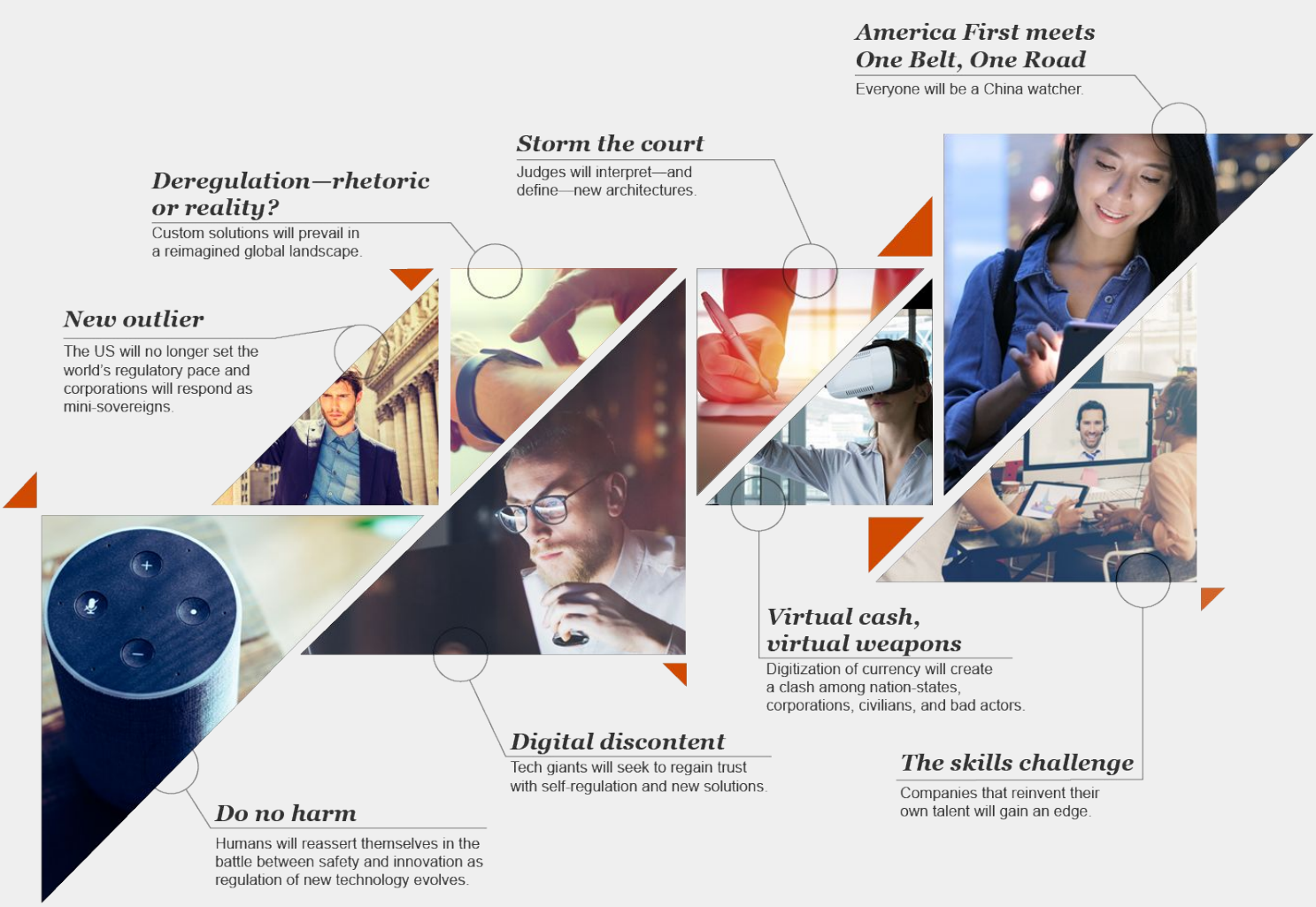
Risk and Regulatory

Top Policy Trends of 2018



PwC is part of the growing chorus that has contemplated the changes that will occur this year due to a game-changing US administration and heightened regulation in Brussels and Beijing.

In 2018, challenges to dominant architectures of trade, taxation, security, and communications will heighten policy and regulatory uncertainty. Meanwhile, 2018 also will be a year of stepped-up innovation, pushing society into areas where existing rules are no longer adequate.

pwc

How should business leaders chart the course for responsible innovation in such a world? CEOs, strategists, risk professionals, policy professionals, and executives need new playbooks; they need to anticipate how different policy and regulatory paths may lead to different outcomes.

PwC highlights the eight most important policy trends to watch.

A synchronous economic expansion around the world should increase prosperity in mature and developing nations alike. Major economic forecasters predict global GDP growth above 3% in 2018, the fastest since 2011. This will mark the first year since the onset of the global financial crisis a decade ago that economic risks across the globe appear muted.

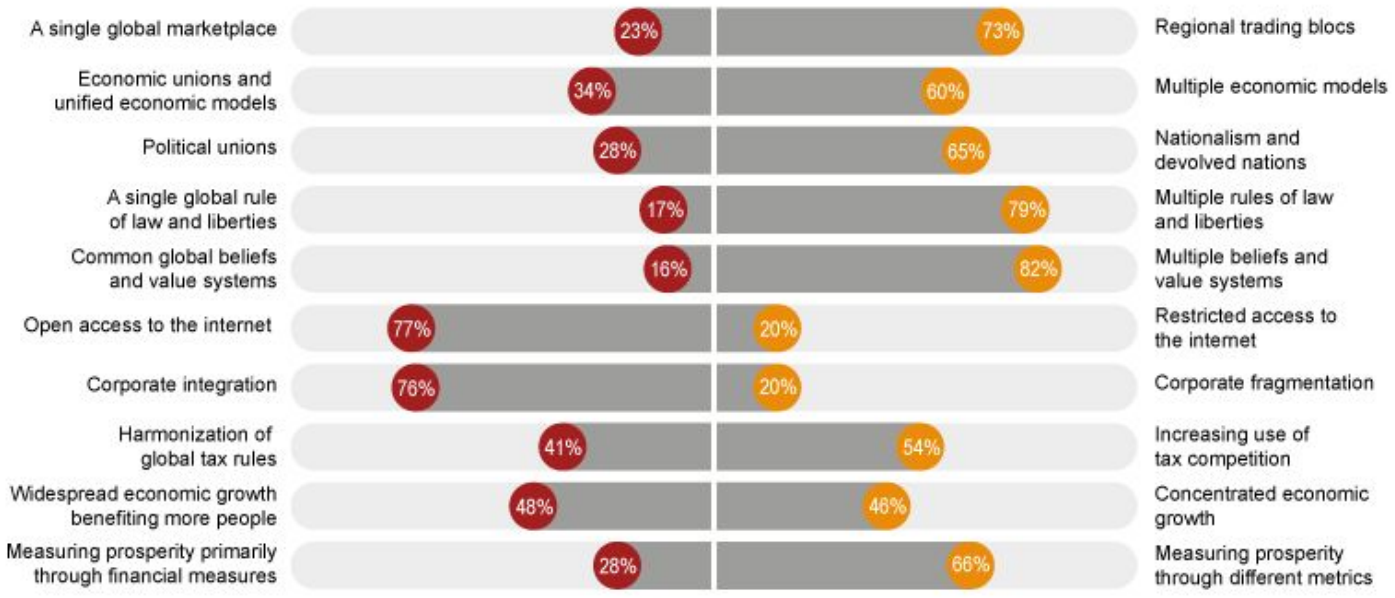
Yet the architecture that developed in the post-war era to support global business faces uncommon threats today that C-suite executives do not fully appreciate. Cyberattacks, gratuitous software innovation, and digital talent shortages are among the hurdles that will saddle growth if business leaders ignore or fail to address them.

For the past generation, several basic assumptions drove global business growth. Increasingly open borders, liberalized trade, and lax investment rules allowed companies to develop complex, integrated supply chains that enhanced productivity. Technology coursed rapidly across borders, thanks to new Internet applications, and skilled employees moved to locations with the best opportunities. Worldwide referees who tried their best to enforce a set of common standards held the system together.

Today, many assumptions that underpinned the expansion of globalization appear to be unravelling and the world's business leaders consider geopolitical concerns to be a rising risk. Nationalism has galvanized voting blocs in the US, UK, and Germany. The effort to root out "corruption" and "insurrection" has been used effectively in China, Russia, Turkey, and Saudi Arabia to help strong political leaders maintain power or topple rivals. Venezuela and the Philippines also have moved away from democratic rule.

Policy and regulatory uncertainty will spiral upwards with the conflict of ideas and models.

Q5: The following question contrasts a series of opposing political, economic, and trade trends. For each alternative, please select the one that you believe the world is moving more towards.



Source: PwC's 21st CEO Survey
Base: 1,293 Note: Some bars may not sum 100%. Respondents who answered "Don't know" are removed from the chart.

Former US ambassador to Russia and US Deputy Secretary of State William Burns sees “a conflict of ideas and models” playing out on the world stage. Both Russia and China offer their managed economic models as alternatives to democratically led free markets. But it goes beyond economics. Harvard Kennedy School professor and national security expert Graham Alison observes a mismatch between American and Chinese conceptions of the state, the role of individuals, relations among nations, and the nature of time.

This fracturing of the foundation that has buttressed global enterprise will fundamentally alter the regulatory and risk landscape corporations and their leaders face over the next two to three years.

The new risk and regulatory landscape

#1 New outlier

The US will no longer set the world's regulatory pace and corporations will respond as mini-sovereigns.

Since the end of World War II, the US has sought to be the world's "honest broker," the nation that brings together competing interests, launches international bodies to harmonize rules and standards, and seeks to be the ultimate arbiter of economic and security arrangements.

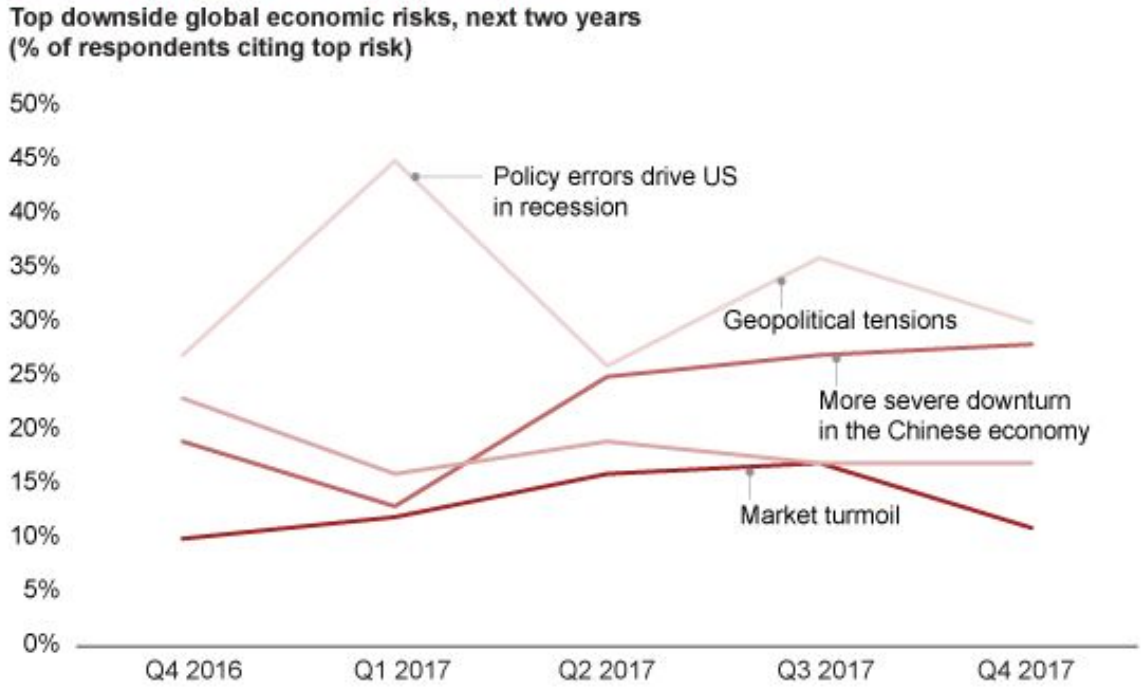
Donald Trump's election signalled an end to that era. From rejecting the Paris Climate Accord to pulling out of the Trans-Pacific Partnership and renegotiating the North American Free Trade Agreement—a majority of US business interests supported these pacts—the new administration has demonstrated that it will pursue an America First agenda focused less on complex multilateral agreements in favor of more streamlined bilateral arrangements. The US has disavowed traditional hallmarks of international leadership in favor of goals that are less aligned with geopolitical stakeholders, especially if these pursuits stand in the way of American prosperity.

Global businesses will deal more frequently and directly with regulators in Brussels, Beijing, and US states.

Implications:

- Washington will no longer be the single most important regulatory actor. With California and New York taking the lead in many instances, states will continue to challenge the federal government for the right to uphold net neutrality, environmental, and other protections.
- Europe will continue to position itself as the world's standard-bearer for privacy and consumer protections with the implementation of the General Data Protection Regulation, Payment Services Directive 2, Markets in Financial Instruments Directive 2, and a revised ePrivacy Directive. The Court of Justice of the European Union will emerge as a major regulatory force.
- Beijing will continue to regulate pricing in retail, express services, finance, and other industries. The data localization requirement in China's cybersecurity law may disrupt, deter, or prohibit cross-border data transfers. US firms may be asked to provide source code, encryption, or other data to regulators, which may be lost or stolen, and Chinese competitors could conduct spot checks.

Oxford Economics survey of business leaders shows rising concern over geopolitical concerns, supplanting macro-economic ones



Source: Oxford Economics Global Risk Survey

#2 Deregulation—rhetoric or reality?

Custom solutions will prevail in a reimagined global landscape.

The US government already has begun a process of rapid deregulation in areas ranging from environmental and consumer protections to financial services. The Federal Communications Commission has voted to repeal net neutrality, while banking regulators likely will ease stress-testing rules for banks and loosen some Dodd-Frank restrictions. Mining and energy companies will face fewer regulatory burdens, which could stimulate investment. The federal government will continue to support an expansion of offshore drilling, which some states are blocking, and will carry out proposals to guarantee large revenues for nuclear and coal-fired power plants in certain markets.

Some firms will seek to gain global and domestic reputational advantage by ignoring deregulation or following non-US rules. Some American manufacturers will continue curbing carbon emissions despite Washington's withdrawal from the Paris accord and some financial service providers may comply voluntarily with the US Department of Labor's now-frozen fiduciary rule. Washington, California, New York, and other states are drafting net neutrality laws that would prohibit Internet Service Providers (ISPs) from blocking or hindering access to online services or from offering premium-bandwidth "fast lanes."

US companies will create their own blueprints to navigate the new regulatory terrain.

Implications:

- Financial services firms in the US may face less scrutiny on certain issues, such as the fiduciary requirement for retirement advisors and balance sheet stress testing. Mortgage originations likely will grow, as the Federal Reserve is poised to raise interest rates and the mortgage disclosure rule will be eased. (For more, see PwC's report on top issues facing the financial service industry.)
- The US health sector faces a period of suspended paralysis as the Affordable Care Act is neither replaced nor revoked. States will develop strategies to combat the federal effort to gut Obamacare. Eighteen attorneys general already are embroiled in litigation involving halted Obamacare subsidies. (For more, see PwC's report on health reform 3.0.)
- Within the US, fear of disruptors and less cross-border trade will lead corporate M&A to mushroom. The tax plan, an influx of cash reserves, and incentives to repatriate funds from offshore affiliates, will lead to unprecedented values.
- States will seek to implement Obama-era regulations. Twenty-one attorneys general filed a lawsuit alleging that the Federal Communications Commission's repeal of net neutrality regulations is a violation of federal law. At least 22 states have introduced legislation to counter the federal rollback of ISP privacy protections.

#3 Storm the court

Judges will interpret—and define—new architectures.

As Trump's America First agenda is implemented, judges—many of whom he will appoint—will review, interpret, and rule on new policy and conflicts. One of the president's legacies will be litigation. More than 150 cases pertaining to the Emoluments Clause, executive orders, and tweets have been filed, including dozens of state attorneys general lawsuits.

In the US, appeals courts will continue to be divided on litigation involving data breaches, data misuse, and other privacy matters. Plaintiffs seeking settlements for disclosure of consumer and business information will argue new theories of liability, often involving pre-Internet legal standards. Historically, the Federal Trade Commission has been the most active in resolving privacy disputes, but, due to policy uncertainty, state attorneys general likely will be more aggressive.

In Europe, there will be a push-and-pull over who resolves conflicts, the courts or the private sector. The GDPR authorizes Internet Service Providers to resolve disputes involving users' privacy and information rights. The Court of Justice for the European Union will continue to interpret the standard for ISP liability and other data protection matters, including the overlap between GDPR and the EU-US Privacy Shield Program.

The US judiciary plays a critical role in interpreting policy and regulation. As the Trump administration remakes the federal judiciary and, possibly, the Supreme Court, his policy prescriptions will become more permanent.

Implications:

- Business-to-consumer and business-to-business breaches will be fuel for the plaintiff's bar. Despite a handful of federal appeals court decisions that did not find liability, several ruled that the Fair Credit Reporting Act requires that consumer reports are for intended recipients, thereby creating a security obligation.
- In Europe, there will be more debate over how much ISPs should monitor users and whether GDPR applies to hosting platforms like social media and news sites. ISPs may over-comply to avoid being placed under review. Conflicts over fines and extraterritoriality are likely. (GDPR applies to foreign firms that are not based in Europe, but have access to personal data of EU residents.)
- China's cybersecurity law will continue to be used for political means. Since the law was implemented, more than 40% of enforcement actions were to remove "politically harmful content," with less than 3% for protecting the "rights and interests" of the "Internet user" according to an article in the National Law Review.

#4 America First meets One Belt, One Road

Everyone will be a China watcher.

For most of the past 45 years since China first opened to foreign goods, global companies have made compromises— or concessions—to access the world's most populous and fastest-growing market. Western entities were forced to create joint ventures with Chinese partners, share technology with local firms, or refrain from repatriating profits.

In 2018, US and other foreign firms could begin to reassess the trade-offs. China's ambitions are accelerating, while the Trump administration has escalated the rhetoric over steel imports and intellectual property, among other issues. In October, President Xi Jinping called for bigger state-owned enterprises and downplayed free-market policies. China's leader will manage risks, like reducing debt and pollution. With a planned $2 billion research park in Beijing, artificial intelligence, biometrics, and other emerging technologies will thrive in an environment of minimal data privacy rights.

The Trump administration will continue to challenge a rising power that has benefited from the open architecture of global commerce while limiting access to its domestic market. The US may explore alternatives to correct the trade imbalance with more positive solutions than a trade war.

For the US and China, everything—from trade to artificial intelligence—is in flux.

Implications:

- Trade and investment between China and the US are likely to face more regulatory scrutiny on both sides. The US Congress is drafting legislation to tighten the rules governing foreign investment in US firms through the Committee for Foreign Investment in the US, addressing national security and competitiveness.
- The US may impose additional duties on Chinese goods in an effort to boost US manufacturing activity and lessen competition from foreign firms. Beijing could retaliate by impeding further US investment in China. If the yuan sinks, there could be a currency devaluation to make its exports cheaper, reducing the impact on American consumer demand of any US tariffs.
- China will spar with the US and Europe over whether it is a "market economy" under World Trade Organization rules, despite the role that the state plays in the Chinese economy. Multinationals could face more government reviews or find it more difficult to get permits or licenses. Companies may get audited or investigated for antitrust violations.

Responsible innovation

We have entered the Second Machine Age, also known as the Fourth Industrial Revolution. Wired magazine co-founder Kevin Kelly predicts that innovations will follow one formula: Take x, add AI.

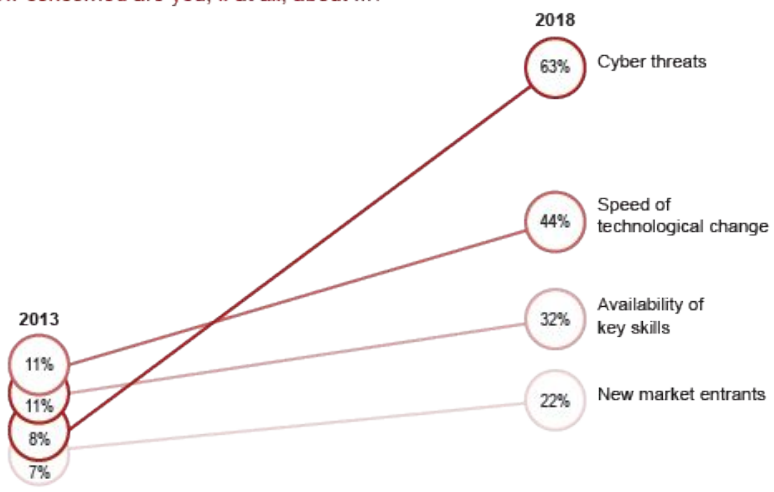
PwC has estimated that AI could contribute up to $15.7 trillion to the global economy in 2030, more than the current output of China and India combined. Of this, $6.6 trillion likely will come from increased productivity due to automation of tasks and roles and $9.1 trillion likely will come from product enhancements that stimulate consumer demand.

PwC predicts where companies will focus in 2018 to capitalize on this potential.

How should CEOs steer their organizations through such a period? And how do risk and policy professionals provide strategic advice to help them anticipate risks we don't understand fully? How do they work together, and with regulators, for responsible innovation?

CEO concerns related to technology have risen the most in the last five years

Q. How concerned are you, if at all, about ...?



Source: PwC, 21st Annual Global CEO Survey–US supplement

Base: US CEO respondents (2018=105; 2013=167), showing % 'extremely concerned' only. Note: In PwC's 2013 CEO Survey, we asked broadly: *How concerned are you about energy and raw material costs and How concerned, if at all, are your about inability to protect Intellectual Property and customer data. In 2018, we asked: How concerned are you, if it all, about ... volatile energy costs ... cyber threats.*

#5 Do no harm

Humans will reassert themselves in the battle between safety and innovation as regulation of new technology evolves.

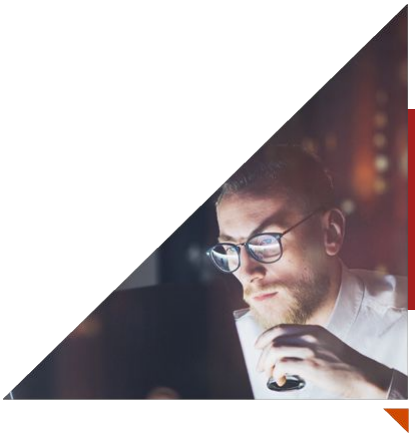
It is hard to exaggerate the influence of emerging technologies. Voice-activated digital assistants like Alexa, Google Home, and Siri have gained popularity. Autonomous vehicles soon may be driving cargo cross-country. Drones are used for firefighting, crop rotation, and industrial inspections. Artificial intelligence is mining visual data, even scanning subway stations, to identify potential threats, and is active in health diagnostics. Moore's law predicts that digital capabilities will accelerate, sometimes in ways that defy human imagination.

Yet these technologies require new rules that don't stifle innovation. With an "AI arms race" among top Silicon Valley firms, some level of regulation, particularly self-driving cars and the Internet of Things, is inevitable. Traditional methods such as product licensing, Research and Development oversight, and tort liability are not well-suited to manage the risks associated with autonomous machines. Regulators will need to untangle issues involving foreseeability, lack of control, and opacity.

In 2018, policy discussions on emerging tech will confront three balancing acts: the value of data-driven decisions versus privacy and security; the public good versus the speed of innovation; and the primacy of global versus local policy.

Implications:

- Tech companies could face new regulations affecting key business areas, including disclosure requirements for sources of online advertising and obligations to police user-generated content, particularly for firms with a social media presence. In the short term, we may see more self-regulation to address policy concerns to stave off a formal—and potentially restrictive—regulatory approach.
- Rising awareness of privacy risk will emerge around digital technologies as consumers try to determine when an innovation is useful or unnecessarily intrusive. Does having an eavesdropping device in the kitchen add security or diminish it? Should your Fitbit send updates to your cardiologist? The market eventually may determine the frontiers of acceptable and unacceptable behaviors, with the federal government intervening in clear cases of unfair, deceptive, or anti-competitive practices.
- Transportation, consumer safety, and other agencies will be obligated to determine the best strategies for regulating and monitoring autonomous vehicles. As accidents happen, systems will be established to resolve questions about whether a manufacturer, developer, or person in control of an autonomous machine is liable when a machine errs, causes harm, or is corrupted.
- On Capitol Hill, there has been a push to establish a federal advisory committee to brief US policymakers on AI matters. States and the market may enact next-generation regulations faster, but federal legislation that will limit the ability to set standards on self-driving cars is pending.



#6 Digital discontent

Tech giants will seek to regain trust with self-regulation and new solutions.

The tide has turned against the growing reach of tech giants after years of breathless enthusiasm over technology's ability to organize data and build social networks.

The EU has taken the lead in limiting that reach. For example, the Court of Justice of the European Union's recent ruling that luxury brands may prohibit retailers from selling their products on third-party platforms could signal new e-commerce restrictions. Executives are beginning to grasp the enormous impact of new EU data and privacy rules and emerging laws to protect firms from foreign takeovers. The EU will continue to hound US tech firms over paying back taxes and storing cash in offshore tax shelters. Europe has signaled that it may pursue antitrust investigations into whether data provides companies unfair advantages over competitors.

In 2018, tech firms will band together and partner with other organizations to regain and inspire consumer trust. For example, more than 75 media entities joined together to create trust indicators, standardized disclosures on news sites to help readers distinguish news from opinions and advertising.

Technology firms face a do-or-die moment to regain trust following a growing backlash amid renewed concerns for privacy and security.

Implications:

- Poor cybersecurity and increasingly sophisticated hacking threats from a range of geopolitical, non-state, and criminal actors will pose mounting risks. Government and industry leaders will strive to make their systems more resilient. (For more, see PwC's insights on building resilience to cyber shocks.)
- GDPR requires that firm data is accessible and easily indexed. For example, companies must ensure that European consumers can find the information businesses collect about them, revise the information if it's inaccurate, move the information to another provider if desired, and delete it if consumers wish to be forgotten.
- In the US, tech firms may face new antitrust scrutiny. While the Department of Justice likely will stay the course—for now —by permitting significant vertical integrations with behavioral remedies, the states may step in. For example, Missouri's attorney general is investigating whether Google mishandled private customer data and manipulated search results to favor proprietary products.
- Global firms will focus more on tech regulations emerging from Brussels and Beijing than the US while listen to US consumers, whose views on privacy and new technologies' intrusiveness increasingly will carry weight. Public outrage over labor issues, including discriminatory practices, will continue.

#7 Virtual cash, virtual weapons

Digitization of currency will create a clash among nation-states, corporations, civilians, and bad actors.

A new generation of investors are cashing in on the boom in Bitcoin and other digital currencies. Growing numbers of businesses accept virtual currencies as payment, as a currency can be a store of value independent of any national government.

Central banks are considering making reserve currency digital, while anti-government groups advocate for a citizen-run market. China, Japan, Sweden, and others will develop their own digital currencies.

But these markets and technologies create new vehicles for fraud and other forms of wrongdoing. Cybercriminals continue to exploit unconventional arms and asymmetrical tactics. The disruption foreign trolls unleashed during the 2016 presidential election is one example that illustrates the growing destructive power of cyberattacks. Perpetrators of North Korea's WannaCry ransomware attack that infected more than 300,000 computer systems tried to hack Bitcoin and other cryptocurrencies.

Organizations with sensitive data in need of protection often seem one step behind the hackers and other bad actors in figuring out how to defuse—let alone anticipate—the next disruptive cyber threat.

Bitcoin and other virtual currencies will continue to be attractive vehicles for creating value, but security uncertainties will prevail.

Implications:

- National governments are investing heavily in the powerful computing resources needed to mine digital currency in an effort to develop closed "permissioned" networks for exchange. Competition is emerging between private syndicates and nation-states regarding the mining and trading of digital currencies.
- Congress will consider drafting new legislation for cryptocurrencies. The Securities and Exchange Commission has cracked down on several fraudulent Initial Coin Offerings. Meanwhile, the Commodity Futures Trading Commission, which has designated Bitcoin a commodity, also filed an enforcement action. States will continue to keep an eye on these markets.
- The rise in cybercrime will require companies to make attacks more costly for criminals. A malicious hack of a cloud service provider could cost losses of about $53 billion, according to a Lloyd's of London report. Specialized and targeted ransomware attacks alongside compromises to data and email will continue.

#8 The skills challenge

Companies that reinvent their own talent will gain an edge.

The tech talent shortage shows no signs of relenting. Chief Information Officers will wake up to the reality that artificial intelligence will not resolve the IT employment crisis. Firms will need to diversify their pool of applicants to find technically agile workers with soft skills.

PwC's 21st Global CEO Survey reveals that companies with an understanding of how to use robots and AI to improve customer experience are more likely to invest in digital reskilling and continuous learning programs. US businesses, higher educational institutions, and cities are working to improve the pipeline of data science and analytics talent. Digital Fitness Assessments identify targeted training to help people reskill.

Federal investment in human capital lags behind the private sector, both in terms of funding and policy focus. China plans to accelerate the training of high-end AI talent to build a $150-billion AI industry by 2030. President Obama called for aggressive policy action to ensure that all Americans develop and share the enormous benefits of AI and automation, but the new administration has largely ignored AI in favor of protecting workers from foreign competition.

According to PwC's 2017 Global Digital IQ Survey, 54% of business and IT executives are making significant AI investments today and 63% will make significant investments in three years.

Firms will prioritize finding employees who meet digital fitness goals and boast cultural dexterity.

Implications:

- Beijing will scramble to find talent with its investment for an AI industrial park, where the state plans to host 400 companies. Meanwhile in the US, Silicon Valley firms will continue to compete by enticing candidates with high salaries, especially in AI, where demand for expertise in booming. Google's professional certificates in IT may lead more tech firms to set up training programs.
- Technology will accelerate growth in the gig economy, undermining employers' ability to attract and retain highly skilled workers. The tax plan includes a 20% business income deduction for partnerships, S-corporations, and sole proprietorships. Blockchain will create faster and more convenient payment methods that will enable opportunities.
- More contingency will emerge in software/IT, finance, and healthcare, creating new policies on compensation, safety, and information sharing. Immigration and cross-border collaboration are essential to the tech sector, but obtaining H-1B visas has become more cumbersome. 2017 saw a spike in "requests for evidence" to support applications. Firms will continue to lean on the administration to rethink its restrictive immigration policy.
- Economies will continue fighting for competitive edge. Only 53% of US CEOs see a responsibility to retrain workers whose tasks and jobs are automated by technology; this figure pales in comparison to Germany (85%), China (84%), and Japan (71%), according to PwC's 21st Global CEO Survey.

New playbooks are needed

For CEOs

It is difficult enough to manage an organization and simultaneously transform it for the future. Today's CEOs have to do that in a fractured world, rife with conflicts of ideas and values. According to 2018 Edelman Trust Barometer, almost two-thirds of survey respondents say they want CEOs to take the lead on policy change instead of waiting for government.

That kind of engagement requires balancing six paradoxes of leadership simultaneously, as PwC's Global Leader for Strategy and Leadership, Blair Sheppard, put it. The CEO must be a high-integrity politician, tech-savvy humanist, globally-minded localist, traditional innovator, humble hero, and strategic executor.

For risk professionals

Risk professionals face higher risk appetites and tolerance, as their firms take on more innovation. Initial experiences with the unintended consequences of AI and other emerging technologies have underscored the need for responsible innovation. Risk managers have a big role to play for their organizations and society at large.

The risk professional must embrace these new technologies in a world with new architectures. Whether improving on existing products or developing new ones, managers need to continue monitoring risk that stems from geopolitical distress, regulatory uncertainty, or innovation.

For policy professionals

The transforming geopolitical landscape requires policy professionals to be fully engaged in the strategic planning process. Companies have the opportunity to play an active role in shaping policy, but they must do so strategically.

Anticipating how regulation will evolve as managed economic models co-exist alongside democratically led free markets is a basic tenet for shaping effective policy. Poor cybersecurity and increasingly sophisticated hacking threats from a range of international stakeholders, including non-state and criminal actors, will emerge alongside opportunities for growth. The policy analyst needs to closely monitor new technologies and developments in Europe and China as US policies evolve—and be prepared to adjust their strategies accordingly.

Contacts

David Sapin
US Risk and Regulatory Consulting Leader
Tel: +1 (202) 756 1737

Alison Kutler
US Strategic Policy Leader
Tel: +1 (202) 730 4233

Sean Joyce
US Cybersecurity and Privacy Leader
Tel: +1 (703) 918 3528