon the French laws may be irrelevant and without jurisdiction. For example, the 1978 law has also been amended several times so as to be in line with new directives set forth by the EU commission, and is therefore in question to be rendered obsolete once the new GDPR requirements come into effect. This is particularly true because many of these measures that were considered groundbreaking at the time are in the new legislation and would have broader arbitrating reach than the French law, as the former is extraterritorial in nature while the

[34] Ciaran Dynes, "Data Ownership: Time to start reading those T&Cs," Data-Informed, October 3, 2017, http://data-informed.com/data-ownership-time-to-start-reading-those-tcs/.

[35] "Online Privacy Law: France," The Law Library of Congress, April, 2012, https://www.loc.gov/law/help/online-privacy-law/france.php.

[36] Marianne Le Moullec, "The French Data Protections Authority Fines Google for Breach of French Privacy Laws," Proskauer, January 31, 2014, https://privacylaw.proskauer.com/2014/01/articles/online-privacy/the-french-data-protection-authority-fines-google-for-breach-of-french-privacy-laws/.

latter has been subject to much judicial debate over its validity in cases of data privacy breach that are not on French soil.[37] To be sure, any country that is not working toward these standards is left out in the cold — GDPR has long tentacles.[38] The breadth of its stipulations, by causality, therefore affect companies as much as governments that do not take measures to abide by the new rules of the game.

France, though, cannot be said to be the only forward-thinking nation with regard to data privacy rights for individuals. In fact, the developing world is charging forward with potential regulations that could help shape the future of data rights for individuals. India, being the largest democracy in the world and having a workforce that is largely technologically adept (450 million strong, and growing, online population) can shape the future of the internet and data privacy through its policy making.[39] Its telecoms authority, for example, has recently recommended to the Government that access to the internet must not be restricted by discriminatory service providers. But more germane to this discussion as it pertains to individual data privacy, its Ministry of Electronics and Information Technology published a white paper for a Data Protection Framework for India. Prompted by the Supreme Court's verdict in the Puttaswamy case,[40] the Indian Government is now working to protect individual privacy in the digital world. While the final law will undoubtedly generate debate, the report notably makes it clear that India will balance civil liberties, security and data-led innovation.

The rest of the developing world will be following this progress in India with great interest, as its role as a developing country suggests that it will account for what matters to the global south, such as affordable access, local content generation and platform security.

So, what does the GDPR actually entail, and what should companies do to prepare for them? In December 2015, following three years of drafting and negotiations, the European Parliament and the Council of the European Union reached an informal agreement on the final draft of the EU GDPR. The main goals of the act are to reinforce the data protection rights of individuals, facilitate

[37] "Online Privacy Law: France," The Law Library of Congress, April, 2012, https://www.loc.gov/law/help/online-privacy-law/france.php.

[38] Mark Scott and Laurens Cerulus, "Europe's new data protection rules export privacy standards worldwide," Politico, January 31, 2018, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.

[39] Samir Saran, "Democratic, innovative and secure: how India can shape the future of the internet," World Economic Forum, December 12, 2017, https://www.weforum.org/agenda/2017/12/democratic-innovative-and-secure-how-india-is-vying-for-online-leadership/.

[40] Alnoor Peermohamed, Justice K S Puttaswamy: The 92-yr-old who fired the 1st shot in privacy war," Business Standard, August 25, 2017, http://www.business-standard.com/article/current-affairs/justice-k-s-puttaswamy-the-92-yr-old-who-fired-the-1st-shot-in-privacy-war-117082401108_1.html.

the free flow of personal data in the digital single market and reduce unnecessary administrative burden.[41] While the new law is undoubtedly similar in many respects to the 1995 European Data Protection Directive, its legal predecessor, there are several differences between the new and old rules. GDPR's geographic scope is much greater than the data directive. While the latter used more of a light-touch approach to data protection, setting out aims and requirements for data protections standards that were implemented through national legislation, such as the UK's data protection act, the GDPR will set strict standards of conformity for all EU nations and citizens. Furthermore, the penalties for non-compliance are increasing from €500,000 or one percent of annual turnover, to €20 million, or 4% of turnover, whichever is higher.

The specific definition of what constitutes 'personal' data is changing under the new law as well, from information used to identify individuals or their personal data to including genetic information, location and identification markers that many third party systems regularly use (such as social media companies). Companies are also held to a much higher threshold of accountability than the old directive. The GDPR imposes direct statutory obligations on data processors, whereas previously data controllers would leverage contractual details to protect themselves against data compliance risk by making it so processors would not be subject to direct enforcement or penalties from regulators. Breach notifications will now be mandatory on all organizations with respect to providing notice of personal data intrusion within a very short timeframe to the supervisory authority (Data Protection Board), or in some cases, the individuals themselves. Understandably, the intransigent differences make it important for companies to be proactive about making sure they are well prepared for the changes.

To fully comprehend the penalties for noncompliance, it is important to understand certain terms as they are defined within the GDPR. A controller is a body, alone or jointly with others, that determines the purposes and means of the processing of personal data. A processor is a body that processes personal data on behalf of the controller, and personal data refers to any information (single or multiple data points) relating to an identified or identifiable natural person such as name, employee identification number or location data.[42] These terms are imperative to clarify because the main concepts and requirements of the GDPR will undoubtedly take some time to be reconciled with the legalities of other standing litigation. In other words, there will be some confusion for firms and governments, including the oversight authorities, in terms of how to regulate the dictums set forth by it in conjoint with other laws or agencies that may have similar long-reaching powers. For example, in February 2018, regulators from the U.K.-based Financial Conduct Authority (FCA) and the Information Commissioners Office (ICO) published a joint statement recognizing the confusion that will arise due to an inherent conflict between the new laws and, for example, anti-money-laundering laws that may require governments or companies to hold information for a longer period of time.[43]

Besides these overlapping jurisdictions that still need to be ironed out for companies and regulators alike, the GDPR's concepts themselves can be at the same time lucid and difficult to grasp. The major requirements are as follows:

1. **Data protection impact assessment:** This assessment, required for high-risk personal data processing activities, can help organizations identify risks and define mitigating actions.

2. **Data privacy accountabilities:** The GDPR states that the controller is responsible for confirming that a firm adheres to the law's privacy principles.

3. **Condition for processing:** The processing of personal data must rely on a lawful basis as outlined in the GDPR.

4. **Data protection officer (DPO):** Firms that conduct large-scale systematic monitoring of EU residents' data or that process large amounts of sensitive personal data must appoint a qualified DPO.

5. **Privacy by design (PbD):** Organizations are required to establish privacy controls from the outset of product or process development.

[41] Konrad Meier and Philippe Zimmermann, "EU General Data Protection Regulation (GDPR)," EY Legal, 2016, http://www.ey.com/Publication/vwLUAssets/EY_EU_General_Data_Protection_Regulation_(GDPR)_2016/$FILE/Factsheet%20GDPR_V3_konrad_meier_new.pdf.

[42] Cindy Doe, Steve Holt, and Jeremy Pizzala, "GDPR: perspectives for global financial services firms," The Alwin Club, December 6, 2017, https://thealwinclub.ey.net/2017/december/gdpr-perspectives-for-global-financial-services-firms/.

[43] "FCA and ICO publish joint update on GDPR," Financial Conduct Authority, February 8, 2018, https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr?utm_source=POLITICO.EU&utm_campaign=248f0d768d-EMAIL_CAMPAIGN_2018_02_12&utm_medium=email&utm_term=0_10959edeb5-248f0d768d-190112185.

6. **Right to erasure:** An individual can request the deletion or removal of personal data when there is no lawful reason for its continued processing.

7. **Consent:** Consent must be freely given and explicit, indicating the individual's specific agreement to the processing of personal data.

8. **Data breach notification:** Organizations must notify the supervisory authority of a data breach within 72 hours of becoming aware of it.

9. **Data portability:** This allows individuals to move, copy or transfer personal data easily from one organization to another in a secure way for their own purposes.[44]

While most companies should be close to the implementation stage of their new GDPR compliance regulatory frameworks, concepts like pseudonymization[45] and "adequacy decisions," can potentially causes hiccups for those who are ill-prepared, particularly because adequacy decisions are made by governments on a multilateral level. So companies operating outside the EU but doing business in it may be stuck between two minds if their headquarters are based in a country that is slow to conform with the EU's regional data policies. What better way to simplify things across the board, while easily complying with the EU's directives, than giving true data ownership to the *individual*. Furthermore, smaller, developing countries would have great impetus to move toward this direction as the EU is linking trade policies and agreements to being acquiescent with the new directives.[46] For companies, belying the risk of noncompliance are large penalties, with administrative fines of up to €20million or 4% of global revenue, whichever is greater.[47] The GDPR is, without a doubt, an innovative and unique policy stance for all the reasons listed above. But perhaps its greatest contribution to society will be the way it has already changed the scope of the conversation toward data privacy on a global scale.

While it will significantly affect all companies that physically do business across all 28 EU member states, as has been noted before, its scope of power is transnational, and there have already been significant preparations made by countries seeking to maintain competitive advantage over one another.

The EU-US Privacy Shield, for example, is a transatlantic data-transfer deal that is in the works, but the main hold up towards finalizing the deal is that the Europeans seem to be having their cake and eating it too, while the US doesn't particularly like the EU flavor of choice. That is to say, the US doesn't want to be held to the EU's high degree of data protections. However, as aforementioned, the US is also looking at legislation aimed at protecting citizens' data in light of recent large-scale cyber attacks.[48]

From Finland,[49]Japan, South Africa, Colombia and South Korea, to the tiny island nation of Bermuda, more and more countries are falling into line with the data protection standards set forth by the EU, for reasons of political and financial pressure, but also from an exportation of European soft power attributed to its oversize regulatory influence on markets, countries and companies around the world.[50] "Data protection is a good example of Europe trying to extend its influence over other countries," said Christopher Kuner, co-chair of the Brussels Privacy Hub at the Vrije Universiteit Brussel. "Call it the "Brussels Effect.""[51] To be sure, the Brussels Effect is in full force as organizations see the May 25, 2018, implementation day just around the corner, and companies now more than ever need robust evaluations of their data storage and management systems to remain agile and to comply with the new regulations.

---

[44] Cindy Doe, Steve Holt, and Jeremy Pizzala, "GDPR: perspectives for global financial services firms," The Alwin Club, December 6, 2017, https://thealwinclub.ey.net/2017/december/gdpr-perspectives-for-global-financial-services-firms/.

[45] Cedric Burton, Laura De Boel, Sara Cadiot, Sára G. Hoffman, Christopher Kuner and Anna Pateraki, "The Final European Union General Data Protection Regulation," Bloomberg Law, February 12, 2016, https://www.bna.com/final-european-union-n57982067329/.

[46] Laurens Cerulus and Mark Scott, "Europe's new data protection rules export privacy standards worldwide," February 6, 2018, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.

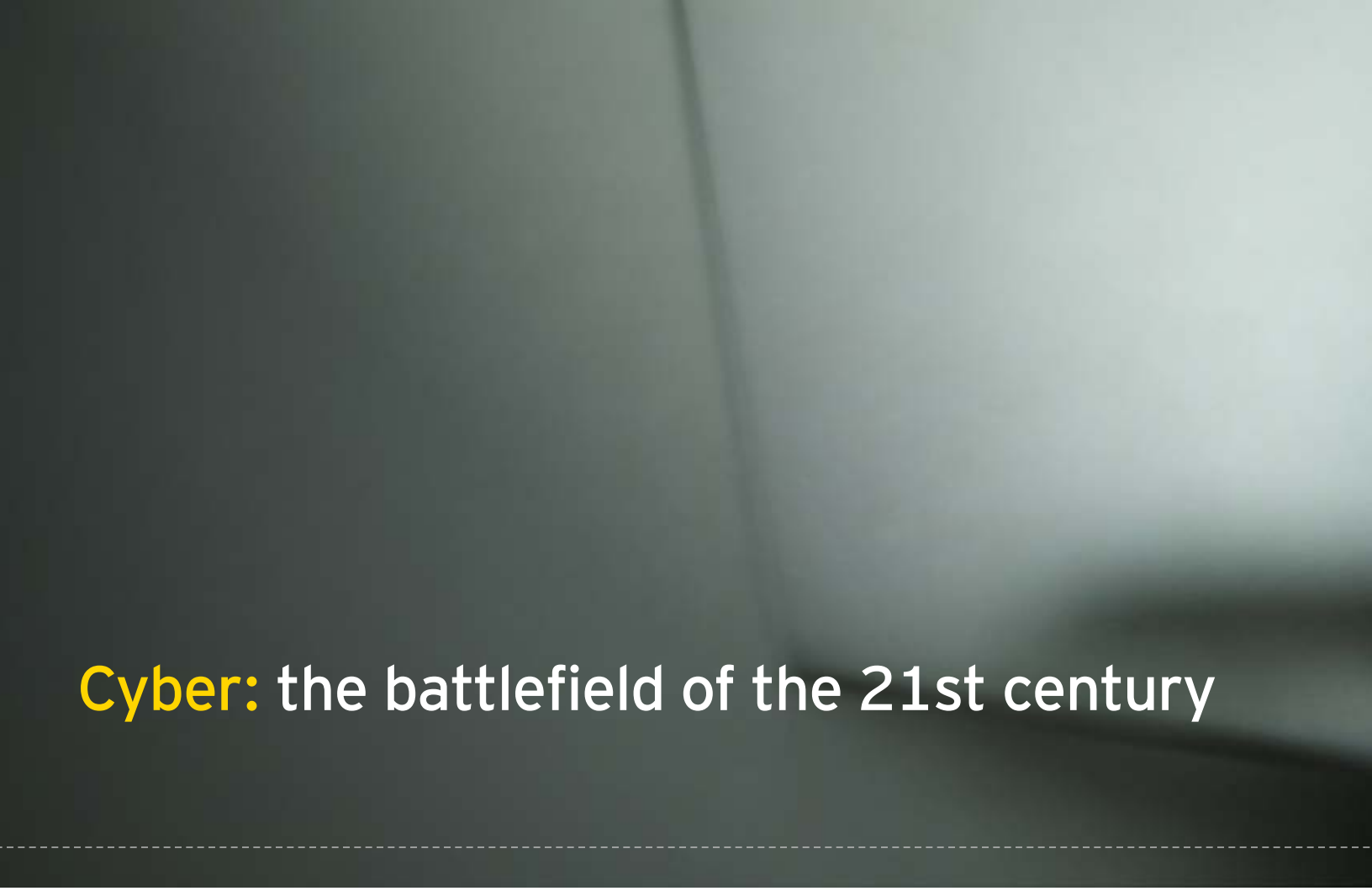
[47] Konrad Meier and Philippe Zimmermann, "EU General Data Protection Regulation (GDPR)," EY Legal, 2016, http://www.ey.com/Publication/vwLUAssets/EY_EU_General_Data_Protection_Regulation_(GDPR)_2016/$FILE/Factsheet%20GDPR_V3_konrad_meier_new.pdf.

[48] "H.R.3806 – Personal Data Notification and Protection Act of 2017," U.S. House of Representatives, September 18, 2017, https://www.congress.gov/115/bills/hr3806/BILLS-115hr3806ih.pdf.

[49] Päivi Niinimäki-Rastas, "FINLAND: Preparing to implement the GDPR," DLA Piper, July 12, 2017, http://blogs.dlapiper.com/privacymatters/finland-preparing-to-implement-the-gdpr/.

[50] Laurens Cerulus and Mark Scott, "Europe's new data protection rules export privacy standards worldwide," February 6, 2018, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.

[51] Mark Scott and Laurens Cerulus, "Europe's new data protection rules export privacy standards worldwide," Politico, January 31, 2018, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.



Cyber: the battlefield of the 21st century

Complying with the GDPR and attracting hires with new expectations of work play no small role in the need for a personal data storage and management service. Nevertheless, perhaps a more urgent reason lies in the need for protection against the increasing and persistent threat of cyber-attacks. The attacks come from various angles and numerous actors, and they strike across multiple industries. DDoS threats are expected to increase, because they are often powered by botnet "Internet of Things" (IoT) devices. By 2020, billions and billions more things (e.g., cars, thermostats, appliances and speaker systems) will be connected, though the precise number is a matter of dispute among experts.[52]

That said, a 2017 Global Cyber Threat Report indicates that attackers are forgoing sophisticated methods for more straightforward approaches.[53] Even if companies themselves are not always utilizing of IoT devices in the same manner as their employees may be in their private lives, some personnel may utilize their work devices for home use, thus presenting an external risk for the company. This is especially true as more firms worldwide shift toward flexible working arrangements that allow employees to work where networks may not be as secure as they are in the office. We need look no further than the internal survey research that EY has performed over the past several years on CFOs' and boards' concerns, as well as the preeminent Global Information Security Survey, to come to the conclusion that these asymmetric threats are of primary importance to top C-suite execs.

In a November 2017 report from EY Financial Accounting and Advisory Services, 56% of the global CFOs surveyed said that managing data security and privacy is the main challenge facing today's corporate reporting environment. And 85% of the more than 1,000 CFOs and controllers remarked that they found it either "very challenging" or "somewhat challenging" to actively manage data flows based upon different jurisdictions' privacy laws; 49% agreed with the statement that, "concerns over security and compliance risks of the cloud are seen as a major barrier to technology transformation and the implementation of innovative new technologies."[54]

[52] Amy Nordrum, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated," IEEE Spectrum, August 18, 2016, https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

[53] "Internet Security Threat Report: Vol. 22," Symantec, April, 2017, https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_.

[54] "Can innovative corporate reporting build trust in a volatile world?" EY, November, 2017, http://www.ey.com/Publication/vwLUAssets/EY-can-innovative-corporate-reporting-build-trust-in-a-volatile-world/$FILE/EY-can-innovative-corporate-reporting-build-trust-in-a-volatile-world.pdf.

"There is a high level of uncertainty among the finance community on how to approach the issues of data security and privacy," says Peter Wollmert, EY global Financial Accounting and Advisory Services leader. He argues CFOs need to have clear governance processes in place for how they look after financial information, to confirm that data is both compliant with relevant local laws and is secure — which can be a huge challenge in large and complex organizations.[55] Findings from three recent surveys appear to support that assertion. The 2017/18 Global Information Security Survey, an EY Center for Board Matters: Top Priorities for Board in 2018 survey, and one from a top consulting firm[56] show the top trends redefining enterprise IT infrastructure. They similarly show that effective cybersecurity posturing, as well as preparing and anticipating for "geopolitical and regulatory changes"[57] remain at the top of the list of global challenges and priorities for companies going forward.[58] Companies need to make sure that their technological innovation extends to their cybersecurity infrastructure.[59] Increasingly, across diverse industries, blockchain solutions are seen as the answer to protecting sensitive data that must be kept secured or verifiable in a specific place and time, as is the case with employee information.

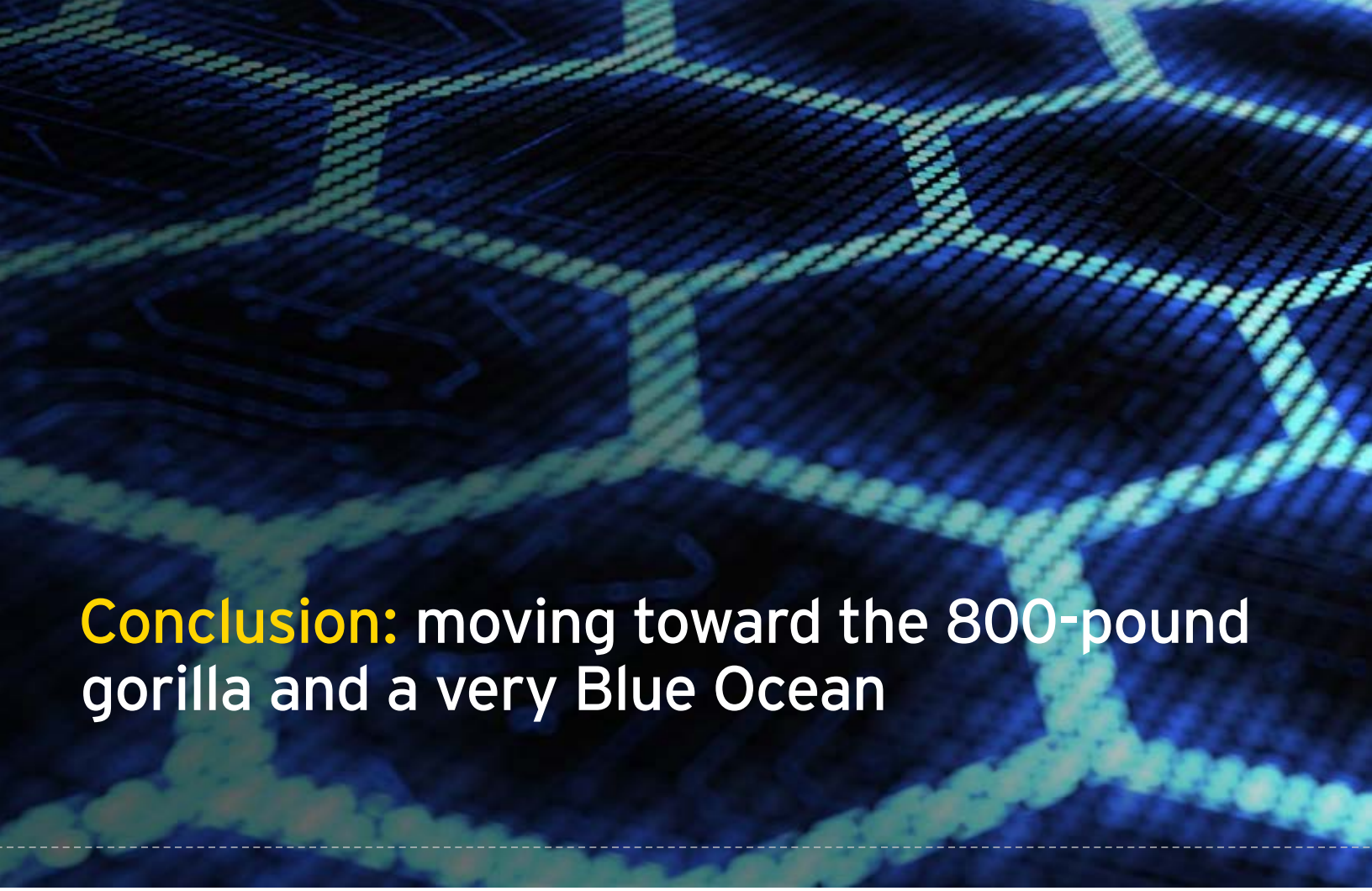
[55] "Can innovative corporate reporting build trust in a volatile world?" EY, November, 2017, http://www.ey.com/Publication/vwLUAssets/EY-can-innovative-corporate-reporting-build-trust-in-a-volatile-world/$FILE/EY-can-innovative-corporate-reporting-build-trust-in-a-volatile-world.pdf.

[56] Arul Elumalai, Kara Sprague, Sid Tandon, and Lareina Yee, "Ten Trends redefining enterprise IT infrastructure," McKinsey & Company, November, 2017, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/ten-trends-redefining-enterprise-it-infrastructure.

[57] "EY Center for Board Matters: Top Priorities for US Boards in 2018," EY, 2017, http://www.ey.com/Publication/vwLUAssets/ey-top-priorities-for-us-boards-in-2018/$FILE/ey-top-priorities-for-us-boards-in-2018.pdf.

[58] "Cybersecurity regained: preparing to face cyber attacks: 20th Global Information Security Survey 2017-18," EY, 2017, http://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf and EY Center for Board Matters: Top Priorities for US Boards in 2018," EY, 2017, http://www.ey.com/Publication/vwLUAssets/ey-top-priorities-for-us-boards-in-2018/$FILE/ey-top-priorities-for-us-boards-in-2018.pdf and Arul Elumalai, Kara Sprague, Sid Tandon, and Lareina Yee, "Ten Trends redefining enterprise IT infrastructure," McKinsey & Company, November, 2017, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/ten-trends-redefining-enterprise-it-infrastructure.

[59] Cindy Doe, Steve Holt, and Jeremy Pizzala, "GDPR: perspectives for global financial services firms," The Alwin Club, December 6, 2017, https://thealwinclub.ey.net/2017/december/gdpr-perspectives-for-global-financial-services-firms/.



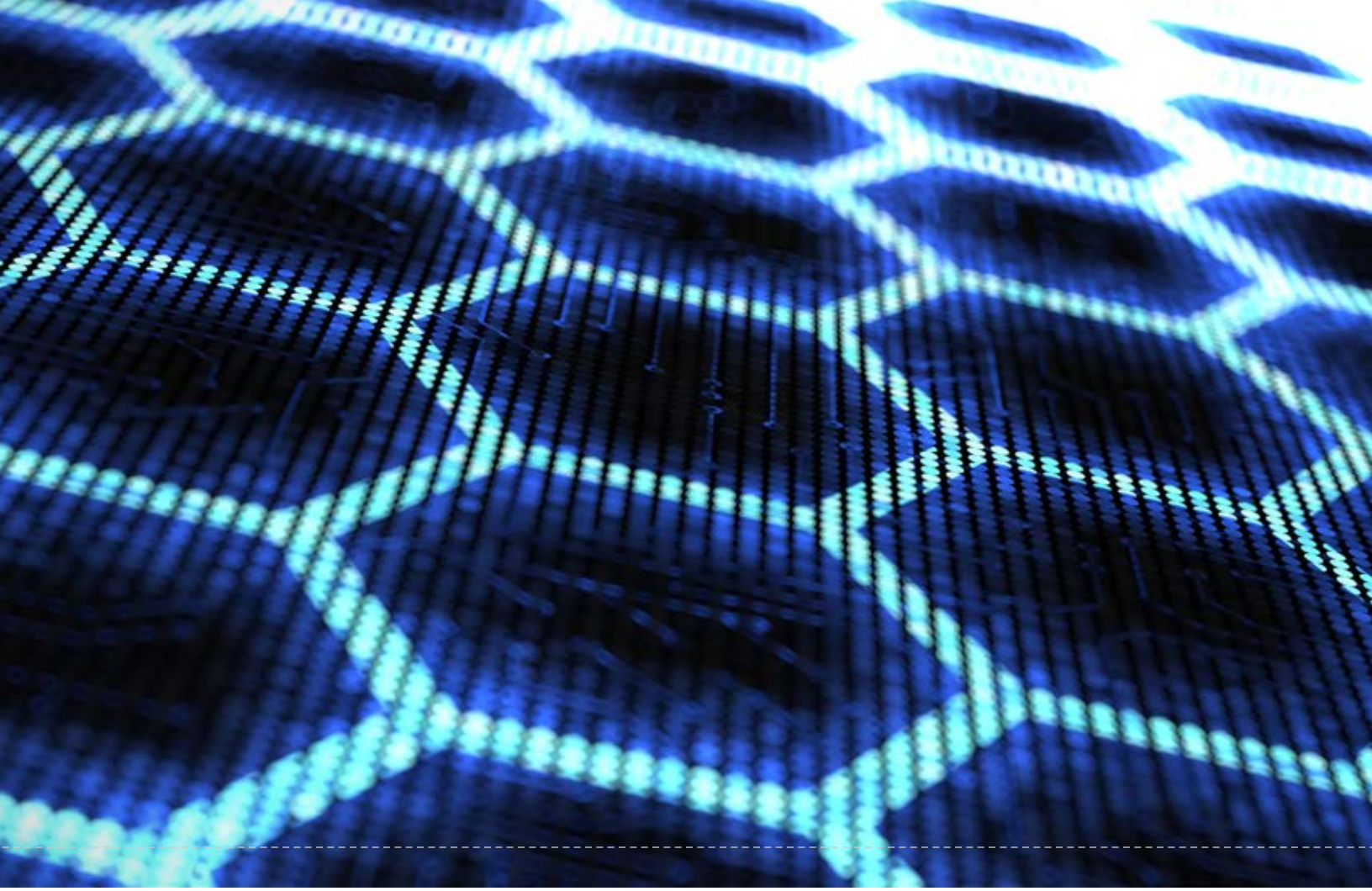
Conclusion: moving toward the 800-pound gorilla and a very Blue Ocean

The 21st century is still young, and there is no way to know with certainty how things are going to look across a variety of spectrums — from technological innovation, to societal changes, to economic performance of the global economy — in even 5 years' time, let alone 50. The age of disruption, the beginnings of the Fourth Industrial Revolution, and the emerging era of AI are seeing convergences in business as well as politics that are unprecedented and would not have even seemed possible when the first microprocessors were invented several decades ago. For businesses, being lean, agile, as well as having the ability to adapt to changing market circumstances and/or regulatory requirements is of the utmost importance. Data ownership and privacy for companies is coming under increasing scrutiny the world over, with the introduction of new frameworks, such as the GDPR, as well as changing demographics and a new mindset in the labor force. Not to mention the prevalent threat to individual and company data in the virtual realm from malicious actors. All of this necessitates a shift in how companies think of data storage and management.

The emergence of blockchain technology, secure and inviolable, has allowed for a broad range of new developments, from Fintech, to smart contracts, to renewable-energy grids, to decentralized currency transactions and peer-to-peer (P2P) lending. Now, it can be used in a manner that benefits individuals in a more direct, immediate way. The creation of a DaaS enterprise system centered on blockchain makes it possible to have a collaborative, innovative and information-sharing economy among companies. It creates an 800-pound gorilla that grows larger and larger as more companies buy into this way of managing data.[60]

"[The] blockchain difference is there is no central authority that sees all the data," says Paul Brody, EY Global Innovation Leader for Blockchain Technology. "Because the center-based model is very powerful, a lot of companies held back. With blockchains,

[60] Paul Brody, Jason Friedman, and Scott Hefner, "The kEY – unlocking the stories and best practices behind our Southwest Region success," EY, 2018, https://webcast.ey.net/events/play.aspx?prog=%7B3825085f-d4b7-4f5c-b67d-83f3e59a6e72%7D.



no one company can get all the power … you can examine code to know provably that you are being treated fairly to all other participants in the network."[61]

There is a reason they are talked about as "trust machines" Brody says. It is because they help people and companies verify one another's data. Trust is key in a global economy built upon alliances,[62] on a corporate and government level — but so is being able to float and survive in an ocean of competition. To be able to do this, and to build and maintain competitive advantage for companies going forward into the 21st century, businesses, governments and organizations must have a true blue ocean strategy that is capable of reaching into untapped market spaces ripe for growth. Developed by preeminent management thinkers W. Chan Kim and Renee Mauborgne of the esteemed INSEAD University, it is the idea that a systemic approach to innovation will help you find new markets and out-win the competition.

Companies can create a Blue Ocean Strategy that works for them by offering a service that grants autonomy of data management to their employees. Personal data ownership in the workplace is the wider trend the world is moving toward. To maintain a competitive advantage a company must do much more than simply march in place — the current unparalleled pace of innovation demands it. As Mark Twain once said, the secret to getting ahead is getting started. It's time to get to work.

---

[61] Paul Brody, Jason Friedman, and Scott Hefner, "The kEY – unlocking the stories and best practices behind our Southwest Region success," EY, 2018, https://webcast.ey.net/events/play.aspx?prog=%7B3825085f-d4b7-4f5c-b67d-83f3e59a6e72%7D.

[62] "EY Global Alliances Playbook," EY, 2018, http://eynetwletters.ey.net/2378107/eyalliances/index.htm#!/ey-global-alliances-playbook.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 03144-181Gbl
1803-2646515
ED None