MARSH & McLENNAN COMPANIES | Global Risk Center | BRINK The Edge of Risk

September 26

2017 Marsh Panel Counsel Symposium

Risk Perspectives for Boards of Directors

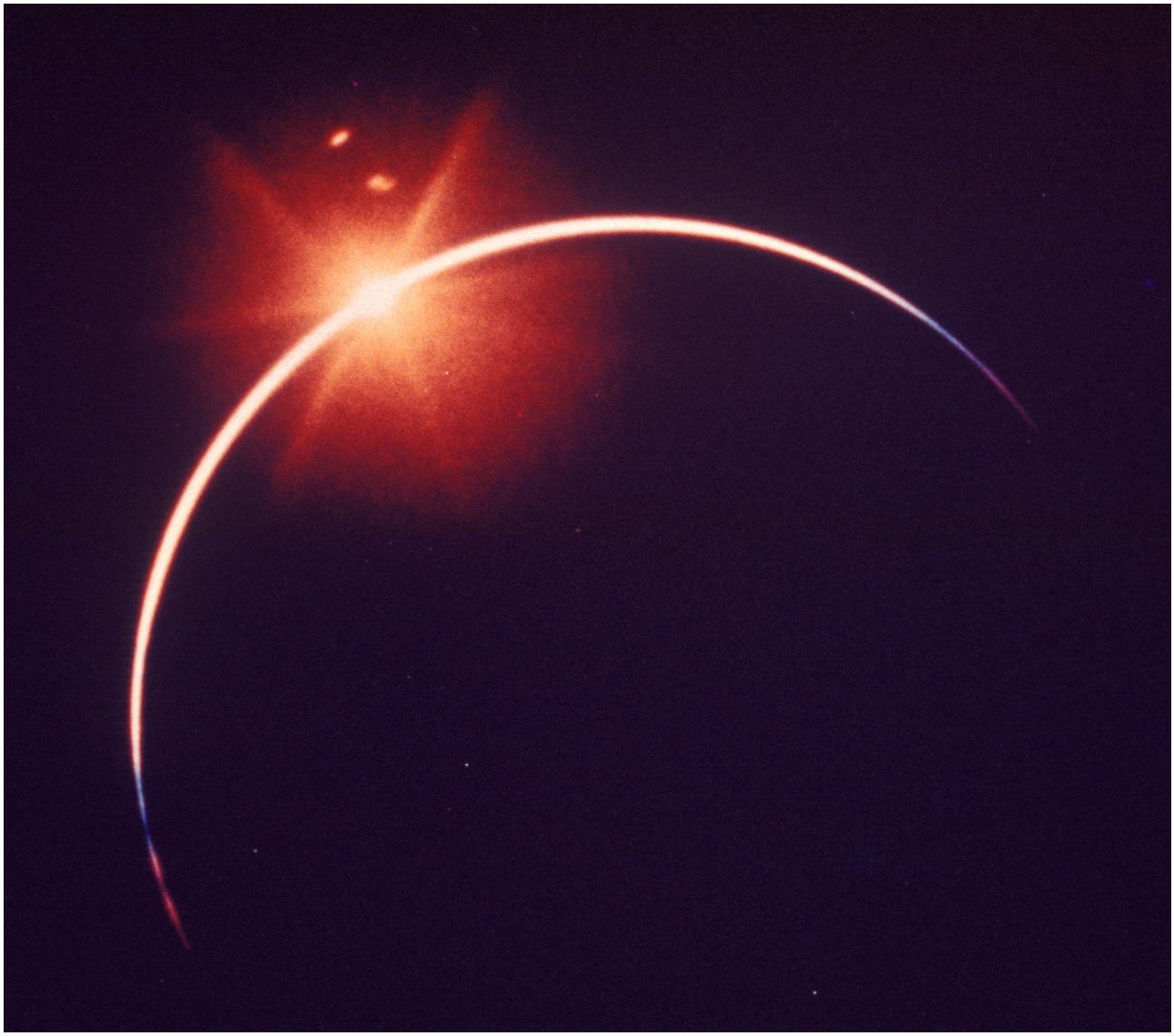


TABLE OF CONTENTS

INTRODUCTION

The articles included in this publication were selected for the ways in which they examine global risk issues critical for boards of directors. They provide key insights into ongoing and emerging risks in the geopolitical, regulation, and emerging technologies and cyber areas, as well as more traditional economic risks. These articles also highlight opportunities available to companies best positioned to take advantage of them.

This report was prepared for Marsh's 3rd Annual Panel Counsel Symposium. As the first and only broker developed Panel Counsel initiative, the Marsh Panel Counsel is a unique approach to retaining top tier legal talent for investigations and litigation on an optional, pre-approved basis, providing Marsh clients with benefits that extend beyond the insurance relationship. The Panel Counsel initiative is designed to foster collaboration between Marsh, its clients, insurers, and law firms.

All articles first appeared on BRINK, the digital news service of Marsh & McLennan Companies' Global Risk Center, managed by Atlantic Media Strategies. BRINK gathers timely perspectives from experts on risk and resilience around the world to inform business and policy decisions on critical challenges.

ON THE EDGE: OPPORTUNITIES IN A POLARIZED WORLD

John Drzik
President, Global Risk and Specialties at Marsh

Business leaders today must navigate a shifting global landscape of risks ranging from geopolitical tensions to social instability to emerging technologies. The shifts are creating new threats as well as new opportunities.

Two years ago, the confluence of global risks was pushing the world toward a tipping point. Since then, geopolitical pressures have continued to grow and societies have continued to polarize.

Political shocks and other unexpected events in 2016 were part of a broad geopolitical turn toward protectionism that has been building for years. This has put global cooperation under strain, as seen in developments ranging from collapsing trade agreements to the rising threat of nuclear proliferation.

On the social front, a number of dynamics are increasing instability. Many citizens in advanced economies are struggling with their economic future, facing protracted threats to employment and retirement security. Meanwhile, in developing economies, more citizens are moving into the middle class, creating new demands on their governments that they have been slow to meet.

The ever-present threat of terrorism changed its face in 2016 as the specter of the "lone wolf" emerged inside the borders of advanced economies to terrorize citizens of Paris, Brussels, Nice, Istanbul and elsewhere. Moreover, cautionary admonishment from high-profile visionaries regarding the weakly governed application of artificial intelligence amplified the already uneasy public debate about advanced technologies exacerbating unemployment and exposing society to new risks.

Companies, either alone or collectively, cannot control the underlying causes that give rise to these global risks, but better awareness of their depth, breadth and scope can inform plans and processes to address the challenges—and opportunities—these risks present.

GLOBAL RISKS REPORT 2017

The *Global Risks Report*, prepared by the World Economic Forum with the support of Marsh & McLennan Companies and other partners, looks at the major threats facing the world today.

The just-released 12th edition of the report highlights the social and political risks that crystallized throughout the world in 2016 and examines some of their root causes, which include rising income and wealth disparity, a fraught geopolitical environment and disruptive technological change.

The 2017 report also explores the interconnections among risks. Social instability was at the center of the web, both increasing and being increased by a number of major risks.

Two major themes dominate the 2017 report: growing social and political turmoil and the emerging technologies of the Fourth Industrial Revolution.

TOP TEN SOCIAL INSTABILITY RISK CONNECTIONS*

Source: World Economic Forum, Global Risks Report 2017

*Global Risk Perceptions Survey (745 responses worldwide): Respondents were asked to identify three to six pairs of the most strongly connected global risks. Thickness of connecting lines corresponds to citation frequency.

SOCIAL AND POLITICAL CHALLENGES

Across the globe, people are sending a clear message to political leaders. They are hurting, frustrated and angry. They feel let down and they want change. At the ballot box in advanced economies, voters have rejected the political establishment and the status quo, most notably in the UK Brexit vote and the United States presidential election. Anti-establishment sentiment is also reverberating across the Eurozone, where populist movements sprung to life and are gaining momentum in Austria, Belgium, Denmark, France, Germany, Greece, Hungary, Italy, the Netherlands, Poland and Sweden.

Citizens have also taken to the streets in large numbers. In France, strikers have disrupted fuel supplies and there have been regular demonstrations in major cities against proposals for labor market reforms. In Germany, policies to accommodate the large influx of refugees have been a lightning rod for broader frustration. In countries such as Argentina, Brazil, Iceland, South Africa and South Korea, corruption exposures and allegations have depressed the trust of citizens in their leaders. Societies are increasingly polarized and the stress on established democratic norms is reaching a breaking point.

Democratic leaders are being confronted with some uncomfortable trade-offs. To restore democracy to a healthier state, policymakers must grapple with several major challenges, including how to make economic growth more inclusive, how to reboot the political system while maintaining continuity in systems of government and how to manage the renewal of societal identity while balancing elements such as assimilation versus diversity.

Surges in social and political instability have the potential to spawn a wide range of potential disruptions to business activity, from civil disturbance and terrorist attacks to government policy reversals and regime change. As a corollary, companies may also more easily find themselves on the wrong side of volatile social, political and environmental issues.

THE FOURTH INDUSTRIAL REVOLUTION (4IR)

Technology will continue to play a vital role in promoting global prosperity. New advances are poised to increase economic productivity, provide radical healthcare solutions and combat climate change, among other benefits. The pace of innovation is also creating new risks, ones that will be amplified in a world where geopolitical and social instability are on the rise.

The report highlights artificial intelligence (AI) and robotics as a technology area needing better governance. AI is quickly showing it has the power to take jobs away from both blue- and white-collar workers, challenging policymakers looking for ways to build resilience to the impact of automation. At a time of significant unemployment concerns and growing social instability among lower-income groups, companies may also experience mounting pressure to align their automation and employment strategies with what is deemed politically and publicly acceptable.

The AI field is fraught with other complications, for example, new liabilities where legal precedent is embryonic at best. If self-driving cars cut the roughly 40,000 annual U.S. traffic fatalities in half, auto manufacturers might get 20,000 lawsuits instead of 20,000 thank-you notes. Where does the liability lie? Is it with the carmaker, the software developer or the individual programmer who wrote the initial code? Development in risk governance for AI in parallel with its commercial deployment is critical to ensure risk/reward tradeoffs are clear for businesses.

IMPLICATIONS FOR BUSINESS

To thrive in such challenging times, businesses will need to think creatively about scenario planning, including second- and third-order consequences such as likely government responses and cross-border impacts. Gaming out plausible developments and worst-case scenarios will provide a baseline for gauging which assets are at risk and the scale of the potential damage. Having done this, companies can stress-test supply chain approaches and investment decisions while evaluating potential changes to business and risk management strategy that will help diversify or transfer exposure to disruptive events within and across countries.

New kinds of analysis are also needed. In this era of "fake news" and volatile social issues, firms should reevaluate whether they are doing enough to protect and manage their reputation with customers, employees and other stakeholders. Rumor and allegation are not new problems for companies, but in today's "always-on" world, such matters can go viral within hours and be more challenging to overcome.

We are living in a time of high risk, but it can also be a time of great reward. Every challenge will need an innovative solution; while new policies may close some doors, they will inevitably open others. With a careful eye on the emerging global risks landscape, companies can thrive in this volatile environment.

PREPARING FOR DISRUPTION, POLITICAL RISK AND CRISIS IN AN ERA OF UNCERTAINTY

BRINK Editorial Staff

Among technological disruption, geopolitical tension, and escalating cyber risk, the future will be defined by its instability. The best way for organizations to respond to this turbulent and uncertain vision of the future is to develop a robust plan that engages with the threats looming on the horizon.

Uncertainty and blind spots regarding risk were the key topics at the recent Marsh & McLennan Companies' annual government contractors' forum titled *Growth in an Unpredictable World: Strategies for Resiliency.* Alex Wittenberg, executive director of Marsh & McLennan's Global Risk Center, emphasized that no single plan for the future could save an organization from disruption; risk managers have to be prepared for a multitude of scenarios.

"Mitigation response has to follow alternative views of the future," Wittenberg said. "You can't just build for a best-case scenario, and certainly if you just build for the worst-case scenario your shareholders are going to crucify you. If you only understand one or two versions of the future, I can pretty much tell you that's probably not what's going to happen."

CYBER RISK IS SOARING

Cyber risk should already be on every risk professional's radar—but few are aware of the full extent of the problem. During the forum's first panel, *Technology Disruption's Impact on Strategy and Risk,* Philip Reitinger, president and CEO of Global Cyber Alliance, predicted that cybercrime would be particularly difficult to limit.

"This is bad math, but if you projected out (the compound annual growth rate in cyber losses) the entire world economy will be eaten by cybercrime in 2025," Reitinger said. "Now that's ridiculous, that's not going to happen, but it's hard to see where (cybercrime) is going to slow down."

Unfortunately, dangerously few working professionals—especially risk managers and C-suite executives—appear to be aware of the disruptive forces on the verge of upending their industries. In a recent survey from

Marsh and the Risk & Insurance Management Society, more than half of the respondents said that their organization had not conducted a risk assessment to expand their understanding of disruptive technologies.

Even more disturbing was the finding that many of those surveyed were unaware of technologies in use within their own organizations. Forty-eight percent of risk professionals responded that their organization wasn't using or planning on using the Internet of Things; the actual use number was 90 percent.

Marsh's Jim Holtzclaw, echoing Wittenberg's keynote, argued that organizations need to develop plans that have a wide berth for future change: "Organizations need to be looking at ways to adopt these technologies, they need to be proactive, they need to plan accordingly."

However, Holtzclaw also cautioned that adoption for the sake of adoption, without the appropriate due diligence, could be catastrophic.

"If you've ever pictured the iceberg that's floating in the ocean, and you see the part that's above the waterline, that's what the vendor is telling you about," Holtzclaw said. "What he's not telling you about is that large chunk that represents the maintenance, the upkeep of that solution that sits below the waterline. That maintenance tail may not fit within your organization, and that technology will be a failure."

However, when an audience member asked the panel about potential avenues for older companies unprepared for newer platforms, Holtzclaw responded frankly: "Those kinds of companies? We're seeing them die every day. They have no choice but to innovate."

GLOBAL EXPANSION MEANS LOCAL RISK

As organizations expand and become increasingly international, they'll need to adhere to local customs and regulations in the variety of countries they're operating in. The second panel, titled *Third-Party Uncertainty from Geopolitical Instability,* addressed the risks of wading into new legal and regulatory environments in the local context.

Nina Gross, head of BDO Consulting's Washington, D.C., Global Forensics practice, explained that many organizations seeking to work abroad often lacked the local context necessary to operate legally.

"Whether I'm Nigeria, or Mexico, or Brazil, or Germany, or Switzerland, or fill-in-the-blank, I'm going to enforce my laws," Gross said. "Many of us don't even know what those laws are. And so I think the dynamic now is: We need to be aware of what's happening—not just in the U.S. or where you're headquartered—but what's happening around the world where you do operations. That, I think, is the biggest risk right now."

However, adherence to local laws can be complicated when countries have a record of corruption, crime, or terror risks. Beyond just knowing local laws and regulations, organizations need a clear understanding of the risk landscape in the country they are in or plan on working in.

Julie Martin, who leads Marsh's Public Agency Team, gave a historical example: "Going back a couple decades, the only way that you could do business, for example, in Indonesia, is if you were in partnership with a Suharto family member. But when Suharto was toppled that then became a big negative. So you obviously need to consider who your partners are."

Identifying potential crises and building response frameworks in advance must be every risk professional's priority.

The best approach, Gross explained, is due diligence well in advance of a deal. Mobilizing accountants to conduct audits and look into potential international partners isn't an extraneous cost—it lays the groundwork for successful business operations going forward.

"When you start to pull back that onion, you realize, 'well their business is dependent upon paying bribes, and the head of the business's son-in-law is the head of trade in such-and-such ministry,'" Gross said. "You've got to start asking questions early on in the deal. Once you get too far in, you're almost beholden and you have to complete that deal and it may end up being a big problem."

RESPOND TO REPUTATIONAL RISK CRISES

The final presentation at the forum, *Social Instability: Optimizing Talent During the Storm,* focused on reputational risk. First, Chandra Seymour of Marsh Risk Consulting put the worth of a reputation into concrete numbers.

"Reputation typically accounts for about 30 percent of a company's actual stock price or value," Seymour said. She cited a recent airline PR crisis, after which the company's stock price took a 1 percent dip. "For that organization, a 1 percent dip represented $255 million," she said. "So that's a big number, especially when, what studies have also shown, is that typically a stock price will dip anywhere from 20 to 30 percent after a major reputational issue."

Reputational risk can be increased by a number of factors, ranging from bad conduct and questionable business judgment, to internal and external attacks. These risks are amplified in a crisis due to a confluence of factors:

- Crises are inherently unpredictable, so most organizations aren't prepared for them
- The 24-hour news cycle and social media have the potential to expand the crisis beyond its original proportions
- Social media also increases the expectations for a company response, which often runs counter to a desire for fact-finding or measured silence
- The unpredictable nature of crises makes accurate information difficult to come by

Seymour emphasized that most problems cannot be easily contained to any one department. A cyber issue, for example, is not an IT problem; it could easily spill over and become a business and communications problem.

Therefore, mirroring the suggestions of speakers before her, Seymour argued that the goal for any organization unwilling to risk its reputation would be to develop a streamlined, comprehensive response structure. That would entail identifying potential crises and response frameworks well in advance and training spokespeople and management to respond quickly and clearly.

CLIMATE CHANGE: AN EMERGING RISK FOR CORPORATE DIRECTORS AND OFFICERS

Arati Varma
Head of FINPRO Practice, Singapore and ASEAN at Marsh

Climate change is fast emerging as one of the most significant risks facing the economy, and Asia is considered to be one of the most vulnerable regions in terms of its physical impacts.

In recent years, climate change has become a headline issue for both governments and the private sector due in part to emerging rules and regulations. However, most companies in Asia have only just begun to address the potential impact of climate change at the board level. The increasing call for clarity in climate risk disclosure has spurred risk managers, board members, and chief financial officers to examine this evolving management risk exposure.

THE TIME TO ACT IS NOW

Regulators, large institutional investors, and sovereign pension and wealth funds are increasingly focusing on the performance of companies in the face of climate change risks. This includes the preparedness of companies and their boards to effectively deal with operational, regulatory, and reputational risks resulting from climate-related exposures. We expect to see the development of claims against companies and their directors arising out of the disclosure (or lack thereof) of climate-change related risks.

Knowledge and awareness of risks and opportunities associated with climate change are critical for boards and senior executives. Directors and officers can expect increased scrutiny in the years ahead from shareholders, regulators, and young prospective employees regarding their companies' responses to address the emerging risks and opportunities of climate change. The absence or lack of board awareness and accountability on climate change and sustainability may result not only in breach of regulations but also reputational damage and lower company valuations relative to those of more engaged industry peers.

Risk managers must therefore understand and communicate climate-change risk issues to their boards. This includes focusing on issues that concern boards and presenting information in a manner that is both meaningful and beneficial to the directors' decision-making process. Boards, in turn, need to provide guidance to the risk committee, as part of enterprise-wide risk management, so that risks and opportunities resulting from climate change can be incorporated into the strategic planning process. Prudent, long-term planning is important to mitigate the adverse impacts and take advantage of the opportunities presented by climate change risks.

Social and environmental considerations fall within the purview of fiduciary responsibility of board members. This is because they have fiduciary duties to act in the best interests of their company with reasonable care and due diligence, in following their mandate to maximize returns, concurrently.

WHAT'S TRENDING?

Directors' and officers' liability exposure continues to grow in the climate risk space. Of particular note are the following trends.

Increasing call for clarity in climate risk disclosure.

Shareholders and regulators alike are increasingly seeking greater transparency on corporate policies related to the environment. Directors and officers may be required to respond to allegations of failure to disclose the company's climate-change related risks, or to ensure compliance with climate related laws and regulations. Recent legislative developments in Asian countries such as India and Thailand now enable investors to commence securities-related class action litigation. A derivative suit might occur where failure to prepare or respond to climate risk results in considerable financial loss to the company. Even a shareholder class action might arise if the failure to disclose climate risk exposure or events was to cause material negative impact to the company's share price.

Increased regulatory action.

Regulators are becoming more vigilant, and enforcement is becoming more broad. Increased regulatory activity often leads to increased liability. Some regulations now require disclosure of a corporation's climate change-related risks. It is possible that within the next few years, guidelines—if not mandatory rules concerning climate risk disclosure—will be established in many countries. Furthermore, as companies expand their business operations to new and foreign jurisdictions, directors need to be aware of the various legal and regulatory developments overseas. This goes beyond traditional financial regulators, and includes other climate change-related regulatory and quasi-regulatory bodies. Severe penalties can be imposed on directors who fail in their duties to consider and disclose the potential risks of climate change, including fines and/or disqualification from holding directorships.

Negative impact on company valuation and reputation.

Liability from direct or inadvertent climate-related risks can be significant, if not catastrophic, as demonstrated in the case of asbestos, oil spills and ground leaching. A company can go bankrupt cleaning up a site or defending lawsuits arising from environmental torts. There is also a danger that adverse publicity generated through unexpected social-media coverage might harm product sales as customers turn to substitutes. Therefore, crisis management preparedness is increasingly valuable. Companies that are unwilling or unable to integrate climate change considerations into operational and investment decisions may be viewed negatively by customers and shareholders.

THE SAFETY NET

As with other parts of the world, many countries in Asia such as Japan, Hong Kong, Thailand and Singapore are moving toward a more litigious culture, with the objective of making companies and individuals more accountable. There is a growing trend toward seeking punitive and personal legal action against senior executives for failure to follow regulations and standards.

The globalization of risks and exposures and increased awareness of consumer rights in Asia is resulting in investigations, criminal prosecutions, or civil litigations over alleged wrongdoing. These action have put company and individual assets at risk. In such cases, senior executives might look to the Directors' and Officers' (D&O) liability insurance policy to help with defense costs, settlement, or judgments.

D&O liability insurance or management liability insurance, provides indemnity to the directors and officers of a company for their personal liability to pay damages to a third party, resulting from an actual or alleged wrongdoing. This includes a breach of their duties in the course of managing the affairs of the company. Noteworthy in the climate change context is the pollution exclusion typically contained in a D&O policy, which is designed to prevent the D&O policy from covering physical and environmental perils, as physical perils are afforded cover under other insurance policies available in the market. However, most D&O insurers allow the insured to "buy back" some cover within the pollution exclusion for non-indemnifiable claims, which are claims for which the company cannot reimburse an executive for liability or defense costs. D&O insurance in Asia has become an integral part of sound risk management for many companies as it provides financial protection for executives against the consequences of actual or alleged wrongdoing.

Climate change is a key global risk. It follows that the law may be increasingly used as a means of forcing the corporate sector to respond to its challenges. As the legal landscapes across Asia evolve, further litigation will likely emerge in Asia from the issues and laws associated with climate change.

Risks for companies and their management are growing and liability claims arising from climate change-related risks can be extremely complex and costly. Action on climate change is gathering pace and boards are more aware of the need to act on the unprecedented challenges posed by it. Directors and officers need to recognize their responsibilities: They need to accept that good management of environmental governance is imperative for the protection and enhancement of shareholder value of the company.

IN PRACTICE

HOW THE BOARD CAN BE A COMPANY'S STRONGEST STRATEGIC ASSET

Peter Gleason
President of National Association of Corporate Directors

The world in which corporate boards operate has been transformed in fundamental ways in recent years. The operating environment has changed dramatically: Globalization, the ascendency of the internet, corporate scandals and financial crises have fundamentally altered the business risk landscape, unleashed mountains of regulatory requirements and prompted greater engagement between investors and companies.

All of these changes have resulted in greater director accountability and new areas of oversight, which is why the modern-day board must be one of the company's strongest strategic assets. This need to encourage self-driven transformation was the impetus for assembling the *2016 Report of the NACD Blue Ribbon Commission on Building the Strategic-Asset Board.*

Building boardroom leadership is no easy task, in part because director turnover remains low, particularly in the U.S. According to a 2015 NACD survey of some 1,000 public company directors, boards added 1.2 directors on average to either replace a director or expand the size of the board. That trend is drawing increasing scrutiny from the investor community. A recent report found

The board of directors can be a company's strongest strategic asset with a bit of nuanced strategy.

that 41 percent of the 413 shareholder activist campaigns mounted in 2015 were intended to unseat a director. In addition, the California Public Employees' Retirement System and the Council of Institutional Investors updated their proxy voting guidelines to call investors to consider length of service as an indication of independence.

Consider these statistics in conjunction with a few troubling boardroom trends. NACD public company survey data indicates that more than 50 percent of boards do not conduct individual director evaluations. In its own study, the Committee on Capital Markets Regulation found that, between 2010 and 2014, 85 percent of the directors who failed to receive majority shareholder backing remained in their board seats.

Although board composition has become a battleground issue, emphasizing change for the sake of change not only fails to get at the heart of the issue, it's a line of thought that can ultimately undermine the efficacy of the board. Specifically, director tenure becomes a target of public criticism. While some readily conflate length of service with an inability to provide independent oversight, long-standing directors can bring invaluable industry experience and institutional knowledge to boardroom deliberations.

This year's NACD Blue Ribbon Commission instead recommends a more nuanced approach that focuses on seven critical dimensions of continuous improvement for boards.

The key takeaways regarding board composition are as follows:

First, boards need to be proactive. There is a tendency for boards to push off evaluating composition and performance until an event demands it, be it a director's departure, an activist investor engagement, or a calamity that leaves the public at large asking: Where was the board? Instead, nominating and governance committees should use the company's strategic plan as the roadmap to determine what skills and capabilities are needed in the boardroom—not just today or next year, but three to five years out.

A proactive stance is also important in communicating board composition choices. Consider how investors might respond to the slate of directors and address any potential concerns well in advance of proxy season. Some boards, in addition to providing the basic biographical information required by the Securities and Exchange Commission in company filings, provide context that speaks to why each director was elected to the board and how they add value.

Second, boards need to have a long-term outlook. As part of their fiduciary responsibilities, directors should always consider the long-term needs of the organization in addition to short-term goals. As noted above, because the nature of doing business is rapidly evolving, it's important to evaluate not only how the skills represented on the board meet current demands, but also how they will meet future challenges. To this end, having a diversity of perspectives represented on the board can be critical to enriching boardroom dialogues.

In addition, continuing education programs can be a powerful tool in ensuring that all board members are staying abreast of the emerging business issues likely to impact their organizations. At the same time, sitting directors should not expect annual renominations as a matter of course. The skills that initially brought a director into the boardroom are not guaranteed to be relevant to the company's strategy in perpetuity. As such, directors need to keep the company's best interests top of mind and have the fortitude to step down if need be.

Third, maintain a pipeline of talent. Formulaic age- and tenure-limiting mechanisms can deprive the board of the richness and depth of knowledge that can only be brought to the table by seasoned professionals. Instead, determine an appropriate balance between retaining tenured directors and bringing on new talent. Candidates should be selected on the basis of how they will diversify the board's thinking and outlook. When bringing on new recruits, leverage institutional knowledge to onboard new directors and get them up to speed on the company and its governance processes so that they can actively and constructively contribute to boardroom conversations as soon as possible.

Another important element of board talent maintenance is performing regular evaluations at the full board, committee and individual levels. A third-party evaluation can be helpful in encouraging candid feedback on how well the board is functioning as a whole.

Aligning board composition with company strategy will ultimately drive long-term performance, and the recommendations of the NACD Blue Ribbon Commission report are designed to help boards look at themselves through a new lens. If boards pay attention to these factors, when it comes time to ask whether they are ready to confidently guide their organizations through the tumultuous year ahead, the answer will be a well-qualified "yes."

GOVERNANCE PRINCIPLES

Source: Report of the NACD Blue Ribbon Commission on Building the Strategic-Asset Board

SIX WAYS TO ENSURE AI CREATES JOBS FOR ALL, NOT JUST A FEW

Stephane Kasriel
CEO of Upwork

Whenever I talk to people about the potential impact of artificial intelligence (AI) and robotics, it's clear there is a lot of anxiety surrounding these developments.

And no wonder: These technologies already have a huge impact on the world of work, from AI-powered algorithms that recommend optimal routes to maximize Lyft and Uber drivers' earnings; to machine-learning systems that help optimize lists of customer leads so salespeople can be more effective.

We're on the verge of tremendous transformations in the way we work. Millions of jobs will be affected and the nature of work itself may change profoundly. We have an obligation to shape this future—the good news is that we can.

It's easier to see the jobs that will disappear than to imagine the jobs that will be created in the future. If, as *The Wall Street Journal* suggests, we think of AI as a technology that predicts, it's much easier to map its impact. We must push ourselves to do that and understand the future of work.

Here are six principles to keep in mind as we imagine how the world of work will evolve.

1. EXPECT MASSIVE DISRUPTION

As Klaus Schwab, founder and executive chair of the World Economic Forum, explains, we're in the midst of a "Fourth Industrial Revolution," after steam power (the first), electric power (the second) and digitization (the third). The fourth, which incorporates AI and robotics as well as other technologies, will have an even greater impact.

Of course, most new technologies create new opportunities at the same time as they eliminate old jobs, but there is rarely a perfect correspondence between these two forces. The people whose jobs go away aren't easily retrained for the new jobs, and that can lead to anger and social unrest—and, in the short term, massive inequalities across both geographies and groups of people.

It's essential to prepare for change by keeping abreast of new technologies, both in general and

in your specific field. Learn as much as you can and keep your skills up to date.

2. AI WILL REPLACE REPETITIVE TASKS MORE THAN JOBS

A recent study from the OECD poured cold water on earlier estimates that nearly half of American jobs are at risk of being eliminated by AI. Newer studies look at specific, repetitive tasks instead of whole jobs and find that, for most of us, some fraction of the work we do each day could be done better with AI. But for most jobs, computers aren't going to replace everything we do.

For the majority of us, AI will take away the most repetitive and boring tasks, enabling us to spend more time on creative problem-solving and on the parts of our jobs that involve complex human interactions and relationships.

To help prepare for this future, investigate AI-powered tools in your own field. Learn how to use them and exploit them to increase your own productivity.

TOP TEN SKILLS

Source: Future of Jobs Report, World Economic Forum

2015	2020
1. Complex Problem Solving	1. Complex Problem Solving
2. Coordinating with Others	2. Critical Thinking
3. People Management	3. Creativity
4. Critical Thinking	4. People Management
5. Negotiation	5. Coordinating with Others
6. Quality Control	6. Emotional Intelligence
7. Service Orientation	7. Judgement and Decision Making
8. Judgement and Decision Making	8. Service Orientation
9. Active Listening	9. Negotiation
10. Creativity	10. Cognitive Flexibility

3. MIDDLE-SKILLED JOBS WILL BE HIT HARDEST

The job market will not, however, be untouched by automation. The OECD estimates that 9 percent of U.S. jobs are, in principle, automatable. If that happens, it's going to have the worst effect on people with mid-level skills. Both mid- and low-level jobs will be the easiest to automate, but there's a stronger business case for replacing mid-level workers with machines because mid-level workers are more expensive.

If the people replaced by AI and robots aren't retrained well, they'll be forced to apply for low-skilled jobs, leading to an oversupply of workers at that level and depressing those wages even further.

At the same time, there will be fewer people qualified for high-skilled jobs, increasing wages in that segment. This dynamic, if unchecked, will hollow out the middle of the job market and lead to even greater polarization.

To mitigate the impact, society needs to provide education and job placement opportunities for those most affected by automation.

4. OPPORTUNITIES WILL BE UNEQUALLY DISTRIBUTED—AT FIRST

Over time, jobs will return. But they won't be the same kinds of jobs, and they will, in all likelihood, appear in different parts of the country from where automation destroyed jobs.

For instance, researchers Daron Acemoglu and Pascual Restrepo have examined the impact of robots on jobs in the U.S. What they found is a strong regional impact: For every new robot introduced in a particular metro region, an estimated 6.2 jobs were lost in the same geographic area. But when examining the country as a whole, they found that the impact was about half or equivalent to three workers losing their jobs for each additional robot.

One possible explanation is that the automation of industrial jobs in the Midwest and U.S. South is partially offset by new types of jobs in coastal cities.

But that's no comfort if you're living in one of the states with a net decline in jobs. Those who have lost their jobs need retraining, and we need an education system that prepares all U.S. children, not just a privileged subset, for the jobs of the future.

We also need to acknowledge the uneven geographic impact of automation and take steps, as businesses and collectively as a society, to increase opportunity in geographic areas that are affected adversely.

5. TECHNOLOGY DESIGNERS HAVE RESPONSIBILITY

The ethical mandate is not just in education, but also in the design of technology products themselves. Autonomous technologies are not value-neutral with respect to the jobs they impact. Carnegie Mellon robotics professor Illah Nourbakhsh makes the case in a recent podcast that the makers of robots and AI software need to think ethically. Are they creating technologies whose sole purpose is to replace human workers or are they facilitating human productivity and happiness?

Designers, computer scientists and CTOs all need to understand the ethical implications of how we create and use robots and AI. This needs to be a topic of discussion among business leaders on national and global stages. Merely calling for a universal basic income is sidestepping the question of how technology makers will account for human dignity and work in their very products.

6. THE LONG-TERM TREND CAN BE POSITIVE—IF WE MAKE IT SO

Eventually, after the Industrial Revolution, there were at least as many jobs as there were before, and they were better ones. The net result was an increase in productivity and in the number of people employed, which raised overall wealth. But that wasn't a foregone conclusion.

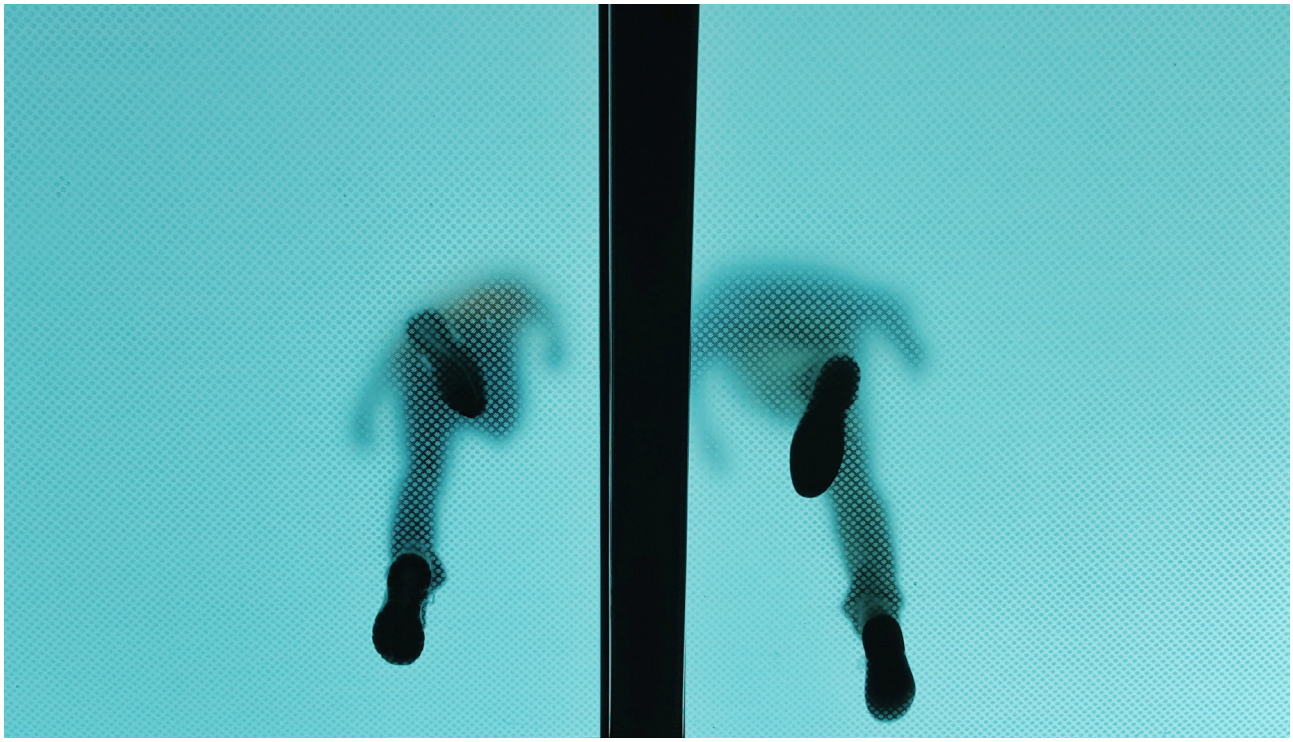
In the 21st century, we're facing a massive change in the technologies and types of jobs available, similar to that faced by our grandparents in the early 20th century. Like them, we can't be certain that both productivity and employment will rise.

We, as a society, need to make the commitment to guide our technologies responsibly and to capitalize on the prosperity we are creating, just as those who came before us did. That way we will ensure that AI technology creates opportunity for all, not just for a lucky few.

This piece first appeared on the Agenda blog of the World Economic Forum.

HOW A 10-MINUTE CONVERSATION WITH A MACHINE SAVED $12 MILLION

Colin Parris
Vice President for Software Research at GE Global Research



A call comes through on my tablet. It's a familiar digital voice letting me know that one of GE's power generation turbines installed at a utility customer's power plant was experiencing a change in its operating profile. This change was causing a critical part to wear more rapidly than usual. It would not necessarily cause a problem today, or even in the coming months, explains the caller. But further down the line, it could become an issue that would reduce the overall performance of the power plant and lead to more expensive repairs.

That voice on the other end of the line is not a human operator. It is the turbine's digital twin, an exact digital replica of the physical machine built with artificial intelligence algorithms that allow it to see, think and act just like human beings do. In my ten-minute conversation with this digital twin, we figure out a solution that will save $12 million for the customer with a simple adjustment in how the turbine operates. The drop-off in performance and higher repair costs will be avoided thanks to a few simple changes the twin itself recommended based on its assessment of historical data, other turbines in the fleet, and its deep knowledge of the physical stress on the turbine in question.

The Internet ushered in the world of connectedness on a level no one had previously imagined. Today, that connectedness has spread from human-to-human, to human-to-machine, to machine-to-machine, and we've given it a new name: the Internet of Things. We see the Internet of Things (IoT) in the home when we talk to Amazon Echo's Alexa or to Google and ask them for information or to perform a simple task. To understand those questions and requests, Alexa uses a dictionary from Wikipedia—and its capabilities are developing quickly, since much of the digital infrastructure of the consumer IoT is already in place.

The industrial IoT is developing even quicker, despite exponentially higher technological and regulatory complexities. Industrial devices—like a power generation turbine, a jet engine, a locomotive, or an MRI

machine—are beginning to be linked via a digital thread. We're building the knowledge domains for digital twins, introducing industrial terms like shroud, nozzle, blade and spallation (that engineers might associate with a jet engine, for example). As the digital industrial dictionary grows, conversations with industrial digital twins will be like those with Alexa, but the economic, societal and financial stakes of this back and forth will be much higher.

Recently, Gartner, one of the world's leading information technology research firms, cited the digital twin in its 2017 list of top 10 tech trends.

Just consider that unscheduled maintenance events with aircraft not only cause great stress and inconvenience for passengers because of flight delays and cancellations, but they also cost the global airline industry an estimated $8 billion according to The Future of Work report published by GE. Eliminating unplanned downtime is routine with the digital twin, which can mitigate airline costs and the inconvenience and stress caused by travel delays. In renewable power, the ability of digital twins on wind farms to talk with each other and to share and act upon insights about factors such as the prevailing wind direction has contributed to making wind cost competitive and helps to reduce our carbon footprint.

We value the contributions of digital twins in the hundreds of millions of dollars. A more specific number is impossible to predict, but if a simple adjustment in a steam turbine's operation saved a company $12 million, the possibilities of what the digital twin can do are endless.

The digital twins' impact on the industrial worker is also worth noting. From the outside, it seems as though the digital twin has taken the job previously done by a human. But no human spends time watching one single turbine or jet engine. Technicians are called when an asset has already broken. The digital twin gets ahead of the problem. This allows for the technicians to better plan their days and eliminate their own downtime. Those who don't service machines but work with them—techs operating the ultrasound, nurses and doctors, etc.—can focus their time on their patients, clients, and customers. Instead of eliminating jobs, the digital twin will enrich them by letting humans focus on personal development, new ideas and interpersonal interactions.

Unlike many of their industry and enterprise precursors, the twins are not just big data crunchers. Through their machine learning and AI capabilities, they continually learn, adapt and change even as the physical machines and their environments change. So a twin of a 20-year-old jet engine will act and think differently than a twin of a newly minted one.

In health care, you often hear doctors tell you to "listen to what your body is telling you" to remain healthy and feel as good as you can. That's what we're now able to do in industry with digital twins. The twins have given industrial machines a mind and a voice to speak their mind. We can listen to what our machines are telling us, so that our customers can receive the highest level of performance, productivity and efficiency possible.

The industrial IoT is manifested through the arrival of the digital twin and it's disrupting how industry will work in the future. For GE and the rest of the industrial world, this means trillions of dollars in new growth opportunities. The digital twin will become a major pillar of the data economy for industry. To date, we have only just begun to scratch the surface of the immense impact the twin will have in years to come.

All views expressed are those of the author.

This piece first appeared in the Perspectives section of GE Reports.

T-MINUS 11 MONTHS FOR EU PRIVACY REGULATION

Omer Tene
Vice President of Research and Education at International Association of Privacy Professionals

With fines of up to 20 million euros ($23 million) or four percent of global annual turnover—which, for Fortune 100 companies, could reach billions of euros—and new rules on a right to be forgotten and data portability, the European General Data Protection Regulation (GDPR) has grabbed the attention of compliance professionals and C-level executives alike. Far from being just a European law, the GDPR extends to companies that handle any European's personal data all over the world. As less than a year remains until the date of its implementation, the GDPR requires companies to quickly devise and implement comprehensive data governance programs.

The GDPR introduces new obligations on matters such as data subject consent, data anonymization, breach notification, trans-border data transfers, and appointment of data protection officers. In addition, it requires companies that handle the personal data of people in the EU to undertake major operational reforms, implementing new governance mechanisms and technological tools.

Companies that already have well-developed privacy programs have less work to do. The GDPR follows the general outline of the 1995 data protection directive and codifies many existing industry best practices. But it also changes the game in some innovative

Companies that have well-developed privacy programs have less work to do in preparation for the EU's new GDPR.

ways. For example, companies need to adapt to new rights and obligations, such as the right to be forgotten and the restriction on profiling, and implement these rights into their products and services.

Companies that are starting from scratch are in for a lengthier journey. They must first understand the scope of application of the new regulation and whether it applies to their activities. Next, they must set up a privacy program, including appointment of a data protection officer (DPO) and appropriate training for staff. Finally, they should build lasting internal accountability mechanisms to map data flows, document privacy impact assessments and deploy privacy by design and by default.

This brief overview serves as a primer to the scope of the GDPR and the provisions that may prove most significant for companies that seek to avoid its substantial penalties.

SCOPE OF GDPR

The GDPR applies to any organization that is established in the EU, offers goods or services to individuals in the EU, or monitors the behavior of individuals in the EU For example, a developer of a dating app that is based in California—but used by thousands of individuals in the UK, Netherlands, and France—is subject to the GDPR, even without any physical presence in Europe.

The GDPR regulates the collection, storage, use and disclosure of personal data—that is, data about identifiable people. This means the GDPR only applies to data about individual human beings, not companies, governments or other organizations. Trade secrets or confidential government information may need to be protected, but since those types of information do not relate to an individual, they are not personal data and are not covered under the GDPR.

It is important to realize that "personal data" under the GDPR is not necessarily sensitive. It could be as mundane as a name, email address or telephone number. Moreover, to be protected, personal data need not be secret. In fact, even publicly available data, such as a class roster or a public comment with a name attached, is considered personal.

The GDPR distinguishes between two types of entities: controllers and processors. This is an important distinction since controllers bear ultimate responsibility for any activity with respect to their customers' and employees' data, even if stored or analyzed by third-party processors. A controller is defined as the entity that "determines the purposes and means of the processing" of personal data.

Processors are entities that actually process personal data on behalf of controllers. For example, a real estate firm may outsource its payroll to a separate company. In this case, with respect to its employees' salary data, the real estate firm is the controller—the entity that controls the information and decides how it is treated. The company processing the payroll information is the processor—responsible for handling, storing and distributing the data to employees, financial institutions and tax authorities.

START WITH EXPERTISE

Once an organization determines it is subject to the GDPR, it must proceed to create a privacy program. Importantly, the GDPR requires certain companies to designate a DPO if their data processing activities fit either of two situations:

- The "core activities" of the company involve "regular and systematic monitoring of data subjects on a large scale"
- The company conducts "large-scale" processing of "special categories" of data, including any data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership," as well as "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

The DPO must be a person with "expert knowledge of data protection law and practices" who reports directly to "the highest management level" of the controller or processor. The job of a DPO involves monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, training data processing staff, and conducting internal audits. The DPO also serves as a point of contact for data subjects and data protection authorities. Given the broad scope of the DPO requirement, experts estimate that the GDPR will drive a thriving market for tens of thousands of data protection professionals in Europe and beyond.

BUILD A LASTING PRIVACY PROGRAM

Privacy professionals use a set of consistent and scalable tools to implement effective data handling practices throughout a company. Chief among these tools is the privacy impact assessment (PIA), a practice that assesses the risks

associated with the processing of customer data at the beginning of any operational process.

PIAs aim to reduce the risks to organizations and data subjects created by misuse of their personal information by mapping data flows, prescribing lines of control, limiting use to specified purposes, and ensuring proper disposal. Under GDPR, privacy pros must also incorporate "privacy by design" and "privacy by default," ensuring that privacy is part of the product development cycle from conception to implementation. When coupled with a robust understanding of the GDPR's requirements, incorporating these practices will help companies to comply with global privacy norms.

A robust privacy program must also implement processes to accommodate the new rights of data subjects under the GDPR: the right to be forgotten and the right to data portability. The right to be forgotten allows subjects to request deletion of personal data and removal from publication. Controllers must comply unless maintaining the information is in the public interest or necessary to defend against legal claims, or where deletion is outweighed by freedom of expression. Additionally, if an individual requests removal of personal information that has been made public, the controller must take reasonable steps to inform other parties that already process the same data about the request.

The right to data portability requires controllers to provide personal data to the data subject in a commonly used machine-readable format and to transfer that data to another controller upon an individual's request. This will no doubt stoke competitive tensions with companies that try to preserve their existing customer base.

DON'T FORGET THE DETAILS

The GDPR creates clear lines of accountability between controllers and processors. It expands the controller's responsibility for processing activities and sets out specific rules for contractually allocating responsibility between a controller and processor. Liability under the GDPR falls primarily on the shoulders of the controller. But if a processor acts as a controller or outside the scope of authority granted to it, then it is treated as a controller for purposes of that processing.

Processors' duties include the requirement to process data only as instructed by a controller, to use appropriate technical and organizational measures to ensure data security, to delete or return data to the controller once processing is complete, and to submit to specific conditions for engaging any sub-processors. In the event of a data breach, processors are required to notify controllers, who are themselves required to notify data subjects and data protection authorities.

Consistent with the recent trend toward regulating the transfer of data across national lines, the GDPR only permits personal data to be transferred to countries outside of the EU under certain conditions. The path of least resistance is an "adequacy decision" from the European Commission, which designates a receiving country as "adequate" under European data protection standards.

Absent adequacy, however, cross-border transfers may still be possible, but companies are required to put in place time-consuming expensive solutions such as standard contractual clauses or binding corporate rules.

CHALLENGE AND OPPORTUNITIES

The GDPR presents a challenge and an opportunity for companies. In our data-driven modern economy, the potential mismanagement of customer data is a serious risk both to companies' brands and consumer trust.

Improper handling of data can expose companies to enormous reputational harm and civil liability. Companies that succeed in implementing privacy practices from the ground up will have a competitive advantage. The GDPR is simply a catalyst, providing a legal incentive and a due date for implementation of best practices for data privacy.

IAPP's Westin Research Fellows, Cobun Keegan and Calli Schroeder, assisted with this article.

TECHNOLOGY

CYBERSECURITY REGULATION ON THE RISE: IS YOUR COMPANY PREPARED?

Pamela Passman
President and CEO of Center for Responsible Enterprise and Trade

Data breaches and other cyber incidents are on the rise and on the agenda for corporate boards and the C-suite, and for good reason: Loss of customer information, trade secrets or other confidential assets can significantly diminish a corporate reputation, financial standing and competitive advantage.

However, these aren't the only risks for companies. The diversity and complexity of cybersecurity risks, and their evolving character, have caused governments to respond in many different ways. Some have taken action directly to require the cybersecurity of various public and private networks and systems, while others have encouraged the development of voluntary frameworks and best practices that industries can choose to adopt.

This rising tide of cybersecurity regulation and recommendations further complicates the landscape for companies. These new requirements are often inconsistent among different governments, between agencies of the same government and from industry to industry. One of the major unknowns for companies is whether they can embrace one overall information security framework, or whether they will face a splintered environment with an unmanageable number of different corporate, industry and government requirements, standards and practices.

The rising tide of cybersecurity regulation and recommendations complicates the landscape for companies.

NEW AND EXPANDED CYBERSECURITY REGULATION

Governments around the world have adopted or are considering legislation that would specifically impose cybersecurity requirements on industry in various ways. For example, more than 240 bills, amendments and other legislative proposals dealing with cybersecurity have been introduced in the U.S. Congress in the past three years.

Requirements fall in a variety of categories. Some are direct requirements to implement cybersecurity protections. For example, companies in the critical infrastructure sector now face regulation in the U.S. and similar requirements in Europe and Asia. Government departments are also seeing a rise in cybersecurity requirements, such as risk assessments, training and controls. Trade secret protection laws also require "reasonable steps" be taken to keep information confidential from cyber threats.

For publicly traded companies, securities laws and shareholder expectations are increasingly demanding that those companies safeguard their confidential information and reputation against cyber-attacks—or face administrative penalties and civil damage remedies. This is particularly true in the U.S., where shareholder litigation and some Securities and Exchange Commission guidance and enforcement have already been launched.

Governments around the world are also increasingly insisting that contractors and suppliers that wish to do business with the government also closely manage cybersecurity risks at their own firms and among subcontractors and suppliers.

The shared view among governments and industry is that cybersecurity is an important and growing problem, and that many existing practices are inadequate or inconsistent. Yet, while there is a common appreciation of cyber risks, at least at a high level, there is little coherence in these efforts, even within national borders, and even less coordination internationally.

GROWING USE AND IMPORTANCE OF CYBERSECURITY FRAMEWORKS AND STANDARDS

With cybersecurity regulation on the rise, how can a company prepare? To help companies seeking to address these new requirements, governments and the private sector are working together to develop security frameworks and guidance designed to protect confidential information more effectively from cyber risks.

The voluntary Framework for Improving Critical Infrastructure Cybersecurity, developed by the National Institute of Standards and Technology (NIST) unit of the U.S. Department of Commerce, is to-date the most comprehensive, risk-based tool for managing information security. U.S. federal government agencies are enthusiastically embracing the NIST Framework. One recent survey of 150 federal government IT and security professionals found that 82 percent are using the NIST Framework to improve their security, while 74 percent say it serves as a foundation for their own cybersecurity roadmap.

The NIST Framework is also being reviewed and considered by governments and the private sector internationally. NIST itself has been meeting with European and other governments and information security bodies, including the European Commission, the UK, Italy, Poland, Romania and others, to discuss how the NIST Framework and other approaches could be aligned on a global scale.

To date, use of the NIST Framework is voluntary. Compliance with the Framework is neither mandatory as a condition for government contracting nor is NIST the formal standard against which information security practices have been measured in litigation following data breaches. However, the landscape is changing. The trend to promote such guidelines—and in particular the NIST Framework—seems likely to develop into more mandatory requirements, to which other cybersecurity measures will be mapped.

The NIST Framework could very well be the guideline that courts and regulators will use to determine whether companies are managing data security adequately in a range of legal contexts.

Other information and cybersecurity standards are also proliferating. The principal information security standard at the international level is ISO 27001, which many companies are implementing and are seeking certification of their compliance. The NIST Framework—although structured quite differently than this ISO standard—includes and makes numerous references to particular ISO 27001 requirements.

IMPLEMENTING LEADING PRACTICES

Cybersecurity tools and standards such as the NIST Framework and ISO 27001 are proving useful to companies and other organizations. Use of a risk management program, such as the NIST Framework, provides the opportunity to bring some uniformity and cost-effectiveness to the varying cybersecurity efforts and requirements that have been developing to date. Such an approach can also help organizations assess, manage and respond to their particular cyber risks more effectively, both internally and down the supply chain.

The bottom line for agencies in the public sector, government contractors, the U.S. and multinational companies: Given the flood of new cybersecurity regulation, the use of leading practices such as the NIST Framework may become virtually, or actually, mandatory. Thus, taking steps now to implement protections will position organizations to proactively meet these ever-evolving cybersecurity requirements.

IN PRACTICE

FIVE PRINCIPLES FOR STRONGER BOARD OVERSIGHT OF CYBERSECURITY

Robyn Bew
Director of Strategic Content Development for the National Association of Corporate Directors

One of the most important jobs of the board is to challenge management and test their assumptions about strategy, the competitive environment, and associated risks and opportunities. Many directors would say that they are most passionate about this part of their role, and in today's business environment it has never been more critical. Cybersecurity is a common theme in such discussions, because it's a significant enterprise-wide risk and strategy issue that affects all organizations.

Just by reading the news headlines, it's clear that cyber risks can have an impact well beyond technology—they affect new business plans and product/service offerings, mergers and acquisitions, supply chain and purchasing decisions, and major capital investment decisions such as facility expansions and upgrades, R&D processes, HR policies and more. As a result, cybersecurity has moved out of the IT silo and sits front and center on boardroom agendas.

Yet 97 percent of respondents to NACD's most recent survey of board members still find cyber-risk oversight challenging (about 60 percent say it is "somewhat or very" challenging), and only 14 percent of directors believe their board has a high level of knowledge about cyber risks.

To help directors make headway on this critical issue, NACD and the Internet Security Alliance recently released an updated edition of the *Director's Handbook on Cyber-Risk Oversight*. It is built around five core principles that apply to boards of organizations in all sizes and sectors:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

5. Board-management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

The five principles help directors to establish processes that support high-quality dialogue on cybersecurity matters. Key takeaways include:

- Understand the specific cyber threats that are most material to the organization. Ask questions such as: What are our organization's most critical data assets? Where are they located? Who has access? How are they protected? From there, the board can work with management to determine the level of cyber risk the organization is willing to accept in the course of its operations, and how cybersecurity resources and investments will be allocated.

- Stay informed by internal and external counsel about the changing legal and regulatory landscape, including industry-specific rules and requirements, as well as those that are applicable at the state/region, national, and international levels.

- Set clear expectations about the format, content, and level of detail of the cybersecurity information management provides to the full board and to key committees.

- Bring additional expert perspectives on cybersecurity into the boardroom by scheduling deep-dive briefings with third-party experts, leaders from government agencies and law enforcement, and/or by leveraging the board's existing independent advisors.

- Individual directors can take advantage of opportunities to enhance their own cybersecurity awareness and knowledge by participating in relevant director education programs.

For some companies in select industries, cyber expertise on the board may indeed be the right decision. NACD believes that responsibility for board composition and director recruitment belongs with the nominating and governance committee: The group that is specifically charged with filling current and future skill requirements on the board. They have the best firsthand knowledge about what the board needs, and are in communication with the company's investors to hear their perspectives.

But directors don't need to be technologists or cyber experts to play an effective role in cyber-risk oversight. Like any other significant business risk, cyber-risk oversight requires directors to have a thorough understanding of the company's business model, experience in strategy and leadership, sound business judgment, and the ability to constructively challenge management—in other words, the fundamental elements of high-quality board leadership. And improving the effectiveness of cyber-risk oversight practices can and should be part of every board's continuous improvement activities.

Fast facts

51%

Directors who report that they are "very confident" their company is properly secured against cyberattack

146

Median number of days an organization is compromised before discovering a cyber-breach

15%

Directors who say they are "very satisfied" with the quality of cybersecurity information the board receives from management.

53%

Cyberattacks first identified by law enforcement or third parties, rather than organizations who have been attacked

$2 trillion

Projected annual cost of cybercrime by 2019

Source: NACD

EU'S NEW DATA REGULATION REQUIRES ACTION NOW

Peter J. Beshar
Executive Vice President and General Counsel for Marsh & McLennan Companies

The countdown has begun. In May 2018, the European Union's General Data Protection Regulation (GDPR) will come into force and impose sweeping new obligations on organizations and their handling of personal data. The rapporteur assigned by the European Parliament to lead the negotiations around the GDPR, Jan Philipp Albrecht, boldly declared that the new regulation "will change not only the European data protection laws but nothing less than the world as we know it."

The harsh reality is that most companies—large and small—will struggle over the next 300 days to comply with the regulation's myriad requirements.

Indeed, the scale of this task and its potential complexity was underscored earlier this month when Germany became the first EU member state to pass national legislation implementing the GDPR. While the GDPR will apply directly to the EU's 28 member states, many of them are expected to adopt implementing legislation that will tailor certain aspects of the GDPR to their national laws. As an example, the just-passed German Data Protection Amendment Act imposes slightly different obligations with respect to the process for obtaining employee consent, for utilizing closed-circuit televisions to monitor security in publicly accessible spaces and for conducting scientific research.

PRIVACY AS A FUNDAMENTAL RIGHT IN EUROPE

Before looking forward, it is helpful to consider the historical context for these new laws. First, in the wake of World War II, Europeans enshrined the right of privacy as a fundamental human right in Article 8 of the European Convention of Human Rights.

Half a century later, the internet and the smartphone have changed the way that we live. With these new technologies, both companies and the government developed unprecedented abilities to track individuals' profiles, aggregate

consumer data and use algorithms to predict habits and preferences.

As these capabilities developed, however, so did a strong belief across Europe that privacy rights were being eroded. It is against this backdrop that European authorities felt compelled to act to limit, control and expose the sweeping collection and use of personal data.

THE CORE ELEMENTS OF THE GDPR

In elevating the rights of consumers, the GDPR represents a sea change in how companies will have to operate. While the regulation is nearly 100 pages long, four themes dominate its core

1. Individuals will have enhanced tools to protect their right of privacy.
2. Companies will be forced to reassess the manner in which they process and retain data.
3. Companies will need to review their contractual arrangements with a host of third parties.
4. Companies will be held to far stricter accountability and sanctions.

Those companies running afoul of GDPR provisions could incur fines of as much as 4 percent of their global turnover. According to Oliver Wyman research, fines and penalties in the first year may exceed $6 billion, for Financial Times Stock Exchange (FTSE) 100 companies alone.

SWEEPING JURISDICTION

The GDPR's reach potentially extends beyond the EU borders, as its focus is its citizens' personal data. The GDPR applies to any organization that collects or processes personal data in connection with the offering of goods or services to EU citizens, or monitoring of such citizens' behavior, regardless of where the organization is located. Accordingly, its data privacy protections, and requirements, follow wherever the data travels. In practice, the broad jurisdictional provisions mean that the GDPR's complex regulations will have a global impact.

BREACH NOTIFICATION

For the first time, European companies will be required to notify regulatory authorities, and potentially consumers, in the event of a significant cyber breach. Following the Dutch implementation of a "mini-GPDR" in 2016, thousands of incidents were disclosed to the Dutch Data Protection Authority within months. Extrapolating this sample across the entire EU provides an early window into the likely ramifications for management teams and supervisory boards.

DATA SECURITY

The GDPR provides guidance on practices to protect data, such as delinking data from names ("pseudonymization"), encryption, regular assessments of technical controls and incident response plans for maintaining the confidentiality and integrity of data. To ascertain what controls are needed, companies will need to undertake privacy impact assessments and consider engaging external experts. Businesses can expect regulatory authorities, the media and individuals to scrutinize their data practices.

AFFIRMATIVE CONSENT AND THE "RIGHT TO BE FORGOTTEN"

The GDPR prohibits any company from collecting personal data without first notifying users of how their data will be stored, processed and protected. It also requires that any individual consent obtained for processing data be "freely given, specific, informed and unambiguous." This "affirmative consent" will potentially require users to click on a consent notice or take other measures to affirmatively demonstrate agreement to allow for the data collection.

The GDPR will also codify the "right to be forgotten," which allows individuals to demand that personal data be deleted so that it cannot be searched online by third parties. European courts have already recognized that this right exists and currently are considering how broadly it can be applied on an extraterritorial basis.

GLOBAL WEB OF CYBER REGULATION

Europe is far from the only government authority seeking to impose greater data and cyber protections on business. Earlier this year, the New York State Department of Financial Services adopted the most comprehensive set of cybersecurity requirements in the United States. The DFS regulation imposes new requirements around concepts such as multi-factor authentication for password protection, encryption at rest and protocols for patching software vulnerabilities (think the WannaCry and Petya attacks).

There is a growing awareness of the cybersecurity threat in Asia, as evidenced by China's new cybersecurity law and its "data sovereignty" requirements. Given cybersecurity threats and this expanding matrix of new regulation, including the GDPR, business leaders may wish to consider one or more of the following steps:

Set a tone at the top of awareness and urgency.

Executives should assert leadership regarding—and take ownership of—cyber risk. Data security is not the sole responsibility of the IT department. The threat is simply too great and cuts across multiple departments within organizations.

Identify translators.

Too often, the technical team responsible for information technology (IT) security speaks a language the C-suite does not understand. Executives need to have translators in place who are able to understand both the technical requirements of the company's systems and the reputational risk to the company's brand.

Implement best practices.

The WannaCry and Petya ransomware events drove home the importance of developing consistent protocols for patching known software flaws. The GDPR and other regulations will require a similar awareness around data processing and privacy issues. In addition to implementing security measures such as firewalls, penetration testing or "detonation" software, has your organization conducted a credible tabletop exercise simulating a cyber attack?

Start communicating with customers and shareholders now.

Companies should prepare their stakeholders for an era of greater transparency and disclosure and the almost inevitable day when a cyber intrusion occurs. Help your customers understand how you collect and use their personal data, and how you are complying with regulations.

Make up for lost time.

The penalties for noncompliance with the GDPR are severe. Executives should reach out to regulators, law enforcement authorities and policymakers—not so much to lobby, but rather to share insight, information and help shape the rules as they evolve.

No one has all the answers. Corporate leaders should act today to give their companies the best chance to adapt to a new world order that offers both great opportunity and substantial risk.

Executives should take ownership of cyber risk. Data security is not solely the responsibility of the IT department.

THE EU'S NEW DATA REGULATION CREATES OPPORTUNITY FOR CHANGE

Peter Johnson
Cyber Leader for Marsh UK

The challenges faced by organizations as a result of the European Union General Data Protection Regulation (GDPR) are substantial. While many of the headlines to date have focused on the potentially sizeable penalties and compliance issues, little attention has been given to the opportunities the GDPR presents for proactive organizations. Key among those are enhancing their data security capabilities, developing a deeper relationship with customers and growing their business.

The GDPR, which represents the most significant change to data protection law in Europe in 20 years, is scheduled to take effect on May 25, 2018. New data protection legislation is certainly overdue. European Directive 95/46/EC, from which the current Data Protection Act 1998 (DPA) derives and which the GDPR replaces, preceded both the internet boom and the birth of social media.

Nowadays, we hear near-daily announcements of new ways that technologies are changing lives and business strategies. Along with that comes numerous cyber attacks aimed at disrupting business and stealing private information or holding it for ransom. It's no surprise, then, that a recent survey from software firm SAS found that 62 percent of United Kingdom respondents welcomed the GDPR provision for the right to erase personal data from certain systems, or that about half of Americans feel their data is less secure than it was five years ago, according to the Pew Research Center.

Data privacy and the right of individuals to choose and control how their data is used and accessed have not kept pace with technological advancements and the digital economy. Along with a loss in consumer trust regarding

The GDPR can repair the breakdown in trust between consumers and organizations in terms of personal data security.

organizations' use of personal data, an impact can be seen on profitability as the number of consumers using ad-blocking software continues to increase.

SEEING THE OPPORTUNITY IN CHANGE

Some organizations will consider compliance with the GDPR a costly and disruptive undertaking. On the other hand, forward-thinking organizations will see it in a different light. They will embrace the challenge to develop their technology and their information management and cybersecurity systems. For too long, many organizations have captured swathes of data without proper protocols surrounding its processing, storage and sharing. Many have lacked an understanding of data's relevance and value to their business, or of consumer preferences on how it is used.

The GDPR and its requirements should help to reduce the staggering cost of cybercrime to the global economy, where estimates range from hundreds of billions to trillions of dollars. Organizations that embrace the GDPR are likely to take steps that enhance cybersecurity and therefore reduce the potential for data loss, operational disruption, physical damage and reputational and brand damage.

Organizations' levels of understanding around cyber risk continue to increase, due in part to continued high-profile cyber incidents, including the recent WannaCry and Petya ransomware attacks. There is still a long way to go for many in order to map and quantify their cyber exposure and establish the cultural change required throughout their organizations.

Under the GDPR, some organizations will face an additional requirement to appoint a Data Protection Officer (DPO) whose role will be to independently supervise compliance with the GDPR and advise staff who deal with personal data. It is hoped that the requirement that DPOs report into the highest management level of their companies will help promote a cyber-risk culture and may even improve board-level ownership of cyber risk within these organizations.

CONSENT AND TRANSPARENCY: A NEW RELATIONSHIP WITH THE CONSUMER

The GDPR aims to provide EU citizens with greater control over the use of their personal data. Some organizations, no doubt, worry about how that will manifest and the potential for consumers to deny them access. As pointed out in a recent study by Lippincott, consumers are increasingly willing to give that consent to companies they trust and with which they want to develop a meaningful relationship.

The customer of the future "expects everything to be precisely tailored to her, especially with all of the data she gives up," Lippincott notes, adding: "Be transparent. ... (The consumer's) trust goes to crowd-verified, fully transparent products and processes, so open up your customer experience for full accountability. Ground your trust in transparency, not authority."

Central to this transparency is consent, and there are challenges: The threshold for consent under the GDPR is higher than under existing legislation. To meet the new requirements, consent needs to be freely given, specific, informed and unambiguous.

Businesses must be able to demonstrate these elements when relying on consent for processing. Special categories of personal data, such as health information, will require explicit consent. When an organization relies on consent to process an individual's personal data, the individual will have the right to withdraw that consent at any time.

They will also have the right to obtain and port their personal data for their own purposes across different service providers ("data portability"), as well as an enhanced right of erasure (the "right to be forgotten"), should they wish to do so.

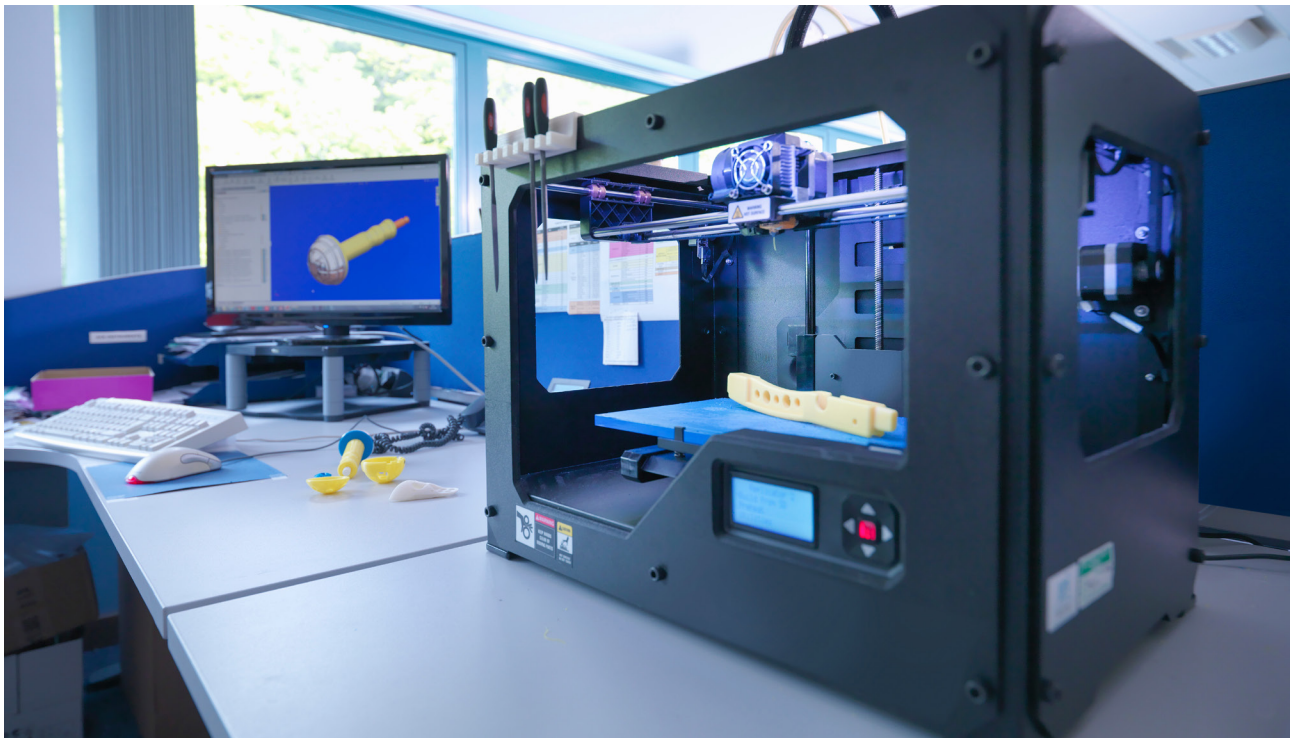
Consent must be a positive indication of agreement that personal data can be used in the specific manner and for the specific purposes set out by the controller. A pre-ticked box will not be valid consent. Consent requires engagement, and engagement enables businesses to better understand the needs and desires of their customers and develop a relationship based on trust and transparency.

Overall, the GDPR will provide an impetus to improve data security and controls around the use of personal information. In turn, it presents an opportunity for organizations to better understand their data and how it may be used to add value to their business. Most importantly, it is hoped that the actions required of organizations to comply with GDPR will go a long way toward helping to repair the recent breakdown in trust between consumers and organizations in terms of how personal data is used.

This can only be done if companies move away from viewing the GDPR as a compliance-driven tick-box exercise and embrace it as an opportunity, a means to improve data management strategies in such a way that drives their business forward.

TAKING CHARGE OF DISRUPTIVE TECHNOLOGY RISKS

Brian C. Elowe
Managing Director and U.S. Client Executive Practice Leader at Marsh



There's a lot of talk these days about disruptive technology—3-D printing, autonomous vehicles, blockchain and more. It's easy to find breathless descriptions of a world gone digital, be it the promise of connecting all the world's people to all the world's knowledge or the perils of poorly governed artificial intelligence running amok.

Despite the abundance of information on disruptive innovation, our research raises questions about the level of discussion companies are having about managing the risks of disruptive technology. The 2017 *Excellence in Risk Management* project from Marsh and RIMS, the Risk Management Society, looks at an array of issues around disruptive technology risks. For this survey, disruptive technology was defined as "one that purposefully displaces an established technology and alters an industry or way of doing business—including jobs—or a ground-breaking product that creates a completely new industry."

For some companies, a lack of focus on such risks will bring financial difficulty; for those with foresight, a focus on the risks will enhance the opportunities.

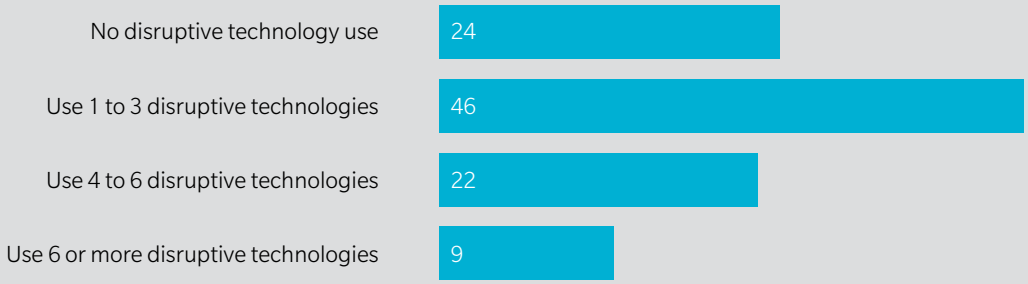
A surprising number of respondents (24 percent) acknowledged that they do not use or plan to use any of 13 common disruptive technologies; the numbers were even higher around individual items.

For example, 48 percent of risk executives told us their organization doesn't use or plan to use the Internet of Things (IoT); yet, according to many estimates, 90 percent of companies will be using IoT technologies within two or more years. Similarly, only 25 percent of our respondents said their organization uses or plans to use wearable technologies, while studies show 93 percent of companies across a range of industries are already evaluating or using them.

Such disconnects show a gap in understanding: Too many risk executives don't seem to realize the pervasiveness of these technologies. Perhaps they are simply mesmerized by the "gradual evolution rather than radical change" with which technology now disrupts the business world. But companies cannot afford to be surprised when technology fails or goes awry.

HOW MANY DISRUPTIVE TECHNOLOGIES IS YOUR ORGANIZATION USING OR PLANNING TO USE?*
(Percent of respondents)

Source: Marsh, RIMS; Excellence in Risk Management



* Numbers add up to more than 100% due to rounding

Risk executives need to fortify their strategic role by understanding how technologies impact not just their own operations and business models but also the direction of entire industries—both theirs and related ones.

ALIGN AND ASSESS

A primary responsibility for any risk executive is to ensure that new and emerging risks are being identified and assessed. Yet we found a significant number (60 percent) of respondents saying no risk assessment is being done for disruptive technologies. That should make people nervous given the impact that disruptive technology can have on an organization's strategy. In fact, such lack of attention to the risks should be viewed as unacceptable.

From a liability standpoint alone these innovations may upend the status quo. Look at a driverless car or truck or train. When the vehicle of the not-so-distant future is involved in an accident and injures a pedestrian or damages property, will that be the fault of the owner, who is not actually driving the vehicle? Will liability fall to the vehicle manufacturer? What about the software designer who built the algorithm to "tell the car" what to do leading up to the accident?

By definition, disruptive technologies can make or break a business. Assessment and analysis of the risks need to be integrated into existing business strategy decisions. Why, then, this lack of focus on assessing disruptive risks? "Other areas have greater priority," was the top answer when respondents were asked about the biggest impediment to understanding disruptive technology risks.

But today's risk executives need to develop insights that will help leadership prepare for the unexpected. Disruption from technology is an area that unexpected events will no doubt emanate from and should be treated as a priority.

TAKE CHARGE OF DISRUPTIVE RISK

The transformational changes that come with managing disruptive technology risks can be difficult. So what can be done now to help organizations map out the way forward?

First, understand.

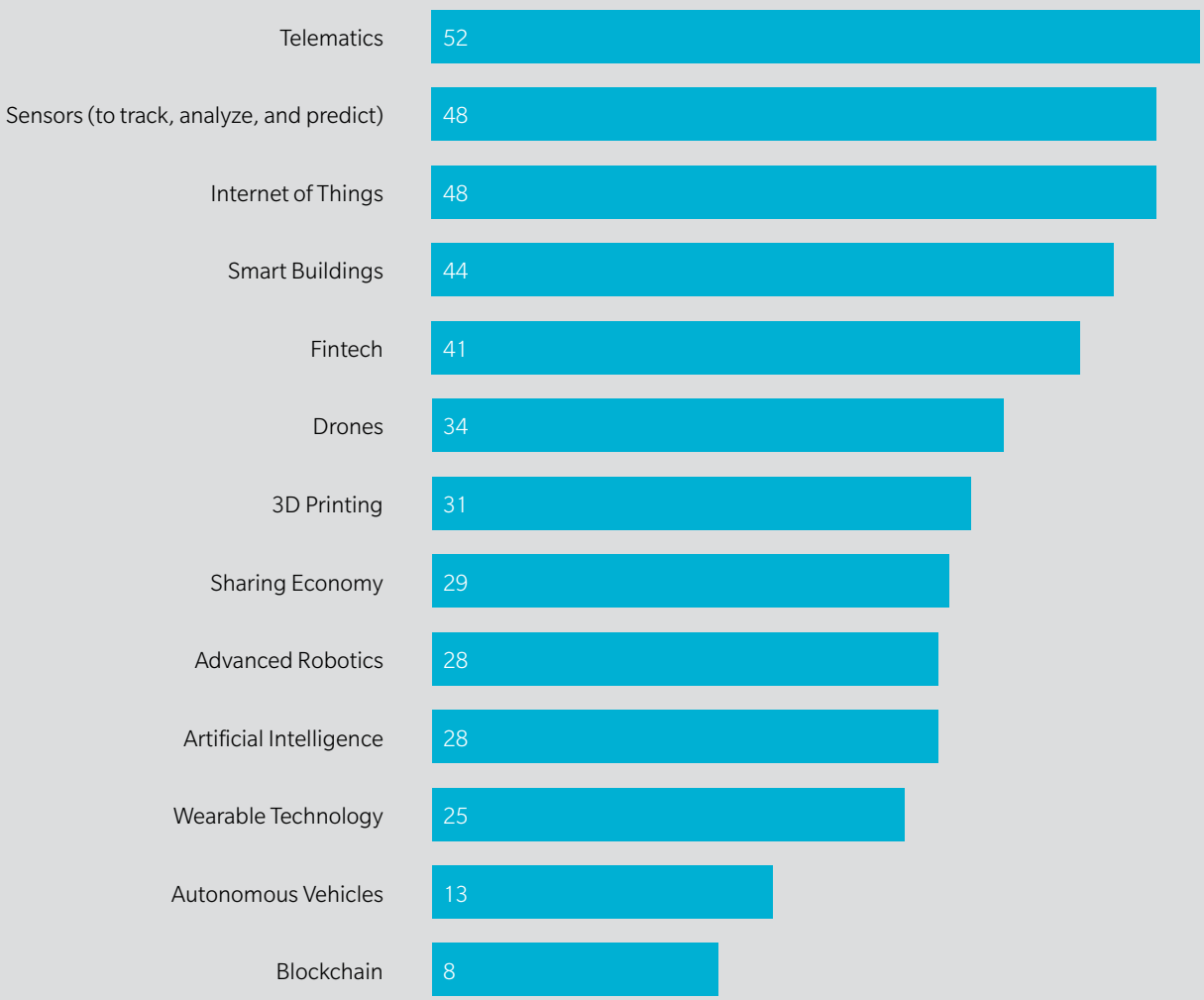
You need to know what disruptive or innovative technology is. What is your organization already using? What is coming? If our *Excellence* survey is any indication, this is a dangerous gap that needs to be bridged by risk executives.

The pace of innovation is truly fascinating. As our colleagues at Lippincott put it: "There is no more important question to answer than 'What is the big, unstated need of tomorrow?' The answer is deep, constant, and insatiable inquiry." Educate yourself on terminology, on leading-edge innovations, about hits and misses, emerging risks, and other disruptive technology topics, especially for those your organization or industry is using or planning to use.

In doing so, expand your network, the people and places you turn to for answers and ideas. There may be other industry sectors with experts you don't typically tap into that can help you to better understand how disruptive technology may

WHICH OF THE FOLLOWING DISRUPTIVE TECHNOLOGIES IS YOUR COMPANY CURRENTLY INVOLVED WITH OR PLANNING TO USE?*
(Percent of respondents)

Source: Marsh, RIMS; Excellence in Risk Management



* Multiple answers allowed

shift your risks—or how it is already changing them.

"You can't stick your head in the sand with what's happening with disruptive technology," the director of risk management for a major freight company told us. "At some point, you have to adapt."

Second, invest.

The inability to model the magnitude of disruptive technology risks was cited as a strong impediment to managing them and undoubtedly contributes to the lack of focus. Models, data, analytics—such tools can help prioritize, but they require investment from leadership.

Risk professionals have told us for many years that their organizations intend to invest in data and analytics, yet usage remains elusive: Analytics ranked near the bottom of techniques our survey respondents said they use to assess and model disruptive risks.

And it's more than just money that needs to be invested. A commitment of time and collaboration to discuss disruptive risk issues across the organization will help set priorities, lay out the implications for decision-makers, and develop mitigation strategies. One way to do that is through the effective use of cross-functional risk committees. And yet, we continue to see a decrease in the number of organizations reporting they have such committees. This year, only 48 percent of respondents said they have a cross-functional risk committee, a drop from 52 percent last year and 62 percent five years ago. Interestingly, 41 percent of respondents without a committee said their company should have one.

Finally, engage.

Organizations generally, and risk management professionals in particular, need to adopt a more proactive approach about disruptive technologies—what is already in use, what is on the horizon, and what are the risks and rewards.

Forward-thinking executives will look for alternative means to generate the necessary discussions to raise the risk profile of disruptive technologies. For example, in most organizations today, the term "cyber" is likely to attract attention. In our survey, "establishing effective cybersecurity" was the top concern related to disruptive technology among respondents across various industries. While data breach and privacy issues are real and should not be downplayed, the focus on cyber risk may at times obscure other concerns organizations should consider regarding disruptive technologies.

Several risk professionals we spoke with suggested using the current allure around cyber risk to pivot to broader discussions: "'Cyber' is a good catch-all word," a risk executive at an industrial contracting firm told us. "It provides a level of comfort that people can understand. If you get too detailed or technical during conversations about disruptive technologies, people may be less willing to engage. But if you keep it general, keep it high level, and talk about potential cyber threats and managing them—that's an easy way to tart the conversation."

Companies should also make use of an executive-level risk committee to discuss broader disruptive technology risks. Risk professionals can help lead the way as companies adapt to technology innovation, but they will be relegated to support roles if they fail to understand and address the unique issues the fourth industrial revolution brings. The good news is that the desire and ability to play a leading role are there.

DISRUPTIVE TECHNOLOGY BRINGS RISK AND OPPORTUNITY TO INFRASTRUCTURE PROJECTS

Adrian Pellen
Infrastructure Segment Leader, U.S. and Canada, Construction Practice at Marsh

The infrastructure industry has not typically been known for its embrace of new technology. In a recent paper, the World Economic Forum (WEF) attributed the industry's relatively slow adoption of technological innovation to a number of internal and external challenges in the engineering and construction sector: "The persistent fragmentation of the industry, inadequate collaboration with suppliers and contractors, the difficulties in recruiting a talented workforce, and insufficient knowledge transfer from project to project."

Change is inevitable and innovation is disrupting the way we design, build, operate and use infrastructure. Whether it's in civil infrastructure—roads, bridges, pipelines, and ports—industrial infrastructure, or social infrastructure, technological advancements are creating efficiencies in the way we operate. While technology adoption can help to promote sustainable growth, there are also risks to be managed.

INNOVATION TRANSFORMS INFRASTRUCTURE DESIGN

Innovation dictates that infrastructure needs to be conceptualized and designed differently. Consider something as basic to society as roads, and add to that the coming of autonomous vehicles—both for passengers and in trucking. Because autonomous vehicles rely to a large degree on sensing technology, we need to consider if roads, bridges, tunnels, and other infrastructure are being designed adequately for this new means of transportation. Beyond efficiency gained from proper design, what are the potential liability implications for inadequate design?

Big data and analytics have also infiltrated how we design infrastructure. For example, building information modeling (BIM) is realizing broader applicability as its technology develops.

Historically used for 3-D modeling in the design phase, continuing innovations in BIM will enable faster and better infrastructure development, as well as provide insights into how a project will perform throughout its life cycle, allowing a view into a project's future risk profile. This innovation in BIM promotes efficiency by allowing those who design infrastructure to provide real-time support to those building it.

BUILDING SITES BENEFIT FROM NEW TECHNOLOGIES

Construction sites are incubating grounds for a range of technology innovations in such areas as wearables and telematics.

Wearable technologies, for example, are rapidly changing the work landscape and promoting safety, accuracy and efficiency. Among the advancements in construction technologies is the smart hard hat, which allows technicians to project 3-D images in the natural environment, such as a bridge span, through augmented reality (AR)—the same technology behind Pokémon Go.

Enhanced safety vests borrow concepts from vehicle telematics. These vests are equipped with GPS and radio-communicating technology to enhance workforce safety and prevent injuries by warning users as they enter hazard zones. It's not hard to imagine a future in which workers wear an exoskeleton that will improve safety, enhance efficiency, and allow for the instantaneous exchange of data.

Technology will also enable infrastructure to be built by fewer humans—potentially enhancing safety and promoting resource efficiency. Balfour Beatty, a large international construction firm, suggests that by 2050 some infrastructure will be built without physical human labor. It is not difficult to anticipate that in our lifetime infrastructure will be designed and constructed using 3-D printing and installed by robots and mechanistic devices that operate with artificial intelligence.

OPERATION AND UTILIZATION OF INFRASTRUCTURE WILL CHANGE

Once these innovative infrastructure assets become operational, they will likely include embedded technologies, such as the intelligent transportation systems (ITS) used on many highways and freeways. These incorporate a variety of technologies including Bluetooth, video, and other wireless systems to promote efficient traffic management, allow for toll tracking and billing, enhance emergency response times, and assist law enforcement. With the coming of autonomous vehicles, it's likely that additional sensing technology will be needed to improve safety.

Beyond impacting how society uses and engages with roads and other infrastructure, interconnectivity will allow individual components to interact on an almost "live" basis. For example, it's anticipated that, in the near future, individual infrastructure components will contain monitoring technology that will provide real-time information about their operating efficiency and life span. When such components need replacement, the sensors will put in the order.

There is no question that innovation in robotics, automation, and other technology will continue to alter the way infrastructure evolves and the way we use it.

Change is inevitable and innovation is disrupting the way we design, build, operate and use infrastructure.

These technologies promote efficiency, connectivity and sustainable growth.

INFRASTRUCTURE RISKS ALSO SHIFT

With innovation comes risk, however, as technological disruption also increases volatility and exacerbates emerging issues, including those related to social stability as well financial viability and cybersecurity.

Social disruption.
If innovation does eventually displace large numbers of construction crews, drivers, or other workers, it's possible there could be considerable social unrest in some parts of the world. According to executives participating in a recent World Economic Forum event, it will be critical for industry to plan ahead by investing in education and training for workers whose jobs could be made redundant due to technological advancement.

Financial viability.
As technology advances, will the infrastructure we design and build today be useful in 20 to 30 years? How quickly will it become obsolete? What if we have flying cars? That may sound harebrained at face value, but compare the world we live in today to what people thought was possible just 20 or 30 years ago. Once we integrate technology into physical infrastructure, it can quickly become outdated.

This is particularly important in the context of privately financed infrastructure, where the private sector takes on the life-cycle management of infrastructure. Obsolescence is of particularly heightened risk to private concession companies who have assumed revenue risk (e.g. tolling) based on financial models that were unable to incorporate disruption in infrastructure utilization. The firms exposed to the financial risk related to infrastructure obsolescence could be builders, engineering firms, and/or equity firms and financiers developing and maintaining infrastructure.

Cybersecurity.
Because infrastructure now needs to be able to integrate with and connect to technology, such as smart buildings, autonomous vehicles, and transit systems, cybersecurity risks become more of a threat than in the past. The interconnectedness of our infrastructure through the Internet of Things (IoT) will face cybersecurity risks. Infrastructure may increasingly become a target for sophisticated organized crime looking to extract sensitive information. Firms with proprietary software, systems and infrastructure may become targets of corporate and political espionage.

Hackers have long probed for weaknesses in critical infrastructure. The ability for cyber events to affect infrastructure has grown, as seen in two recent global attacks involving malware—WannaCry and Petya. Infrastructure from hospitals to marine ports suffered financial losses and damage due to those events.

Perhaps the most frightening risk from an infrastructure perspective is that of cyberterrorists seeking to invoke fear. In the age of digitization and IoT, there are legitimate concerns that cyberterrorists could gain access to flood control gates, traffic lighting systems, public transit systems, or even the doomsday scenario of shutting the electric grid down completely. Cybersecurity continues to be one of the global risks of highest concern.

Today's new technologies almost always increase connectivity, including in the ways we build, operate, and maintain infrastructure. Companies involved in infrastructure can no longer afford to think of cyber risk as an afterthought, but need to adopt strong cyber-risk management practices from day one.

Thankfully there is a bustling market emerging in the risk management and insurance industry to address cybersecurity. In addition to consulting services developed to assess and manage cybersecurity exposures, insurers have developed products to transfer the risks that infrastructure stakeholders face as well as support risk mitigation by establishing incident response plans. These products, which are triggered by cybersecurity breaches whether motivated by financial crime or terrorism, can cover expenses related to extortion, property damage or financial loss related to a data and privacy breach or network outage.

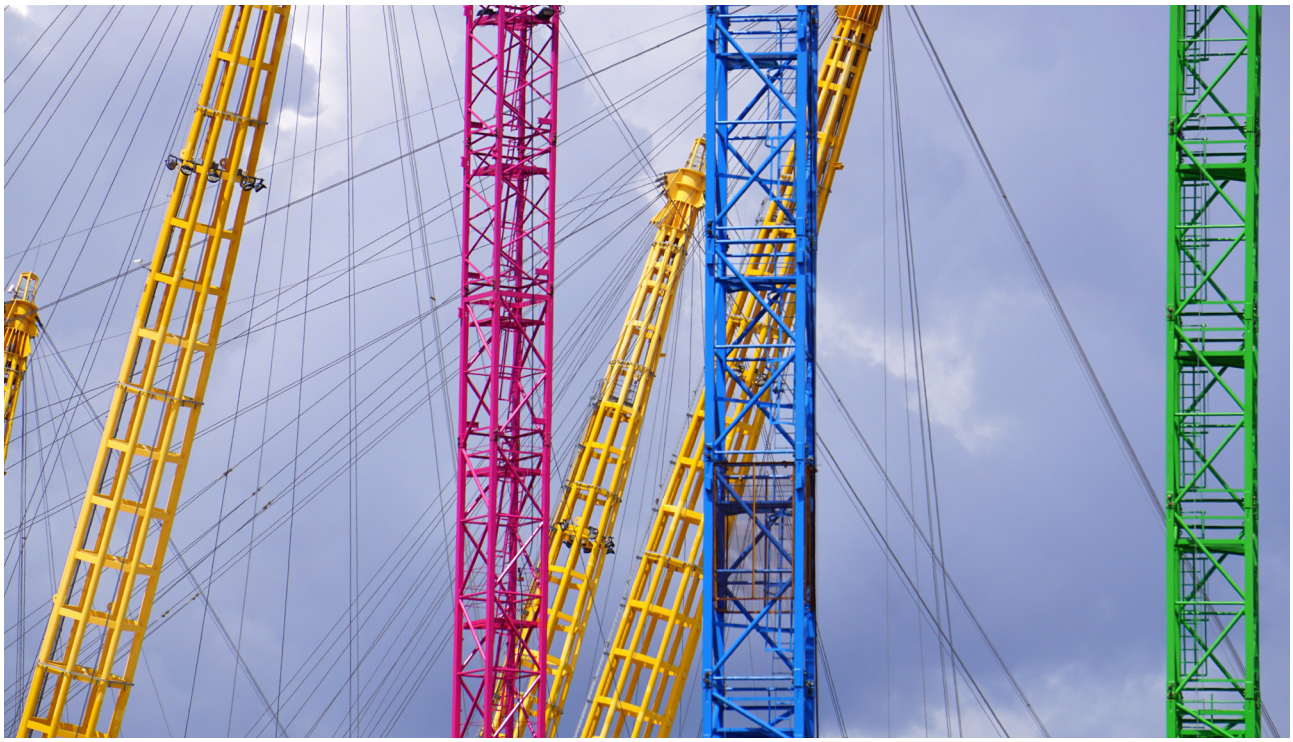
One recent estimate from the Global Infrastructure Hub, a G20 initiative, says there is a need for $94 trillion in infrastructure investments by the year 2040.

At the same time, it's clear that rapid technological advancement is changing the way we design, build, operate, and use infrastructure. Innovation in infrastructure will enable growth and promote economic, environmental and social vitality.

But advancement comes with risks—including social disruption, obsolescence and cybersecurity threats. These risks can be mitigated by forward-thinking city planning, investment, and integration of education into our workplace as well as an increase in cyber-oriented defenses.

WHY ASIAN INFRASTRUCTURE NEEDS MULTILATERAL DEVELOPMENT BANKS

Ryan Soon
Senior Research Analyst at Preqin
Tom Carr
Head of Real Assets Products at Preqin



What do a highway in rural Philippines, a power plant in Laos and a natural resources refinery in Indonesia have in common? They are all funded by multilateral development banks (MDBs).

MDBs such as Asian Development Bank (ADB), World Bank and the recently established Asian Infrastructure Investment Bank (AIIB) play an important role in Asia's infrastructure by filling a funding gap that was opened due to traditional lenders shunning investments in emerging economies as they are likely to face an uncertain political environment and a lack of transparency with regard to regulations.

According to Preqin's Infrastructure Online (IO) (subscription-based),the pace of infrastructure investments in Asia has accelerated in the past few years, from just over $28 billion in transaction value in 2012 to $139 billion in 2016 (Exhibit 1). The average transaction size has also surged; it is now $306 million, a 151 percent increase compared to $122 million in 2012.

Developing Asian nations, especially in Southeast Asia, are actively pursuing social and economic infrastructure expansion. Vietnam is seeking investors for public-private partnership (PPP) transportation projects, while Myanmar recently unveiled an urban improvement plan for public utilities and roads. Based on *Meeting Asia's Infrastructure Needs*, a report published by ADB, developing countries in Asia require an estimated $26 trillion in infrastructure investment from 2016 to 2030—or $1.7 trillion per year—to meet infrastructure demands.

PLUGGING ASIA'S INFRASTRUCTURE GAP

MDBs have the financial firepower to help emerging Asian nations

modernize roads, rail networks and ports, as well as improve access to electricity and clean water.

ADB was involved in one of the largest MDB-sponsored deals—a $465 million loan facility to construct the Nam Ngum 3 Hydro Power Plant in Laos. Not only will the 440 MW hydro-generated power plant reduce energy shortage in Laos, it will also export excess power to Thailand. In 2016, the Manila-based institution's lending and grants provided to the region hit an all-time high of more than $30 billion. ADB has also recently pledged to increase its financial support to Asia over the next few years.

MDBs will work together with other institutions to maximize their financial assistance for infrastructure development. Data from Preqin's IO shows that Indonesia is the greatest beneficiary of MDB infrastructure financing in Asia with participation from various institutions making up one-fifth of such loans in the region (Exhibit 2). For example, in June 2016, AIIB and the World Bank each contributed $216 million to the National Slum Upgrading Project in Indonesia, which aims to improve urban infrastructure and services in several shanty towns. In terms of project stage, greenfield assets constitute 79 percent of MDBs' financing projects, followed by brownfield (17 percent) and secondary (4 percent).

AIIB ENTERS THE FRAY

2016 witnessed a record high in terms of lending by MDBs in Asia; 18 MDB-backed infrastructure deals were completed worth an aggregate $3.8 billion, a portion of which was contributed by AIIB, the new kid on the block. Officially established in 2016, AIIB has a smaller capital base than either the World Bank or ADB, but has already approved loan facilities for several major development projects. More recently, AIIB revealed that it was in discussion with World Bank to co-finance more infrastructure projects in 2017 and 2018, underscoring the institution's commitment to the region. With a quick start, AIIB has already become an important player in the MDB financing landscape, and its importance will only increase going forward.

MORE THAN JUST CAPITAL

Besides the provision of capital, MDBs also promote private sector participation by acting as anchor investors in unlisted infrastructure funds. ADB previously committed to Berkeley Energy's Renewable Energy Asia Fund, which targets a range of renewable projects in developing markets, including India, the Philippines and Vietnam, while World Bank invested in IDFC Alternatives' India Infrastructure Fund. The vehicle seeks opportunities in India's energy, transportation, telecommunications and social sectors. With the dry powder—or uninvested capital—of Asia-focused unlisted infrastructure funds at an all-time high of $25 billion as of September 2016, MDBs are in a position to play a significant role in narrowing the disparity between the supply and demand of assets.

PPPs are an important method in securing private financing; 90 percent of infrastructure investors with a preference for Asia participate in such partnerships. However, emerging Asian economies generally have limited experience and expertise in structuring a PPP framework. MDBs can add value by working with governments on regulatory reforms, establishing PPPs and managing risks. By providing guidance on standards and best practices, MDBs build a solid foundation that can attract additional financing into a country. They can also provide governments with hands-on support during the preparation, construction, and ultimate implementation of infrastructure projects.

MDBs also seek to develop quality0infrastructure assets. Japan has recently agreed to provide $40 million over a two-year period to ADB, which aims to bring high-level technologies to the design and implementation of projects, as well as promote quality infrastructure in Asia. This benefits both parties; private investors can earn long-term returns and achieve diversification in their portfolios, while developing nations in Asia can get much needed infrastructure investment and technical know-how.

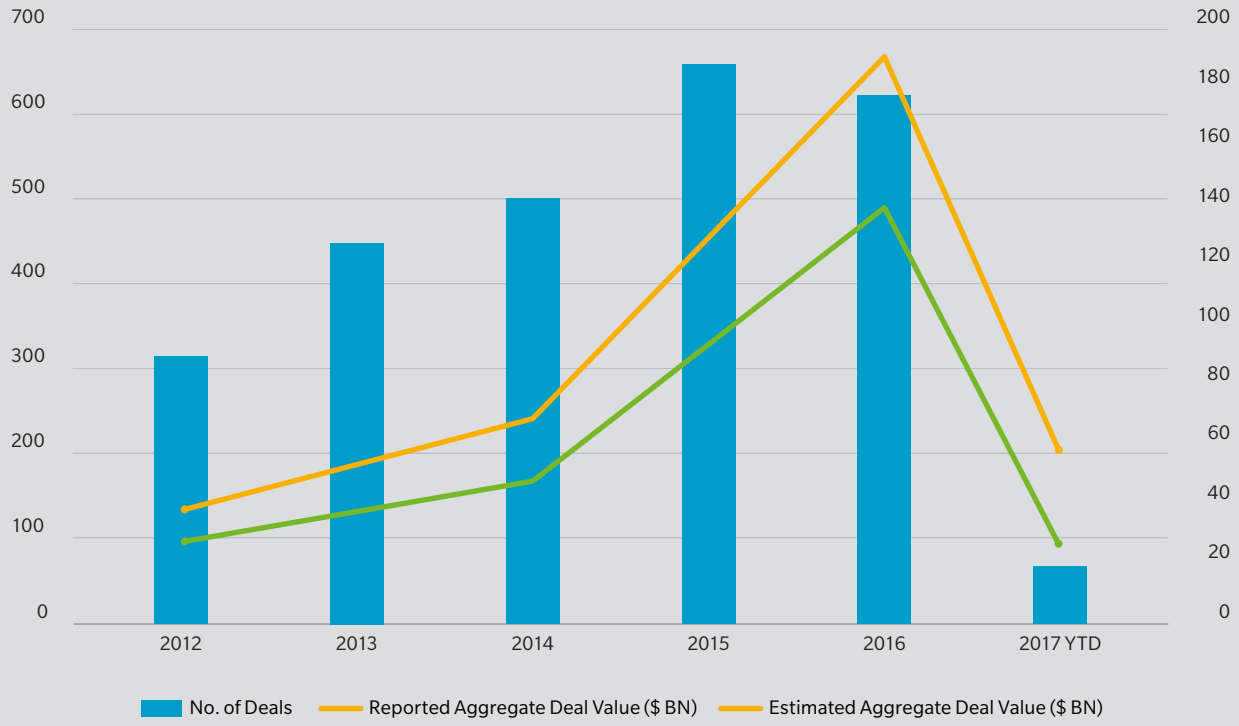
COOPERATION IS KEY

Cooperation between MDBs, the private sector and governments is key to infrastructure development in Asia, because it can encourage economic growth, improve local livelihoods, and enhance regional connectivity.

Infrastructure investments in developing countries may hold less appeal to some investors as they typically involve greater risks, but the presence of MDBs has helped instill investor confidence in emerging Asian economies and their infrastructure development. MDBs are increasingly partnering with other institutions, including export banks and sovereign wealth funds, via co-financing arrangements, syndication or project bonds. Asia faces several challenges in its pursuit of infrastructure progress, but MDBs are doing their bit in helping address the region's infrastructure funding gap with capital and by providing their technical expertise.

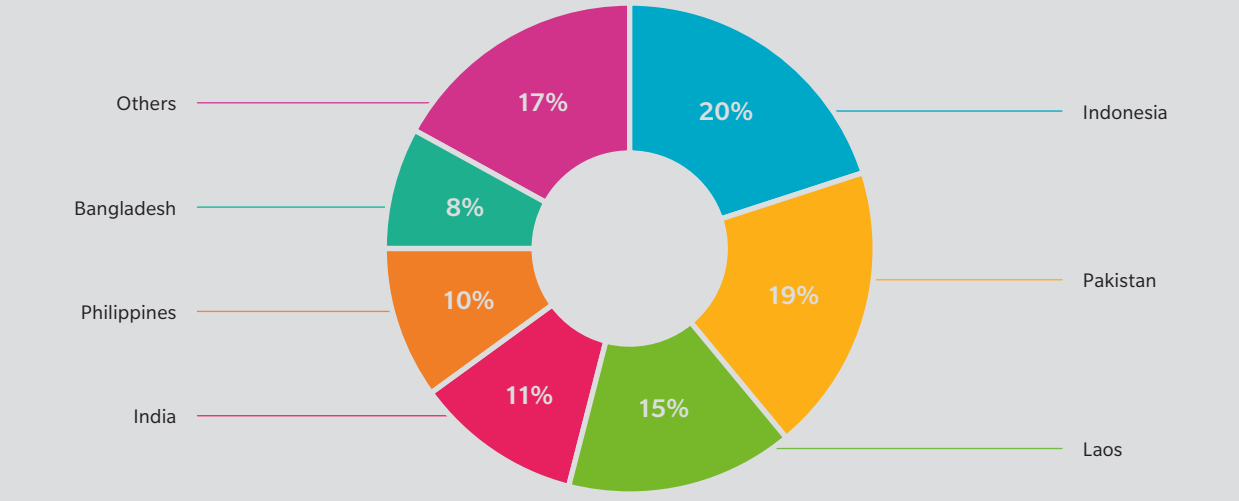
NUMBER AND AGGREGATE VALUE OF INFRASTRUCTURE DEALS COMPLETED IN ASIA, 2012–2017 YTD (AS AT MAY 2017)

Source: Preqin *Infrastructure Online*



PROPORTION OF INFRASTRUCTURE DEBT FINANCING TO ASIA WITH PARTICIPATION FROM MDB'S BY LOCATION, ALL-TIME

Source: Preqin *Infrastructure Online*



TECHNOLOGY

HOW BANKS CAN KEEP UP WITH DIGITAL DISRUPTORS

Scott A. Snyder
Senior Vice President, Managing Director and Chief Technology and Innovation Officer for Safeguard Scientifics

Hardly a day goes by without seeing a new business article or blog post on digital disruption. Blockbuster is dead, taxis are struggling and hotels are losing customers, who are increasingly renting rooms in homes of ordinary people. We get it: Incumbents get disrupted by new entrants armed with digital technologies, talented and highly incentivized teams and fresh venture capital. There are very few industries in which CEOs do not live in fear of digital disruption.

Banking is no exception: Executives believe digital disruption will drive 40 percent of companies out of the top 10 in the next five years. As Antony Jenkins, former CEO of Barclays, aptly put it in a 2015 speech: "Over the next 10 years, we will see a number of very significant disruptions in financial services, let's call them Uber moments."

Ten years may be wishful thinking, as significant disruption is already happening. Massive investments in fintech are spawning a wave of new companies reinventing everything from payments and money management to lending and financial planning. The chart below shows examples of companies disrupting financial services. Some analysts believe Fintech disruption could take as much as 10 percent to 40 percent of bank revenue and eliminate 1.7 million banking jobs by 2025.

Despite their historic advantages, banks need to start transforming themselves to deliver highly personalized physical and digital experiences.

Couple this with increasing regulation, historically low interest rates and the fact that most (73 percent) millennials would prefer to get their banking services from a non-financial services company, and banks seem to be headed the way of Blockbuster.

Before we declare the game over, let's think about some of the unique advantages banks possess.

Frequency.

Next to social media platforms, banks are the second-most frequently touched platforms in our lives. People engage with their banks 17 times per month on average, versus 14 times per month for retailers. Most brands spend billions to increase customer engagement. Banks already have it, yet bank loyalty is not much better than cable companies.

Reach and trust.

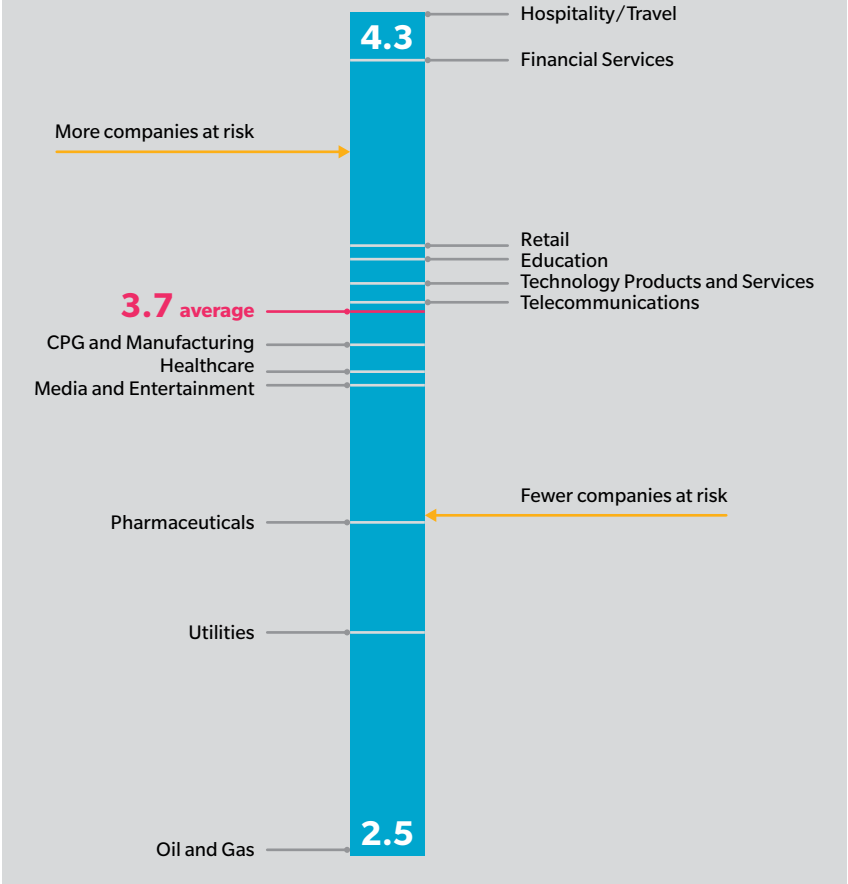
The blend of physical and virtual touch points can extend to more of people's everyday needs; people want to know banks are nearby and part of the community. Defunct online banks such as Wingspan and ING Direct, now Capital One 360, didn't scale without the brick-and-mortar element, much like Amazon, the e-commerce giant, now sees the need for physical presence with the roll-out of lockers, pick-up points and even Amazon Go stores.

Knowledge.

Banks have an enormous amount of data on customers and their needs, spanning from where you work to what you buy, how much you save and even where you like to vacation. Banks should know if you have a side job as an Uber driver to save for a new house and therefore be ready with a business banking account, a car loan to upgrade and even home-financing options. Yet most of this data lives in silos across disparate data sources, preventing these types of integrated offers.

IN YOUR INDUSTRY, HOW MANY COMPANIES WILL LOSE THEIR PLACE IN THE TOP 10 DUE TO DIGITAL DISRUPTION (OVER NEXT FIVE YEARS)?

Source: Global Center for Digital Business Transformation, 2015



Despite these historic advantages, banks need to start transforming themselves from inflexible, analog monoliths to delivering highly personalized physical and digital experiences in order to be relevant to the next generation of banking consumers. The key opportunities to do this are the following:

Make banking seamless.

When Disney launched its MagicBand wristband at its theme parks, the company integrated a wearable that combined frictionless transaction and personalization features that improved the customer experience and increased consumption by around 8 percent per guest without requiring additional effort on their part. Banks need to do a similar job of integrating banking into everyday life experiences to stay relevant. Examples include BBVA's Wizzo app, which makes getting and sharing money easy; TransferWise, which takes the pain out of moving money across borders or Quicken Loans' Rocket Mortgage, which enables mortgage approvals when you need it.

EXAMPLES OF COMPANIES DISRUPTING FINANCIAL SERVICES

Source: Author's research

Category	Companies
Payments	PayPal, Dwolla, Square, M-Pesa, Billtrust, Kantox, Traxpay, Venmo
Alternative Currencies	Bitcoin, Bitstamp, Xapo, BitPay, Etherium, ZCash
Product and Service Advice	Bankrate, MoneySuperMarket, LendingTree, Credit Karma
Personal Finance Management	Fintonic, Moven, MINT, Digit
Wealth Management and Advice	Batterment, Wealthfront, SigFig, Personal Capital, Nutmeg
Crowdfunding (Capitol and Debt)	Lending Club, Kickstarter, Crowdfunder, AngelList, SeedInvest
Peer and Pre-approved Lending	LendingClub, Prosper, Kreditech, Lenddo

Hyper-personalize.

While 69 percent of customers have tried mobile banking, only 25 percent use it regularly. Much like the challenge other mobile apps face in maintaining ongoing engagement, banking apps tend to lose relevance by using a one-size-fits-all approach, failing to leverage recent activity patterns and context, and not taking advantage of different modes of engagement based on what users prefer. In order to deliver "hyper-personalized" experiences that increase engagement, banks must combine predictive analytics with multiple modes of interaction. By using data to adapt to customer behaviors, banks can determine which customers will respond well to self-service robo-advisors versus human ones, or which customers can elevate their financial literacy and savings discipline through apps such as Simple or Digit. With emerging touchpoints such as voice agents and wearables, the opportunity to capture data and personalize will only improve.

Turn branches into experience centers.

Nearly 6,000 bank branches have been closed in the U.S. since 2009, according to the FDIC, and with greater digitization, the trend seems to shift away from physical touchpoints. As we see in retail, the leaders are figuring out how to rationalize their physical space with smaller footprints and automation while also equipping employees to become ambassadors in the customer experience, since brick-and-mortar conversion rates (25 percent) are still significantly higher than online (2.3 percent).

Retail brands such as Sephora and Nike have enabled customers to easily move from online to the local store experience by allowing them to browse store inventory, make appointments and even interact with associates. Bank of America has started to connect its online and local branch experience more tightly via its mobile app, and Capital One now has 16 banking cafes aimed at creating a more relaxed banking environment. The industry as a whole is still behind when it comes to offering a truly connected and personal branch experience. To make the experience more like Starbucks and less like McDonald's, banks will need to ramp up investments in automation (digital integration, automated tellers) as well as attracting and training talent to match the new digital-savvy customer base.

Adopt a customer-centric innovation model.

In this new era of empowered digital end users, either you find a way to make the customer part of your innovation model or they will innovate around you. The best part is organizations that do this well—such as Waze, Pandora and Betabrand—are incredibly capital efficient because they leverage OPM, or "Other People's Money," via smart devices, broadband connections and social media platforms that someone else already paid for.

J&J has created a patient experience center for iterating on new healthcare innovations firsthand with patients and providers before deploying into the field. In the case of the African micro-finance service M-Pesa (created by Vodafone), it was the local wireless carrier, Safaricom, that saw the opportunity to innovate around the large population of unbanked mobile consumers, and the two teamed up to do it. Now M-Pesa has become the largest payment platform in sub-Saharan Africa. In banking, TD Bank partnering with Moven to engage millennials with basic

banking services is a good example of customer-centric innovation, but banks still have a long way to go to fend off consumer-centric players such as Apple, Google and Amazon from disrupting their markets.

Create a two-speed business model. When GE CEO Jeff Immelt declared that the data coming from equipment is now worth more than the equipment itself, it forced GE to rethink how it captures and delivers value to its future customers. As part of GE's transformation, every business unit now has a chief digital officer, and GE Digital is becoming one of the largest industrial software companies in the world, projected to generate $15 billion by 2020.

In a similar vein, BBVA chairman Francisco Gonzalez has said that the innovation process for banks "might be compared to changing the tires of a truck while still in motion." BBVA started its journey towards a two-speed business capable of big innovations ("Big I") more than seven years ago, shifting from an 80/20 current operations/future innovation focus to 60/40. This came with dramatic changes to the organization structure, a dedicated digital organization and a number of external innovations and ventures that allowed transformation of the company while still executing on the current business.

Other banks are starting to follow suit, such as Citi with its Innovation Labs, Umpqua with its Pivotus Ventures subsidiary or Rabobank incubating its MyOrder venture separate from the core business. In order to support continuous innovation in the core business, or "Little I," in parallel with creating and accelerating "Big I" innovations that will likely disrupt the core business, banks need to have talent aligned to both missions. They also need an agile infrastructure that supports rapid experimentation along with the reliability, security and scale required by the core business. IT is no longer just the cost of doing business, but a key enabler to innovation.

In October, banking regulator Office of the Comptroller of the Currency (OCC) established an Office of Innovation, implemented a framework for responsible innovation, and is even exploring special bank charters for fintech companies. With the potential for a more relaxed U.S. regulatory environment under the new presidency, we could see these innovation avenues open up even further. This is similar to what the FDA has been doing around digital health and mobile medical apps: establishing guidelines and examples to facilitate innovation versus being a barrier to it.

While there are signs of progress on the regulatory front, most banks continue to lag on digital innovation. Despite being one of the top sectors for technology investment over the last two decades—including the creation of major products such as ATMs, debit cards, credit scoring and check scan and deposit—banks are lagging behind other industries, such as those in retail, transportation and even healthcare, when it comes to digital transformation.

The good news is that banks are still very well-positioned to win with the new wave of empowered digital customers, given their rich historic data and balance of physical and digital touchpoints; however, it will take a strong commitment to a customer-centric vision, a two-speed business model and agile infrastructure to enable "Big I" innovation and a data-driven approach to delivering personalized, relevant banking experiences.

For bank executives, it's time to decide if you want to be Netflix or Blockbuster. Your customers won't wait forever.

This piece first appeared on Knowledge@Wharton, which is the online research and business analysis journal of the Wharton School of the University of Pennsylvania.

REIMAGINING THE PHARMACEUTICAL SALES REPRESENTATIVE MODEL IN ASIA

Joseph Mocanu
Principal and Practice Lead, Life Sciences and Digital Health, Asia-Pacific at Oliver Wyman

In this age of information, unprecedented levels of scientific understanding, increasing use of formularies, and the growing call for evidence-based medicine, why do we still see pharmaceutical sales driven primarily by sales representatives (sales reps) who rely more on messaging and relationships than on hard clinical evidence?

Indeed, the role of the sales rep has been facing significant pressures from regulators, physicians and policymakers (see table), but they are still ever-present. There are an estimated 450,000 sales reps still directly employed by the industry, and their related activities account for 62.5 percent of all sales and marketing expenses.

The diminishing returns of sales reps have been highlighted even earlier. More recently, two key catalysts prompted change. First, the looming pricing uncertainty, and second, the emergence of viable alternative models.

PRICING UNCERTAINTY

For most countries in Asia, a combination of increasing health technology assessment use, reference pricing, and strong negotiating power have kept prices substantially lower than in the U.S. Even Japan, traditionally viewed as a pricing haven (sometimes even awarding companies with superior pricing to the U.S.), has made an unprecedented move of directly intervening in the price of several drugs, most notably demanding a 50 percent price cut in Opdivo, a leading immuno-oncology drug.

Today, with roughly 70 percent of pharmaceutical revenue coming from the U.S., EU and Japan, how would price cuts of even 5 percent or 10 percent impact the industry? Can they hope to make up those losses elsewhere in the world, or will they have to look inward? In the near term, the latter seems more probable. The Chinese government recently announced price cuts for 36 branded drugs, averaging discounts of 44 percent compared to the previous year and with some reaching as high

as 70 percent. Other governments in the region are undoubtedly taking notice.

DIGITIZATION AND THE EMERGENCE OF VIABLE ALTERNATIVES

Dr. Stanley Li of DXY gave a particularly compelling internal example (DXY is a leading Chinese digital health platform that has 70 percent of all doctors in China as users) during his keynote speech at the Galen Growth Asia Health Tech CEO Summit last December.

He described a small "experiment" of "only" 27,000 doctors who sought to compare the effectiveness of message delivery between the DXY platform and traditional pharmaceutical sales reps. The hypothesis was that by understanding what physicians read and shared, and how they interacted with their patients and communities online, a virtual profile of the physician could be constructed in much greater detail than what a typical sales rep could do in their daily interactions. Moreover, how physicians portray themselves to a rep may differ from what the physician is really interested in and how the physician actually practices medicine. The experiment was a success with the effectiveness of message delivery improving by 3.6 times.

The striking part of this pilot was not that it was more effective in message delivery, but rather how well DXY knew its doctors. If a company knows its doctors better, it is obvious that it will have better results. This also shattered the myth that you need a face-to-face relationship to be successful.

The good news is that DXY is not alone in this regard in Asia. Some health insurers, third party administrators and even startups thrive by better knowing their doctors, and a good number of them are looking for ways to better collaborate with pharmaceutical companies.

But why do sales reps need all this if they already know their doctors very well from their numerous visits? Can sales reps do more?

Some reps surely do and can, but they are simply not properly incentivized to. In the increasingly short and scarce visits, they must focus what little time they have on products rather than the needs of their physicians (let alone patients and other stakeholders) in order to satisfy their own performance targets as well as their company's targets.

Some pharmaceutical companies have publicly changed their sales rep compensation model as a first step to changing the way they behave and interact with physicians; yet fundamentally they are still focused on a face-to-face "push" interaction. In the minds of most pharmaceutical companies, alternative channels mean providing the rep an iPad, or leaving behind more elaborate reading materials, rather than fully exploring the various channels in which the physicians wished to interact and truly understanding what the physicians need from pharmaceutical companies to better practice medicine and save patient lives.

Sales reps and their organizations need to adapt to the increasing complexity of care, with physicians sharing decision-making roles with payers, third party agreements (TPAs), hospital administrators, and even patients as they become more empowered. Focusing solely on the physician is not going to be enough in most Asian markets going forward.

THE WAY FORWARD

Thousands of sales reps can't be eliminated overnight, but their roles can gradually be transformed through upskilling and remodeling incentives. This transformation needs to be accompanied by partnerships with those who understand doctors in a more neutral and systematic way, as well as by maximizing technology that can replace the traditional sales rep function at scale. Some companies are trying to do just this, albeit in the medical device space, replacing the in-person support provided by traditional sales reps with virtual tech consults that are less intrusive and far more cost effective.

Thousands of boots on the ground still have direct visibility to what is happening in the real world. A first step may be evolving their roles into one that is more oriented to customer and institutional support, community engagement, or even involved in the collection of real-world evidence and competitive intelligence (potentially even threatening the monopoly of certain health informatics companies). As they do this, there will be numerous opportunities for digital health companies to support them in this journey.

Ultimately, it's the patients who will benefit most.

ROLE OF SALES REPRESENTATIVE UNDER PRESSUE

Source: Oliver Wyman

Country	Year	Example
Australia	2014	"No Advertising Please" campaign by Australian general practitioners, calling on physicians to make a pledge and display signs refusing sales representative visits
China	2017	State Council of China calls for the restriction of sales representative activities to only communicate academic information and to provide technical support, neither of which can be tied to sales (effectively acting as medical science liaisons)
Russia	2011	Proposal by Prime Minister Vladimir Putin to ban all sales representatives (did not pass)
Turkey	2015	National registration and ID system to track sales representative visits and reduce illegal promotional activities
U.S.	1998	The Everett Clinic group banned all sales representatives from visiting their physicians
U.S.	2014	The Sunshine Act, preventing any gift greather than $10 as well as requiring doctors to publicly declare the compensation they receive from pharmaceutical companies
U.S.	2016	ZS Associates reports that only 44% of physicians are readily accessible to sales representatives, 18% of physicians have severely limited access

RISING MIGRATION DEMANDS "ROAMING" HEALTH COVERAGE

Eduardo P. Banzon
Principal Health Specialist, Sustainable Development and Climate Change Department at the Asian Development Bank

As movement across countries becomes easier and more frequent, the one situation most people dread is getting sick and needing to access health services in a foreign country. Even as they worry about getting well, they end up worrying more about how to pay for it.

For low-income migrant workers from developing countries of Asia and the Pacific, getting sick may not only put them at risk of losing their jobs and income, with huge bills to pay. It may very well drive them into poverty.

Many Asian countries have made impressive strides toward providing health coverage for their citizens—particularly the poor—by setting up national health insurance systems (NHIs) that compel the formal sector to contribute to premiums. NHIs also facilitate the enrollment of the non-poor informal sector, and fully subsidize the insurance coverage of the poor and other vulnerable populations.

Pooling these various revenue sources, NHIs then leverage their purchasing power to buy health care services from public and private providers for their respective covered populations.

Indonesia's national health insurer now covers 169 million people; and the Philippine government reports that 92 percent of all Filipinos are insured. India will soon expand health insurance coverage to over 800 million people, while the covered population in China is over a billion.

But as countries expand health care services for the covered population, they also need to guarantee the same health coverage for citizens when they are in foreign countries, as well as for foreign residents.

CROSS-BORDER HEALTH COVERAGE FOR MIGRANT WORKERS

Countries need to make their health coverage "roam." If increasing mobility, innovative thinking, and collaboration across countries has rapidly made phone roaming a reality, health coverage should be able to roam as well.

Asians, up to 31 million in 2015 alone, are increasingly moving around the region—mostly to find jobs. That number will rise as the Association of Southeast Asian Nations (ASEAN) Economic Community makes it easier for workers to cross borders. The increasing movement

across borders into growing and interconnected economies will surely make roaming universal health coverage (UHC) a reality soon.

This is crucial for informal communities like migrant workers, who are vulnerable to a range of infectious and noncommunicable diseases, mental health disorders, maternal mortality, substance use, alcoholism, malnutrition, and violence. They face barriers to decent health care—especially if their legal status is uncertain.

Imagine how much easier their lives would be if their home country NHI could cover the treatment they need overseas and also foot the bill. Within ASEAN, for instance, a national health insurance card of one member country would be enough to ensure coverage in the others. People of the Asia-Pacific region would finally have health care that is at least regional, if not universal.

Sadly, roaming health coverage has not matured in Asia.

The Philippines requires its outgoing migrant workers to get health insurance coverage, but this means paying upfront and getting reimbursed later. Indonesia, Nepal and other countries are implementing similar schemes and experiencing the same weaknesses and problems.

MORE BUY-IN FOR UHC

The limited coverage is not surprising given that several countries still struggle to ensure financial protection with their NHI and other health coverage schemes. The share of household out-of-pocket payments for health care services is persistently high, at more than 50 percent of total health spending in Cambodia, the Lao People's Democratic Republic, India, Pakistan and the Philippines.

But here, too, there is positive news. NHIs are pooling all types of pre-payments, including taxes and insurance premiums, into single funds that not only cross-subsidize from the rich and young to the poor and old, but also reduce implementation inefficiencies. This has happened in the Republic of Korea, where the introduction of a single-pool NHI decreased administrative costs from 6.5 percent to 4.5 percent of total expenses. Government health purchasers are being strengthened by social and political buy-in for UHC.

In the Philippines, lawmakers earmarked in 2012 the most incremental sin tax revenue increases to subsidize the poor and other vulnerable people. And there is increasing centralization of health information and sharing of health data across public and private health systems. This is making many NHIs more strategic and efficient.

These developments provide a solid platform for roaming health coverage. It would also help to have more clarity in benefits packages, payment methods, and health guarantees. Interconnected and interoperable health information systems across countries would facilitate bilateral and multilateral mutual recognition and agreements that could formalize roaming.

Within ASEAN, negotiations for multilateral recognition of Southeast Asian countries may not be needed at all. ASEAN can act as a launching pad for roaming coverage as the EU does, which allows roaming health coverage for any EU citizen in any EU country.

In a world where borders are blurring and becoming increasingly permeable, health coverage needs to be just as mobile. If ot, it will never be truly universal.

This piece first appeared on the Asian Development Blog.

In a world where borders are becoming increasingly permeable, health coverage needs to be just as mobile.

FINTECH IN CHINA: WHAT'S BEHIND THE BOOM?

Cliff Sheng
Partner and Head of Financial Services, Greater China at Oliver Wyman
Jasper Yip
Engagement Manager of Financial Services, Greater China at Oliver Wyman

China has struggled to shake off the perception that it's lagging behind developed economies in technology and innovation. And while much of that perception is warranted, there is one industry where China can be considered a leader: fintech.

The country makes some of the world's largest investments in the sector, and it has adopted fintech technologies faster than anywhere else. Companies such as Alipay, Lufax and ZhongAn Insurance have made their names across the globe by using fintech to develop some of the most disruptive business models. These players have enjoyed the fruits of fintech's unprecedented growth by filling the gaps in China's structurally imbalanced financial system in an open regulatory environment.

We believe the development of fintech in China has reached an inflection point. From this point, technology will be the key driver of value-chain disruption in an increasingly data-driven industry.

UNPARALLELED GROWTH WITH UNIQUE CHARACTERISTICS

Over the past half decade, we have witnessed phenomenal growth in the Chinese fintech industry. 2013 is widely recognized as the onset of the boom. Since then, major segments of the fintech market have, on average, doubled or even tripled every year. For example, the outstanding loan balance for online peer-to-peer lending platforms surged from 31 billion yuan ($4.64 billion) in January 2014 to 856 billion yuan three years later (Exhibit 1).

The explosive growth in China's fintech sector is further characterized by its relatively short maturity curve. For example, it took four years for peer-to-peer transaction volume to exceed $5 billion in the U.S., while it took only two years in China. Lufax, a Chinese peer-to-peer lending platform founded in 2011, reached an annual loan origination amount of 9 billion yuan in just two years,

compared to five years for Lending Club, the biggest peer-to-peer lending company in the U.S.

Venture capital investments in China's fintech sector are soaring, and these investments have given rise to several unicorns.

"FIN" AS THE HISTORICAL VALUE DRIVER— RIDING THE WAVE OF TRANSFORMATION

When compared to the U.S., China's financial system has historically exhibited three main structural imbalances or inadequacies, namely underserved retail and small- and medium-enterprise (SME) segments in the bank-dominated indirect financing model, a deposit-driven investment model and trailing infrastructure development.

For example, direct financing amounted to only 69 percent of GDP in China from 2011 to 2015, compared to 166 percent in the U.S., according to our analysis. The bank-driven indirect financing model in China has historically been structured around large and government-related corporates. Most SMEs and retail customers have been largely unserved, amid limited and imperfect credit infrastructure.

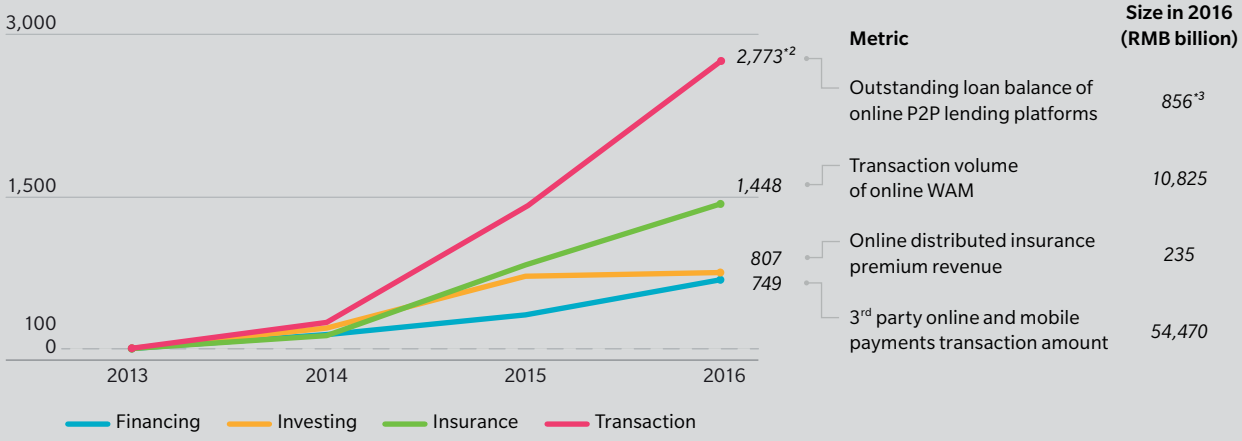
Noticing the structural imbalances, the Chinese government is gradually pushing for financial reforms. Coupled with the timing of the Internet boom, this has created an opportunity for fintech players to bridge the gaps in traditional financial services by capitalizing on their strong online presence and loose regulation.

Despite the impressive growth, not all players that emerged in this wave of transformation are truly "fintech" in nature. Some of the players grew rapidly by exploiting their less-regulated status to offer products that were stringently regulated in the traditional financial services system. The unregulated growth has led to several high-profile scandals. For example, over 60 percent of the 5,890 online peer-to-peer platforms that ever existed are estimated to have ceased operations based on data from Wangdaizhijia.com. Ezubao, a peer-to-peer lending platform that raised more than 1.5 billion yuan in a year and a half, was proved to be a Ponzi scheme, making it the biggest-ever financial fraud case in China. The recent Zhao Cai Bao default illustrated how online wealth management products were offered to investors who did not have access to transparent information.

Such incidents created growing concerns over the legitimacy of fintech and prompted policymakers to incorporate fintech into the regulatory framework. The tightened regulatory environment will undoubtedly challenge some of the fintech players that have grown uncontrollably amid regulatory loopholes.

INDEXED GROWTH OF CHINA FINTECH SEGMENTS*1

Source: WIND, Analysys, CIRC, Insurance Association of China



*1. Methodology: One representative metric for each area adopted and indexed at 100 in 2013. Metric selection: Financing – outstanding loan balance of online P2P lending platforms; Investing – transaction volume of online wealth management platforms; insurance – online distributed insurance premium revenue; payment – total 3rd party online and mobile payments transaction amount.

*2. Used outstanding loan balance at the end of the first month of the year after in lieu of the year-end figure as no official pre-2014 data was available, i.e. the outstanding loan balance of January 2014 is indexed at 100.

*3. Figure at the end of January 2017 (see note 2 for details).

TECH AS THE FUTURE VALUE DRIVER—NEW, DISRUPTIVE BUSINESS MODELS

As the window of regulatory arbitrage closes, future fintech leaders will differentiate themselves by pushing the frontiers of technological innovation and disrupting traditional financial services business models (Exhibit 2).

We believe big-data analytics, the Internet of things (IoT), and blockchain technologies and applications will form the bedrock for future fintech leaders, owing to their ground-breaking capabilities to acquire, assemble, analyze, and apply information. Data treatment and information processing are at the heart of decision-making for financial services, especially in China where data are often incomplete, not transparent, and sometimes questionable.

For example, technology leaders in China have already achieved a major leap in big data analytics computation capacity and made significant progress in machine-learning capabilities. Leading fintech players are also increasingly adopting such techniques to facilitate their understanding of the market and customers by building know-your-product (KYP) and know-your-customer (KYC) capabilities. They also use such techniques to support the development of innovative products and dynamic pricing. In addition, big-data analytics also enable the automation of decision-making processes and reduce labor costs.

The application of these technologies will create significant disruption along value chains and bring about distinctive values for each of the four major areas of financial services:

1. Financing.
With the availability of nonfinancial data and improved knowledge of how to use it, Chinese fintech companies could considerably improve their credit-risk management capabilities and enhance the customer experience. They could expand the "lendable population" from around 200 million credit-card-carrying prime borrowers to around 800 million, creating value for—and from—otherwise neglected subprime segments.

2. Investing.
With stronger computing capabilities, online wealth management platforms can conduct detailed analysis by pulling together various types of data about the market, individual securities, and investors. They can then offer low-cost, bespoke investment solutions that are free of subjective and behavioral biases. Assuming these solutions attracted 2.5 percent of invested assets by China's historically self-directed investors by 2020, these would represent assets under management worth a whopping 5 trillion yuan.

3. Insurance.
The emergence of connected ecosystems, along with the increased adoption of technology gadgets, provides not only gateways to innovative insurance products but also alternative data sources for tailored products and pricing. In our *recent publication, Insuretech in China*, we estimated that such technology upgrades and ecosystem embedding would present insurers with premium revenues amounting to 400 billion yuan by 2020.

4. Transaction.
Although still nascent, blockchain and its applications could potentially be used to provide low-cost, reliable transaction solutions across different areas of financial services. They could potentially promote mutual growth with budding fintech business models that are only economically possible with support from such solutions.

We have not yet seen the full potential of fintech in China; but we believe that technological advances, coupled with the unique circumstances of China's financial system, will propel fintech companies to further drive innovation and disrupt the traditional financial services space.

A second part to this piece will be published next week—it will delve into the implications of China's growing fintech market on various stakeholders.

RECENT REGULATORY DEVELOPMENTS FOLLOWING GROWING CONCERNS AND INCIDENTS			
	KEY CONCERNS	EXAMPLES / INCIDENTS	RECENT REGULATORY MOVEMENTS
Financing	• Borrower appropriateness/ borrowing terms • Inappropriate collection approach • Enlarging but untraceable leverage; multiple sources borrowing	• Nude selfies for loan • Student suicides amid loan shark collection	• More stringent requirements on lending to university student*1 • Capping borrowing balance by individuals (RMB 200 thousand) and organisations (RMB 1 million)*3
Investing	• Visibility/transparency/ traceability of investment flows (e.g. Ponzi scheme) • Investor-asset risk mismatch/ mis-selling • Liquidity mismatch	• Ezubao's Ponzi scheme • Corporate default related to Zhaocaibao • Accusation on JD.com "Baina" model	• Prohibit P2P players from exaggeration in prospectus and concealing of flaws and risks (e.g. any guaranteed principal & return of interests); disallow P2P players from asset securitisation*3 • Investigation against Internet Co with AM license conducting inappropriate activities; against Cos without AM license but conducting such activities; against Cos with multiple licences on potential tunneling*4 • Prohibit crowdfunding platform from engaging in public equity raising activities (more than 200 shareholders) and selling private funds*5
Transaction	• Fraudulent transactions/ anti-money laundering • Overexpansion of third party payment to deposit taking	• Yu'E Bao attracted transfer of bank deposits	• Require real-name identity verification*2 • Classification of individual payment accounts, capping transaction volume and account balance*2 • Disallow settlement and custodian for other FI*2
Protection	• Inappropriate product nature for speculation instead of protection • Sustainability/potential fraud of emerging insurance platforms	• Emergence of "innovative" insurance • Emergence of internet "mutual help" model	• Suspension of speculative products such as "limit down insurance ( )" by CIRC • Challenge the provision of insurance activities by non-regulated platforms (e.g. Quarkers ( ))*6

*1 "Notice on Strengthening Risk Management and Education Against Inappropriate Lending in Universities", 2016 April

*2 "Administrative Measures for the Online Payment Business of Non-Banking Payment Institutions", 2016 July

*3 "Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions", 2016 August

*4 "Issuing the Implementation Plan for Special Rectifications on Risks in Asset Management and Carrying Out Cross-boundary Financial Business Through the Internet", 2016 October

*5 "Issuing the Implementation Plan for Special Rectifications on Risks in Equity Crowd-funding", 2016 October

*6 "Note on Potential Risks Associated with Unlicensed Operation of Insurance Business by Internet Comapnies", 2016 April – internal document of CIRC which was later exposed and discussed publicly

Source: Oliver Wyman analysis

A RAPIDLY EVOLVING RISK LANDSCAPE: WHAT HAS CHANGED FOR RISK MANAGERS?

Lutfey Siddiqi
Visiting Professor-in-Practice, London School of Economics and Adjunct Professor at the National University of Singapore/Risk Management Institutek

As today's global risk landscape continues to change, the role of the risk manager needs to evolve in tandem. Given the interplay of a multitude of rapid developments globally, specifically in Asia, the context of risk management and risk preparedness has changed in recent years.

STRUCTURAL DISRUPTION

We are living through a period of multidimensional disruption, often referred to as the "fourth industrial revolution." Developments in extreme connectivity and extreme automation have consequences beyond the world of technology: business models, industries, markets, regulatory and governance regimes have been thrown into flux.

New dimensions such as cyber risk have entered the fray. It is increasingly difficult to differentiate between structural change and cyclical change. What were earlier considered structural and institutional constants—the concept of a non-negative risk-free rate for example—have turned into variables. As such, it is harder to differentiate risk from uncertainty. Are we wasting time trying to estimate "standard deviation" when the underlying

Risk management is much more than tools and metrics: it is about people, conduct, processes and culture.

distribution may be far from normal and bear no resemblance to its own historical series?

In recent years cyberattacks have plagued both organizations and individuals. They have breached nations and governments—often temporarily crippling them. The Bangladesh Central Bank was robbed when hackers used the SWIFT credentials to send fraudulent money transfer requests to the Federal Reserve Bank of New York. Similarly, there was a hacking attempt on Singapore's Ministry of Defence in early 2017. More recently in May and June 2017, the Wannacry and Petya ransomware attacks disrupted individuals, organizations, government services, and even hospitals. Countries such as China, Japan, Australia, India and South Korea were all affected.

Asia provides an almost perfect environment for cybercriminals to thrive in. This is made possible due to high digital connectivity, massive digital penetration accompanied with low cybersecurity awareness, and growing cross-border data transfers. As an example, government officials in some Asian countries still continue to use personal email accounts for official communication.

Though many countries in Asia are now developing and introducing cyber regulations, the framework is still weak and much more needs to be done. In this context, Asian businesses and governments need to have a strong cybersecurity policy in place to minimize damages.

SELF-INFLATING RISK

We are also living through a period of rapid feedback loops in which risk factors combine and aggregate in intricate ways. In several arenas, risk has become endogenous—that is, dependent on seemingly risk-mitigating action—resulting in a potentially wide divergence between perceived risk and actual risk.

We see this in the buildup of loss-absorbing bank capital on the one hand and a system-wide reduction in trading liquidity on the other. We see increased use of unconventional prudential policy at a macro level and more granular microprudential regulation of investment banks at a "book level"—not always in a mutually consistent manner.

For example, the imposition and withdrawal of a cap on the Swiss Franc (which had the effect of dampening local risk and heightening tail risk) had a direct bearing on subsequent value-at-risk calculations and trading risk capital. The "taper tantrum" of May 2013 and the Chinese stock market volatility of August 2015 were arguably policy-induced sources of macro risk with consequences for micro risk.

COORDINATION FAILURE

We are also witnessing a slowdown, if not a reversal, of the kind of global coordination that was a key risk-diminishing factor in the immediate aftermath of the global financial crisis. Global financial standards are being rolled out in fits and starts, the pace of implementation is uneven, national regulators rightly impose entity-level constraints, and administrative macroprudential measures (including capital controls if required) are now an acceptable part of central banks' repertoires. This, together with geopolitical flashpoints and a weaker backdrop for international conflict resolution, adds considerably to the base level of risk in the system.

In the Asia-Pacific region, the territorial dispute in the crowded shipping lanes of the South China Sea remains a potentially combustible source of risk. In South Korea, we saw the impeachment of the then president, fresh elections and the appointment of a new president. Meanwhile, North Korea remains in the headlines with increasingly belligerent missile tests.

Separately, in January, the U.S. withdrew from the Trans-Pacific Partnership (TPP), a trade pact that many Asian countries had pinned their economic hopes on, leaving the trade agreement in limbo. Ramifications such as these put businesses, governments and individuals at risk. While events such as these do create massive trade problems, they also cause geopolitical imbalances that leave the entire region in a state of uncertainty.

THE PEOPLE FACTOR

There is now a clear realization that risk management is much more than tools and metrics: it is about people, conduct, processes and culture. While modeling and continuous refinement of risk models will remain key to decision-making, it is important to underline that models will not replace the role of decision-takers. Judgment calls need to be made and trade-offs need to be assessed. To that extent, risk resilience is enhanced through the deliberate design of decision-making processes.

How do risk committees function within banks? How much constructive challenge is entertained? How do they ensure that a diversity of perspectives is considered?

From an Asian context, the cultural values imbibed in the region may be such that, across the board, hierarchy is rigidly followed and not enough constructive challenge is posed in the decision-making process. This could make those processes brittle and less nimble. Asia needs to be appropriately prepared.

CAN EMERGING MARKET MULTINATIONALS BECOME GLOBAL LEADERS?

Lourdes Casanova
Senior Lecturer and Academic Director of Emerging Markets Institute, Johnson School of Business, Cornell University
Anne Miroux
Visiting Fellow at Emerging Markets Institute, Johnson School of Business, Cornell University

Emerging economies have gained strength in wealth and influence over the past two decades, bringing about radical changes in the global economic landscape. The rise of their multinationals, the so-called emerging market multinationals (eMNCs), is an illustration of this phenomenon.

The overseas expansion of eMNCs has indeed been remarkable: For instance, about 20 percent of global outward investment flows today are accounted for by a group of 20 top emerging economies, the E20*; which had a share of 2 percent at the turn of the century. Not only have emerging market multinationals significantly increased their investment abroad, but they have also made significant inroads in the global corporate world.

For instance, today, about 30 percent of the firms in the Fortune Global 500 list (based on revenues) are enterprises from emerging markets (less than 10 percent 10 years ago). China leads the trend: With 98 companies, it ranked second in 2015 in terms of number of Fortune 500 firms—not far from the U.S. (128), but much more than the number 3, Japan (54). However, a wide array of emerging economies is represented in the list: 14 of the E20 grouping are mentioned, although sometimes with only one entry in the list. The new players come mainly from China, Korea, India, Brazil, Russia, Mexico and Indonesia.

CHINESE MNCS EMERGE AS LEADERS

Beyond the fact that emerging market multinationals significantly increased their presence among the largest corporations in the world, perhaps as remarkable is the fact that several have made it to the very top, becoming world leaders in their own sector. Let's take eight key industries: banking, logistics, automobile, telecom, engineering and construction, petroleum refining, mining, crude oil production and mining. In 2004, based on the Fortune Global 500 ranking, there was no emerging market multinational among the top five world leaders in these industries while, in 2015, 40 percent of such leaders came from emerging economies, largely dominated by China.

The shift has been particularly marked in banking (where all but one of the five leaders are Chinese), engineering and construction (where all top five are Chinese), and mining and crude oil production, as well as metals. In less traditional industries, such as IT consulting for instance, three Indian corporations are among the world's largest (TCS, Infosys and Wipro). In e-commerce, or platform industries, a similar trend is developing; witness Alibaba, and Wechat (Tencent), for instance.

PROFIT LAGS REVENUE

While they have made remarkable inroads as global corporations, emerging market multinationals still have a significant gap to close compared to the more established western multinationals regarding profits. Indeed, the average profit margins of emerging market multinationals lag behind those of their U.S. and Japanese counterparts. This difference can be quite important: About 27 percent of the Fortune Global 500 firms from emerging countries in the E20 group achieve a profit margin above 5 percent versus an average of 39 percent for the totality of Fortune Global 500. This suggests that, in their present expansion phase, emerging market multinationals have a stronger focus on revenues and market growth than on profit margins.

The overseas expansion of emerging market multinationals has disrupted the global competition landscape. These firms have been deploying themselves not only in their natural markets—mostly other emerging economies—but also more recently, and quite effectively, in developed markets, conquering industry leadership positions (as illustrated above) in the process.

The competition from these new leaders has become more acute both in developed and emerging markets. Will the trend continue? Is the balance tilting in favor of these newcomers? Some observers would argue that it is, given the increasing weight and influence of emerging markets in the world economy and the importance of consumer demand in those markets. It is an open question, even more today than before, and this is for several reasons:

1. Because growth has slowed worldwide, including in many of the emerging market multinationals' home markets. This is not really to the advantage of those firms that have surfed on this growth wave, many of them focusing on the search for revenues rather than profit.

2. Because the established players—the large corporations from developed economies—should not be underestimated in their capacity to react to this new competition, building on their long experience of operating in very competitive markets, and their capacity to overcome serious challenges and learn.

3. Because the past few months have brought about a significant degree of uncertainty, as protectionist measures are being seriously considered in a number of key economies. On the other hand, the past 10 years have shown that many of the newcomers are fast learners, able to expand globally and reach the top at an impressive speed.

   (Argentina, Brazil, Chile, China, Colombia, Egypt, India, Indonesia, Iran, Korea, Malaysia, Mexico, Nigeria, Philippines, Poland, Russia, Saudi Arabia, South Africa, Thailand, Turkey.)

About 30 percent of the firms in the Fortune Global 500 list are companies from emerging markets.

ABOUT THE GLOBAL RISK CENTER

Marsh & McLennan Companies' Global Risk Center addresses the most critical challenges facing enterprise and societies around the world. The center draws on the resources of Marsh, Guy Carpenter, Mercer, and Oliver Wyman – and independent research partners worldwide – to provide the best consolidated thinking on these transcendent threats. We bring together leaders from industry, government, non-governmental organizations, and the academic sphere to explore new approaches to problems that require shared solutions across businesses and borders. Our Asia Pacific Risk Center in Singapore studies issues endemic to the region and applies an Asian lens to global risks. Our digital news services, BRINK and BRINK Asia, aggregate timely perspectives on risk and resilience by and for thought leaders worldwide.