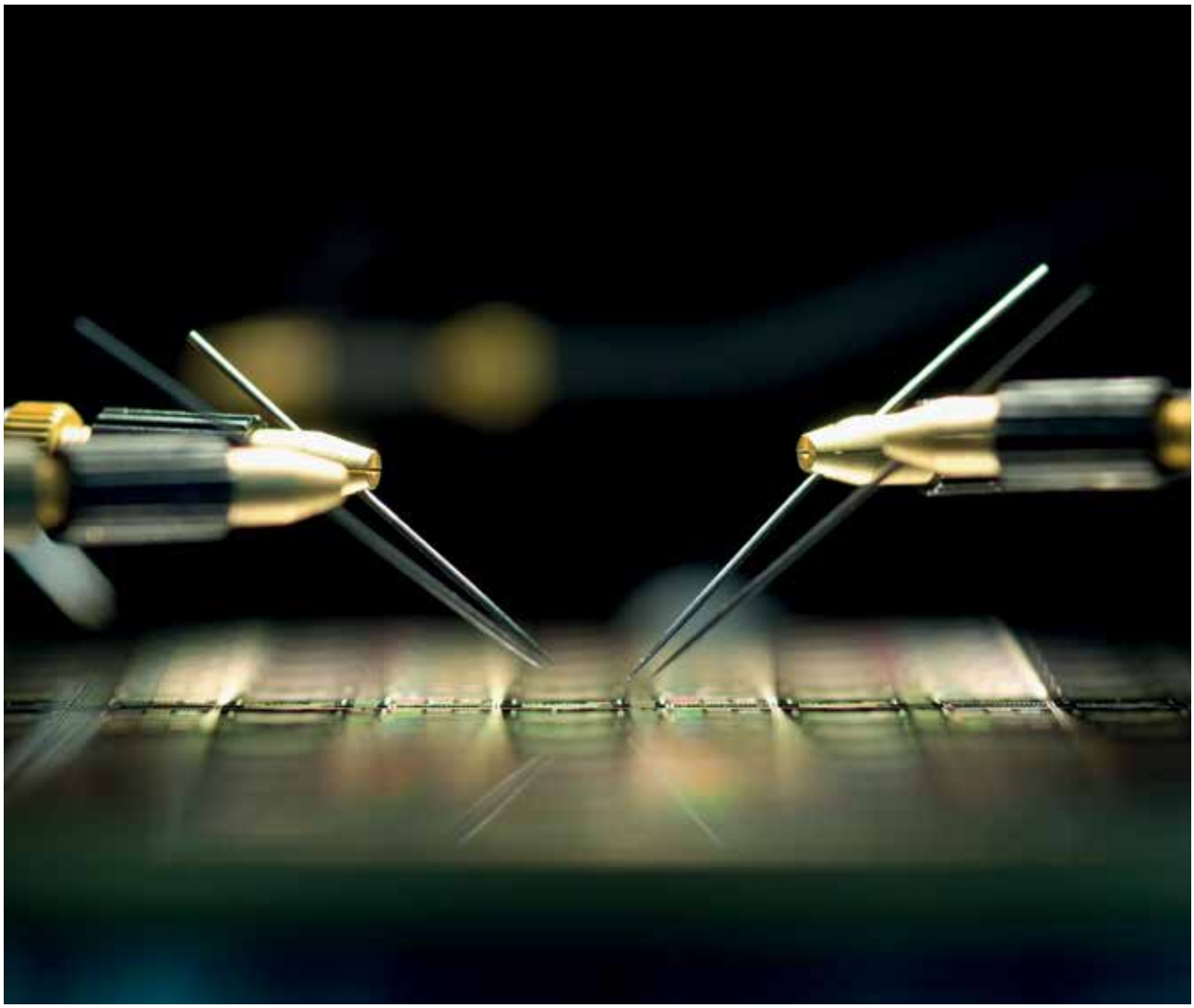
MARSH & McLENNAN COMPANIES | Asia Pacific Risk Center

BRINK The Edge of Risk

Embracing the disruption by emerging technologies

Expert perspectives on the Fourth Industrial Revolution



MARSH GUY CARPENTER MERCER OLIVER WYMAN

TABLE OF CONTENTS

CYBER RISKS AND SECURITY

ASIA IN FOCUS

WHAT'S NEXT?

INTRODUCTION

Artificial intelligence, robotics, and the digital revolution are just some of the expanding scope for emerging technologies to drive productivity across sectors such as transportation, healthcare, financial services, and the energy industries, to name a few.

While most businesses across industries are trying to master and deploy the disruptive technologies to enable economic benefits, they also present new hazards that exacerbate global risks, introducing opportunities as well as challenges across sectors. In particular, this disruption takes place against a backdrop of rising cyber threat landscape, a top risk concern for executives, including the more advanced economies in the Asia-Pacific region.

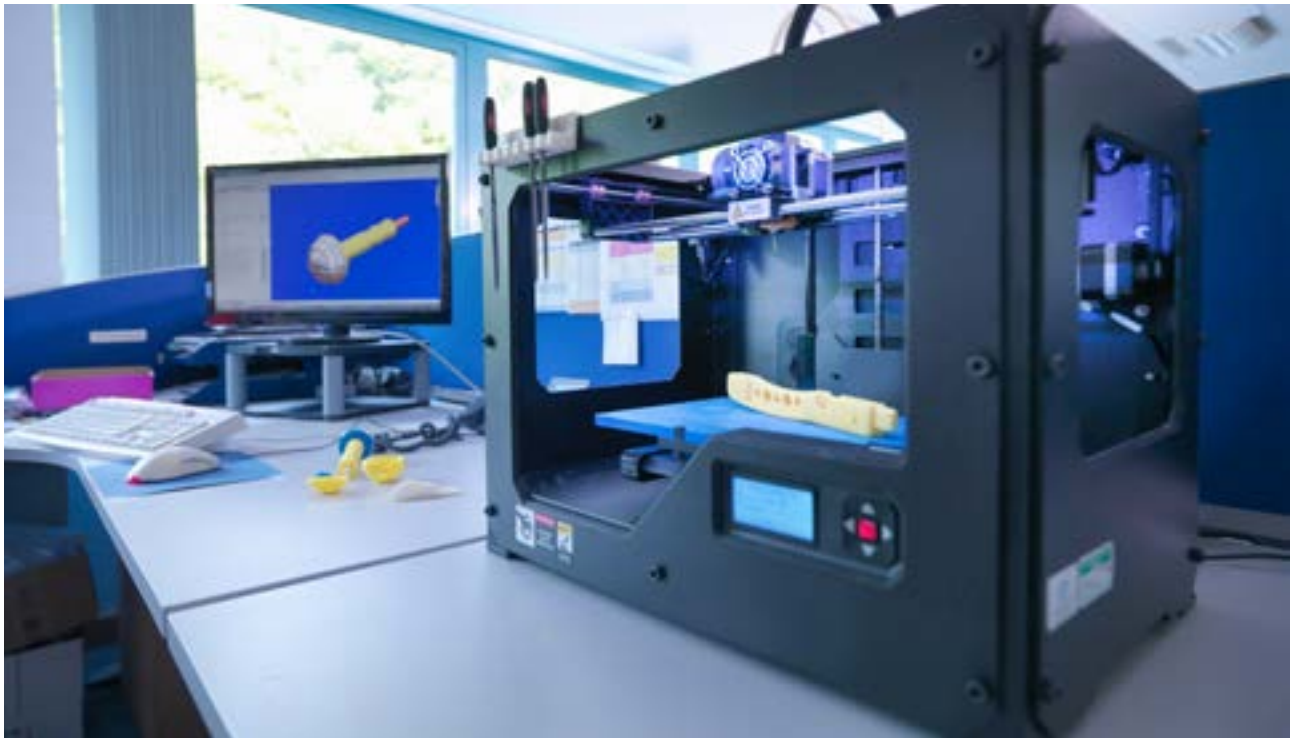
The articles presented in this publication have been selected to illustrate the key technologies and applications relevant to Asia, the associated risks and rewards to ensure successful navigation and management of this unprecedented change we all face today.

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

TECHNOLOGY

TAKING CHARGE OF DISRUPTIVE TECHNOLOGY RISKS

Brian C. Elowe
Managing Director and US 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.

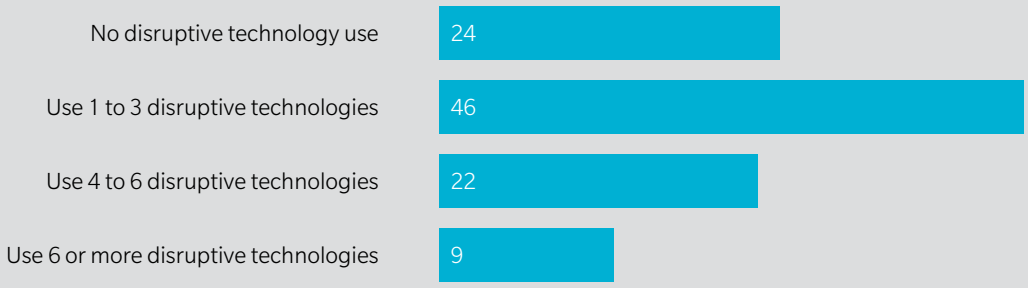
For example, 48 percent of risk executives told us their organization doesn't use or plan to use the Internet of Things (IoT); yet, according to many estimates, 90 percent of companies will be using IoT technologies within two or more years. Similarly, only 25 percent of our respondents said their organization 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.

Risk executives need to fortify their strategic role by understanding how technologies impact not just

EXHIBIT 1 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

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.

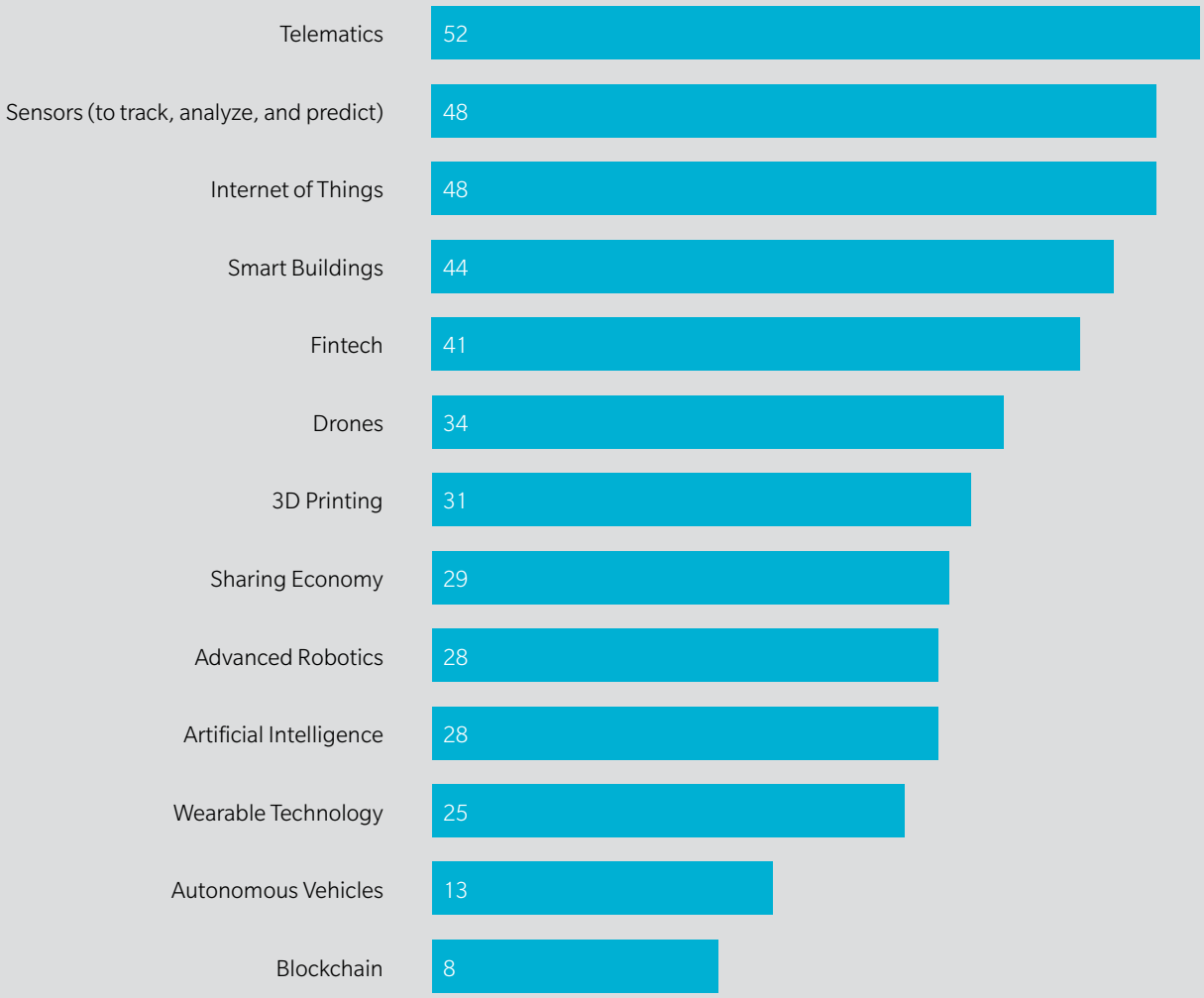
The pace of innovation is truly fascinating. As our colleagues at Lippincott put it: "There is no more important question to answer than 'What is the big, unstated need of tomorrow?' The answer is deep, constant, and insatiable inquiry." Educate yourself on terminology, on leading-edge innovations, about 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 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."

EXHIBIT 2 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

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 start 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.

This article first appeared on BRINK on April 24, 2017.

SOCIETY

TECHNOLOGY INNOVATION IS DISRUPTING RISK MANAGEMENT

Melissa Gale
Senior Manager, Risk Solutions at Lyft

Technological innovation in today's fast-paced business environment is full of potential benefits, but it is also fraught with risks. As more companies feel pressured to innovate, assessing the risks of disruptive technologies can sometimes fall by the wayside. Risk professionals who recognize the rewards along with the risks will help their companies successfully adopt new technologies.

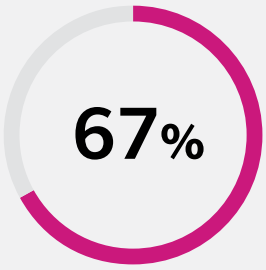
Traditionally, risk managers have been seen as isolated within their organizations. Nowadays, this can mean that a company's so-called innovators or disruptors may avoid seeking out the risk team for guidance. They fear that doing so may only lead to a lecture on why a new venture, process, or technology is a hindrance and shouldn't be pursued.

Fortunately, risk professionals today are increasingly aware of that scenario.

EXHIBIT 3 MAJORITY OF RISK PROFESSIONALS BELIEVE TECHNOLOGY INNOVATION IS KEY TO GAINING COMPETITIVE EDGE IN THEIR INDUSTRY
Source: Marsh New Reality of Risk online poll, 6 July 2017

91%
of risk professionals believe their organization will fall behind if it doesn't take advantage of new technologies.

EXHIBIT 4 SIGNIFICANT PROPORTION OF COMPANIES HAVE YET TO UNDERTAKE RISK ASSESSMENTS AROUND DISRUPTIVE TECHNOLOGIES
Source: Marsh New Reality of Risk online poll, 6 July 2017



of risk professionals are not aware of their organization having processes and procedures in place to trigger a risk assessment of a new technology before it is actually used.

In a recent poll conducted by global insurance broker Marsh, an overwhelming majority of risk professionals agreed that understanding technology innovation is *essential* in order to stay at the forefront of their industry.

Yet at the same time, two-thirds of these same professionals said their company either hasn't established plans and procedures to assess new risks or they were not sure if such processes are in place.

This lines up with the results from a recent survey conducted by Marsh and the Risk and Insurance Management Society, in which more than half of respondents said their company had not undertaken risk assessments around disruptive technologies.

"Given the impact that disruptive technology can have on the strategy of an organization, such lack of attention to the risks should be viewed as unacceptable," the report says.

A thorough assessment of the risks emanating from the use of tech innovations within an organization can enhance the understanding of a company's changing risk profile.

For example, at Lyft, our risk team works very closely with legal, finance, compliance, government relations, and others to fully understand technology risk from all angles. In general, challenges may have to do with reporting structures, conflicting priorities, and bandwidth, making cross-functional collaboration critical.

In recent years, a heavy focus on data breach and privacy due to cyber risks may at times steal the limelight from assessing other important risks.

EXHIBIT 5 KEY THREATS TO NEW TECHNOLOGIES TO RISK PROFESSIONALS
Source: Marsh New Reality of Risk online poll, 6 July 2017

Q: What aspect of new technology use at your organization is most likely to keep you up at night?

- **8%** Ability to assess risks
- **8%** Liability issues (legal and insurance)
- **7%** Integration with ongoing operations (including business interruption)
- **7%** Changing risk profile
- **6%** Errors and omissions
- **6%** Potential public relations crisis
- **4%** Contractual risk
- **3%** Regulatory compliance
- **1%** Board/leadership awareness and buy-in

EXHIBIT 6 TAKING CONTROL OF DISRUPTIVE TECHNOLOGY RISKS

EDUCATE

yourself about disruptive technology, terminology, innovations, and relevance to your company.

EXPAND

your network and foster collaboration through cross-functional teams and relationships and with outside experts.

PUSH

for investments in relevant data and analytics tools and skilled people to use them.

CONSIDER

the wider impacts – beyond cybersecurity – of disruptive technology on your company's risk profile.

Data breach, privacy and other cyber risks are certainly not to be taken lightly, but there is a broader range of risks related to disruptive technology that need to be accounted for as companies adopt new innovations.

Modern risk professionals need to look for solutions and alternatives that allow for innovation while balancing risk. And to do so, they need to help their company break down organizational siloes and ramp up discussions.

In a time when it is "disrupt or be disrupted," risk professionals must assert a leading role in understanding, assessing, and managing the risks and rewards of technology innovation.

This article first appeared on BRINK on June 26, 2017.

TECHNOLOGY

HOW RISKY ARE THESE TOP 10 EMERGING TECHNOLOGIES?

Andrew Maynard
Director, Risk Innovation Lab at Arizona State University

Take an advanced technology. Add a twist of fantasy. Stir well, and watch the action unfold.

It's the perfect recipe for a Hollywood tech-disaster blockbuster. And clichéd as it is, it's the scenario that we too often imagine for emerging technologies. Think superintelligent machines, lab-bred humans, the ability to redesign whole species – you get the picture.

The reality, of course, is that the real world is usually far more mundane: less "zombie apocalypse" and more "teens troll supercomputer; teach it bad habits." Looking through this year's crop of Top 10 Emerging Technologies from the World Economic Forum (WEF), this is probably a good thing.

Since 2012, I've been part of a group of WEF advisers who help compile an annual list of emerging technologies that are poised to transform our lives. This year's list includes autonomous vehicles, blockchain (the technology behind BitCoin), next-generation batteries and a number of other technologies that are beginning to make their mark.

The list is aimed at raising awareness around potentially transformative technologies so that investors, businesses, regulators and others know what's coming down the pike. It's also an opportunity for us to think through what might go wrong as the technologies mature.

WEF'S TOP TEN EMERGING TECHNOLOGIES 2016

1. Nanosensors and the Internet of Nanothings
2. Next Generation Batteries
3. The Blockchain
4. 2D Materials
5. Autonomous Vehicles
6. Organs-on-chips
7. Perovskite Solar Cells
8. Open AI ecosystem
9. Optogenetics
10. Systems Metabolic Engineering

Admittedly, some of these technologies would stretch the imagination of the most creative of apocalyptic screenwriters – it'll be a while, I suspect, before "Graphene Apocalypse" or "Day of the Perovskite Cell" hit the silver screen. But others show considerable potential for a summer scare-flick, including "brain-controlling" optogenetics and the mysterious-sounding "Internet of Nano Things."

Putting Hollywood fantasies aside, though, it's hard to predict the plausible downsides of emerging technologies. Yet this is exactly what is needed if we're to ensure they're developed responsibly in the long run.

TECH PROBLEMS, TECH SOLUTIONS

It's tempting to ask what concrete harm technologies such as those in this year's top 10 could cause, then simply figure out how to "fix" the problems. For instance, how do we ensure that "logical" self-driving cars safely share the road with less "logical" humans? Or how do we prevent bacteria that are genetically programmed to produce commercial chemicals from polluting the environment? These are risks that lend themselves to technological solutions.

But focusing on such questions can mask much more subtle dangers inherent in emerging technologies, threats that aren't as amenable to technological fixes and that we all too easily overlook. For example, being infused with internet-connected nanosensors that reveal your most intimate biological details to the world could present social and psychological risks that can't be solved by technology alone.

Similar concerns arise around "open artificial intelligence (AI) ecosystems," the next step up from systems like Amazon's Echo, Apple's Siri and Microsoft's Cortana. Combining "listening" devices, cloud computing and the Internet of Things, machines are increasingly combining the capacity to understand normal conversation with the ability to take action on what they hear.

This is a truly transformative technology platform. But what happens when these AI ecosystems begin to listen in on private conversations and share them with others? Or independently decide what's best for you? These possibilities raise ethical and moral concerns that aren't easily addressed solely by tech solutions.

EXPANDING OUR CONCEPTION OF WHAT WE VALUE

One way to tease out the subtler possible impacts of emerging technologies is to think of risk as a threat to something of value – an idea that's embedded in the somewhat new concept of risk innovation. This "value" depends on what's important to different individuals, communities and organizations.

Health, wealth and a sustainable environment are clearly important "things of value" in this context, as are livelihood, and food, water and shelter. Threats to any of these align with more conventional approaches to risk; a health risk, for instance, can be understood as something that threatens to make you sick, and an environmental risk as something that threatens the integrity of the environment.

But we can also extend the idea of a threat to something we value to less conventional types of risk: threats to self-worth, for instance, or culture, sense of security, equity, even deeply held beliefs.

These touch on things that define us as individuals and communities and get to the heart of what gives us a sense of purpose and belonging. In this way, relevant threats might include inequity or an eroded sense of self-worth from new tech taking away your job. Or anxiety over who knows what about you and how they might use it. Or fear of becoming socially marginalized by the use of new technologies. Or even dread over sacrosanct beliefs – such as the sanctity of life or the right to free choice – being challenged by emerging technological capabilities.

Threats like these aren't easy to capture. Yet they have a profound impact on people – and as a consequence, on how new technologies are developed and used. Thinking more broadly about risk as a threat to value is especially helpful to understanding the possible undesired consequences of tech innovation and how they might be avoided.

RISKS OF MISSING OUT ON NEW TECHNOLOGIES

This approach to risk also opens the door to considering the potential risks of not developing a technology. Beyond existing value, future value is also important to most people and organizations.

For instance, autonomous vehicles could eventually prevent tens of thousands of road deaths; optogenetics – using genetic engineering and light to manipulate brain cell activity – could help cure or manage debilitating neurological diseases; and materials such as graphene could ensure more people than ever have access to cheap clean water. Not developing these technologies potentially threatens things that many people hold to be extremely valuable.

Of course, on the flip side, these technologies may also threaten what is important to some. Self-driving cars might undermine human responsibility, not to mention the enjoyment of driving. Optogenetics raise the possibility of involuntary neurological control. And graphene might be harmful to some ecosystems if released into the environment in sufficient quantities.

By considering how emerging technologies potentially interact with what we consider to be important, it becomes easier to weigh the possible downsides of developing them – or at least developing them without due consideration – against those of either impeding their development or not developing them at all.

THE GREATEST RISK OF ALL

What emerges when risk is approached as a threat to value is a much richer way of thinking about how emerging technologies might affect people, communities and organizations, and how they can be developed responsibly. It's an approach that forces us to realize that the consequences of developing new technologies are complex and touch people in different ways – not all of them for the better. It's not necessarily a comfortable reconceptualization, but looking at risk from this new angle does pave the way for technologies that benefit many people and disadvantage few, rather than the other way around.

In reality, unlike the simplicity of Hollywood blockbusters, the risks associated with emerging technologies are rarely clear-cut and almost never straightforward. Yet they nevertheless exist. Every one of this year's World Economic Forum top 10 emerging technologies has the potential to threaten something of value to some person or organization, whether undermining an established technology or business model, jeopardizing jobs or influencing health and well-being.

These dangers are context-specific, often intertwined with each other, sometimes conflicting and often balanced by the risks of not developing the technology. Yet understanding and addressing them is essential to realizing the long-term benefits that these technologies offer.

Here, perhaps, is the greatest risk: that either in our enthusiasm for developing these technologies or our Hollywood-inspired fears of potential consequences, we lose sight of the value of developing new technologies that make our world a better place, not just a different one.

This piece first appeared in *The Conversation and BRINK on July 4, 2016.*

TECHNOLOGY

DISRUPTIVE TECHNOLOGY BRINGS RISK AND OPPORTUNITY TO INFRASTRUCTURE PROJECTS

Adrian Pellen
Infrastructure Segment Leader, US 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. These technologies promote efficiency, connectivity and sustainable growth.

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

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.

This piece first appeared on BRINK on August 14, 2016.

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.

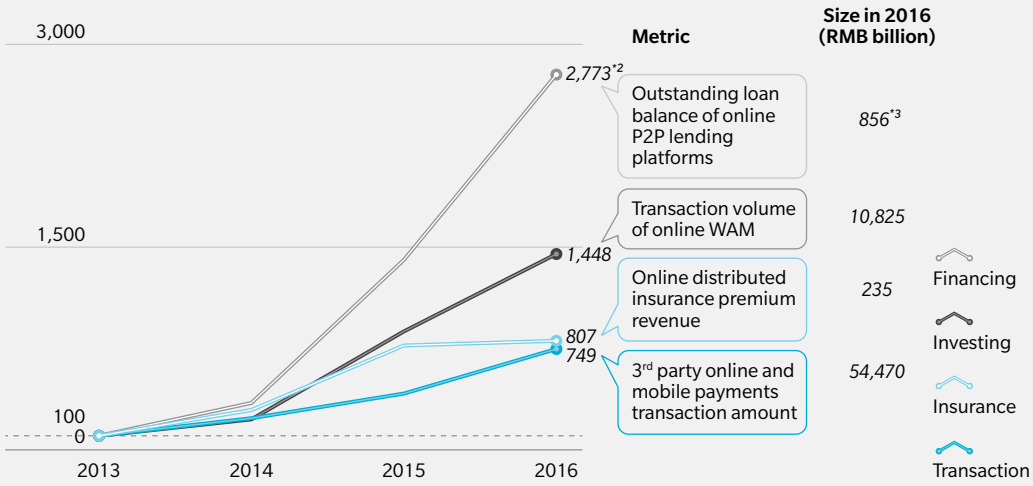
We believe the development of fintech in China has reached an inflection point. From this point, technology will be the key driver of value-chain disruption in an increasingly data-driven industry.

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 7).

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 US, 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 US.

EXHIBIT 7 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)

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 US, 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 US, 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.

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

CAs 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 8).

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:

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.

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.

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.

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.

This article first appeared on BRINK on August 24, 2017.

EXHIBIT 8 RECENT REGULATORY DEVELOPMENTS FOLLOWING GROWING CONCERNS AND INCIDENTS
Source: Oliver Wyman analysis

	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 (跌停险)" by CIRC • Challenge the provision of insurance activities by non-regulated platforms (e.g. Quarkers (夸克联盟))[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 Aug
4. "Issuing the Implementation Plan for Special Rectifications on Risks in Asset Management and Carrying Out Cross-boundary Financial Business through the internet", 2016 Oct
5. "Issuing the Implementation Plan for Special Rectifications on Risks in Equity Crowd-funding", 2016 Oct
6. "Note on Potential Risks associated with unlicensed operation of insurance business by Internet companies", 2016 Apr – Internal document of CIRC which was later exposed and discussed publicly

FINTECH

FINTECH SPURS INNOVATION IN ASIAN WEALTH MANAGEMENT

Steven Seow
Head of Wealth Management, Asia for Mercer

Asian wealth management is at an interesting inflection point, and the next five years will reveal some path-breaking developments in the industry. At one end of the spectrum, financial technology – fintech – is spurring innovation that is disrupting traditional banking and wealth management, and on the other end, banks are seeking to reinvent themselves by focusing on technology to offer more to customers.

When DBS, which is partnered with Kasisto, recently announced their first digital-only retail banking platform in India, naysayers and old guards truly started taking note of the buzz surrounding fintech and admitted that this is not a passing fad.

Recognizing the trend, Ravi Menon, Managing Director of the Monetary Authority of Singapore, is bullish on creating a strong ecosystem for fintech development in Singapore by way of the new FinTech & Innovation Group.

On the wealth side, a start-up called Robinhood now offers a free trading platform; whereas another, called R3, is building a 'blockchain' union among traditional banks. Blockchain, which is the technology on which the cryptocurrency bitcoin is based, could potentially be deployed to legitimize fintech-enabled transactions without the need to comply with the typical know-your-customer norms used in traditional banking.

Large traditional banks have begun to fortify their positions by either investing heavily in their technology infrastructure or, better still, launching their own fintech outfits to foster innovation from within – Citi FinTech being a recent case in

Banks are fortifying their positions by either investing in technology infrastructure or launching fintech outfits.

point. However, when we look past the novelty, we find that while every fintech entrepreneur may claim to have found the 'the next big idea,' only a select few have been able to successfully monetize that idea and turn it into a sustainable business model. Yet it is already disrupting private banking in Asia.

THE SLOW YET STEADY RISE OF THE ROBO-ADVISOR

Most players in Asia still advise funds way below the critical mass needed to be sustainable. The going rate for advisory fees currently hovers between 0.15 percent and 0.35 percent of the investment, which implies gross revenue of only S$150,000 ($111,940)-S$350,000 ($261,194) for S$100 million ($75 million) in assets under management (AUM). So for a robo-advisory business to sustain, it would need significantly more than S$100 million in AUM given the fixed cost structure of operating a robo-advisor business.

Another trend we see is the relatively small size of investments, typically under $200,000. This may be due to the fact that when someone is attempting to augment their retirement income, they implicitly accept a relatively lower rate of return. Inherent to robo-advisors is the concept of portfolio investing. With high returns from single asset classes becoming increasingly elusive with the current economic headwinds, investors are keen to spread their investments in portfolios. And robo-advisors offer advice based on sophisticated algorithms mapping portfolios rather than investments in, say, equities alone.

To offset the need for "human touch," especially for high-net-worth individual investors, a number of players in this space have begun migrating to a "bionic" or hybrid tech-augmented advisory model, where, in addition to the algorithm, there is a human advisor to guide the investor along the way.

The rise of robo-advisors points to an underserved need – the ability to see investment performance in real time rather than in static snapshots over a period of time – giving robo-advisors a leg up over traditional private banks and advisors. Investors like being able to track performance relative to standard benchmark indices for each of the asset classes within their portfolio.

A start-up called Future Advisor now provides such sophisticated analytics for free. This leads us to believe that banks will be compelled to up their game and offer more than periodic paper-based reports.

BETTING ON FINTECH

Beyond robo and analytics, the growth in fintech has been marked by the rise of multiple peer-to-peer lending start-ups, which endeavor to disintermediate lending to individuals and small enterprises. In 2015, three Singapore-based P2P start-ups – MoolahSense, Capital Match, and Funding Societies – raised more than S$10 million for small and medium enterprises.

Another sweeping trend we see in Asia with the rise of fintech is the investment directed at fintech itself. In particular, ultra-high-net-worth individual investors, and more discerning family offices in Singapore and throughout Asia, are looking at more avenues to seek higher returns.

The fintech industry itself has begun to look like a promising high-return investment haven.

With the increased volatility in equities and slowing returns in alternatives, the fintech industry itself has begun to look like a promising high-return investment haven and there has been a surge of investments into the sector.

As the fintech industry begins to bring together these start-ups and digital solutions in blockchain, analytics, lending and cybersecurity, we will find some degree of consolidation with either traditional banks acquiring promising fintech start-ups or multiple fintech companies merging or acquiring each other to broaden their value proposition.

Fintech continues to spur innovation along the entire wealth and banking value chain and will ultimately benefit individual investors above all. Traditional banking will evolve and become better as it becomes more digital. And banks will always be relevant as custodians of wealth, governed by strong legal frameworks, processes and regulation. Their challenge will be to match fintech companies in the speed of delivery, customer experience, and ability to provide financial information in real time.

The rise of fintech is as much a social phenomenon as it is technological. There is a need to ensure that enough checks and balances are in place, coupled with a longer-term view of what constitutes success in fintech as it relates to wealth management. Fintech is a strong means to an end, not an end unto itself. And the end is all about how an individual investor is empowered with more choice and better information in real time.

This article first appeared on The Business Times and BRINK on September 15, 2016.

WHAT ARE THE IMPLICATIONS OF THE RAPID GROWTH OF FINTECH IN CHINA?

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's fintech market has grown rapidly in recent times, but the potential for the sector's growth in China remains massive. Against that backdrop, the ability to develop and apply cutting-edge technology will be increasingly important for tomorrow's fintech leaders in China if they are to make the most of this phenomenon.

While different types of players will attempt to penetrate the market, we don't believe there is a one-size-fits-all formula for success, but rather that certain factors can increase the likelihood of success.

KEY SUCCESS FACTORS

We see five major key success factors for the future China fintech market:

Data abundance and application: Business models in financial services will be increasingly data-driven, and data will be at the core of the value chain. Therefore, innovation and impact in future fintech will be greatly helped by access to or ownership of large amounts of proprietary data, as well as the ability to derive insights from the data (Exhibit 9).

Large customer base: A large customer base will complement data capabilities, completing a virtuous cycle of mutual benefits for fintech players and their customers. First, fintech companies can apply data-driven insights to monetize their large customer bases, deriving direct economic value from the data. A large customer base, in turn, allows for faster accumulation of valuable data that can be analyzed to further improve products and services for customers, risk management and dynamic pricing.

Availability of proprietary and comprehensive products: Chinese consumers will increasingly seek unique, proprietary products. Fintech players will need to develop adequate scale and obtain necessary licenses so that they can offer a comprehensive suite of products to satisfy their customers' needs and differentiate themselves from peers.

Strong knowledge of financial services and risk management: A strong combined core of financial services expertise and risk management capabilities remains a prerequisite for success, allowing for more efficient identification of useful data and building of effective risk models.

"Fin plus tech" organization and culture: Constant innovation will be crucial in the future of fintech, and the right operating model

EXHIBIT 9 AVAILABLE DATA SOURCES FOR CREDIT-RISK MANAGEMENT
Source: Oliver Wyman analysis

DATA SOURCE	EXAMPLE	PURPOSE
TRADITIONAL DATA		
Central bank	Individual credit data	✓ Credit record
Proprietary data	User behaviour	✓ Identity verification
ONLINE SOURCED DATA		
Third-party credit agencies	Individual credit data	✓ Credit record, financial condition
Third-party data institutions	Blacklist, anti-fraud data	✓ Identity verification, credit record
Telecommunication operators	Telecom data	✓ Identity verification
E-commerce platforms	Consumption records in Taobao	✓ Consumption habit
CHSI, universities	Education level	✓ Identity verification, personal reputation
Information authorised by users in app	Private information (e.g. emails, messages)	✓ Assist collection
Social media	The use of Wechat, QQ, Weibo, etc.	✓ Personal reputation
Third-party payment institutions	Third-party payment data	✓ Financial condition
Other small loans/P2P/ online consumer finance platforms	Borrowings on other platforms	✓ Liability condition

and culture will be integral to success. This implies a lean, flat organizational structure with product-driven teams comprising both financial and technology talents in order to shorten product development cycles through hypothesis-driven experimentation and maximize returns by tailoring products for customers

IMPLICATIONS FOR FINTECH MARKET PARTICIPANTS

During the explosive growth of fintech in China in recent years, we have witnessed the establishment of four major types of players, with each type of player possessing its own strengths and weaknesses. Such dynamics result in rather different strategic foci for each type of player.

All-around Fintech Players should maintain their advantages by cementing their pioneering roles in the fintech space through technology-enabled innovation. First, they should continue to build their customer base and drive innovation using insights derived from their massive data pools. Second, using this abundance of data and their insight-generating capabilities, they should identify opportunities for needs-based cross-selling of financial services products. Third, given the recent regulatory trends, they should proactively apply for necessary licenses to sustain their business models.

Niche Fintech Players should expand and perhaps transform their business models. The first and most intuitive way is to grow organically beyond a niche. Qudian, for example, has expanded beyond its legacy focus on university borrowers to develop an e-commerce ecosystem driven by a consumer finance model. At the same time, we anticipate mergers between some niche players to consolidate their strengths and resources. Some players are actively considering expansion outside China in order to replicate their success in markets with similar needs, such as Southeast Asia. Since banks and all-around fintech players are dominant in their customer base, niche players could export their technological know-how to partner with traditional financial institutions.

Traditional Financial Institutions should build data capabilities under flexible organizational setups. First and foremost, they need to create leaner structures and culture with operating models

that are more suitable for fintech. This could also be done by setting up separate business units with more-independent authority and decision-making processes. It is important for traditional financial institutions to then invest in data processing capabilities and infrastructure to effectively monetize the traditionally offline customer base by leveraging on innovative data sources.

Players from Non-Financial Industries should carefully consider whether and how to best leverage their strengths and large customer bases to expand laterally into the fintech space. For example, logistics providers such as S.F. Express possess proprietary information on massive daily inventory flows, which is then incorporated into a risk-assessment methodology and used to power their supply chain financing and consumer lending ventures.

IMPLICATIONS FOR FINTECH INVESTORS

Capital investment in China fintech is hotter than ever. However, as the development dynamics of the industry are bound to change in the future, we believe that China fintech investors should follow the four key rules below.

Avoid overvaluing regulatory arbitrage. The historically open regulatory environment was one of the major growth drivers for a lot of fintech players. But tightening regulations are bringing the age of arbitrage to an end and will likely have a negative impact on fintech expansion. So, investors should identify targets' underlying growth drivers and avoid overestimating future value driven by regulatory arbitrage.

Explore the broader landscape. The integration of fintech into the regulatory framework has, to a certain degree, leveled the playing field for traditional financial institutions such as banks and securities firms. The recent strategic partnerships with fintech players by China Minsheng Bank and the introduction of online lending products by ICBC are just a few signs that fintech investors should start looking beyond fintech startups.

Assess the potential downside. Despite not bearing credit risks in legal terms, fintech platforms could face reputational losses, regulatory actions, and even liquidations due to potentially problematic products.

This has been illustrated by the cases of Ezubao and Zhao Cai Bao. Although the number of such products will likely diminish under the tightening regulations, investors ought to be aware of downside scenarios and diligently assess their potential impact.

Capture value from technology and the surrounding infrastructure. As technology-enabled disruption is the main trajectory for China fintech, investors should look beyond the actual innovative solutions and products. There is also value in the infrastructure enablers behind such products, such as large user bases for trials, access to proprietary data for analysis, and agile fin plus tech governance structures.

While current leaders might be able to build on their strengths and expand on all fronts, the chaser pack could still find major places for themselves by applying differentiated technology in spaces where it is needed. Strategic planning, significant and rightly directed investment and prompt action are required for tomorrow's Chinese fintech leaders. The fintech landscape in China is evolving fast – only those who weigh it right will be able to hit gold.

This article first appeared on BRINK on August 31, 2017.

Strategic planning, significant and rightly directed investment and prompt action are required for tomorrow's Chinese fintech leaders.

FINTECH

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."

EXHIBIT 10 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

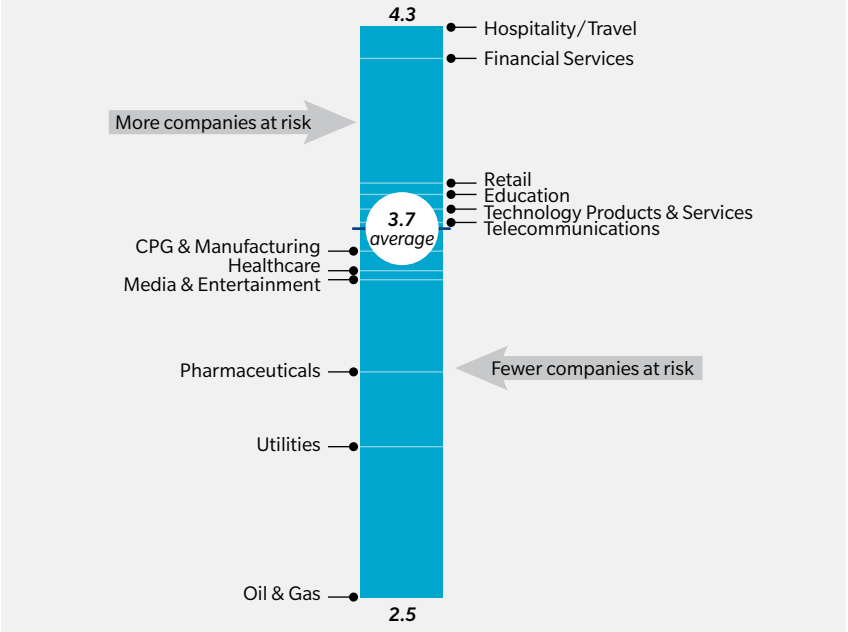


EXHIBIT 11 SELECTED EXAMPLES OF HOW COMPANIES DISRUPT TRADITIONAL FINANCIAL SERVICES USING EMERGING TECHNOLOGIES
Source: Author's research

CATEGORY	COMPANIES
Payments	PayPal, Dwolla, Square, M-Pesa, Billtrust, Kantox, Traxpay, Venmo
Alternative currencies	Bitcoin, Bitstammp, Xapo, BitPay, Etherium, ZCash
Product and service advice	Bankrate, MoneySuperMarket, LendingTree, Credit Karma
Personal finance management	Fintonic, Moven, MINT, Digit
Wealth management and advice	Betterment, Wealthfront, SigFig, Personal Capital, Nutmeg
Crowdfunding (Capital and debt)	Lending Club, Kickstarter, Crowdfunder, AngelList, SeedInvest
Peer and pre-approved lending	Lending Club, Prosper, Kreditech, Lenddo

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. Exhibit 11 above 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.

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.

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.

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 US 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 US 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, the online research and business analysis journal of the Wharton School of the University of Pennsylvania, and BRINK on July 28, 2017.

FINTECH

INSURTECH IN CHINA: REVOLUTIONIZING THE INSURANCE INDUSTRY

Cliff Sheng
Partner and Head of Financial Services, Greater China at Oliver Wyman

China's capital markets aren't yet mature enough to support financial innovation; meanwhile, existing state-owned financial institutions are not reforming quickly enough. This gap in supply has provided opportunities for Chinese fintech players – who are being supported by rapidly growing online ecosystems and a tech-savvy population – in diverse fields ranging from investing to payments.

A GROWING INSURANCE MARKET

While insurance penetration in China is currently low (3.6 percent in 2015) compared to developed markets such as the UK (10 percent) and the US (7.3 percent), strong government support, coupled with a growing middle class, is making insurance products more accessible.

In 2015, for example, total insurance gross written premiums (GWP) in China increased by 20 percent in 2015 to 2.4 trillion yuan ($355 billion).

In fact, the Chinese insurance market has doubled in size over the past six years. Based on China Insurance Regulatory Commission's (CIRC) five-year plan and various other sources, the insurance market is forecasted to grow at 13 percent (compounded annually) up to 2020 to 4.5 trillion yuan.

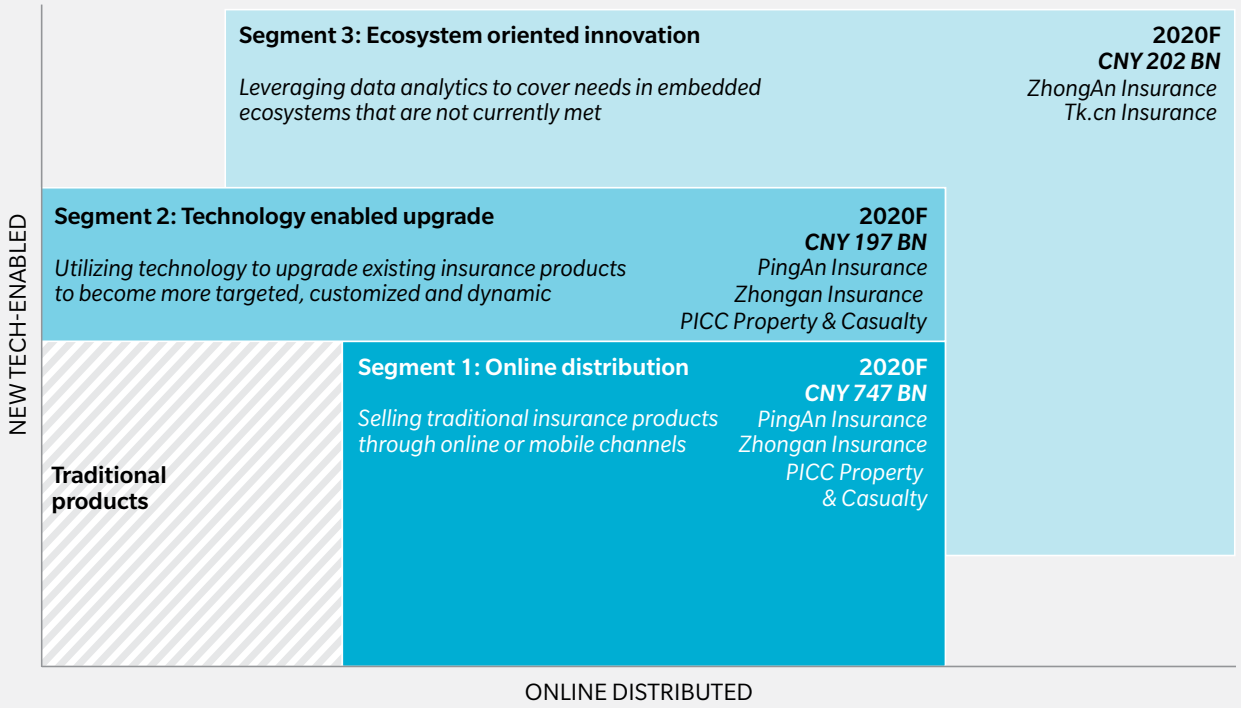
The rapidly growing insurance market – albeit from a low base – in China is also opening up plenty of opportunities for insurtech (defined as insurance further enhanced through technology in a customer-centric way).

INSURTECH MAKES GAINS

Insurtech is revolutionizing the insurance industry by bringing disruptive products and services to a market that is fast adopting, and increasingly moving toward, an online ecosystem. The market is also seeing a surge in the number of people who are aware of and are starting to understand the benefits of insurance.

The CIRC is supporting these gains by fostering a favorable regulatory environment for insurtech. As a result, the insurtech market is experiencing rapid growth and is expected to rise from 250 yuan in 2015 to more than 1.1 trillion yuan in 2020.

EXHIBIT 12 CHINA INSURTECH SEGMENTS, KEY PLAYERS AND MARKET SIZE FORECAST BY 2020
Source: Oliver Wyman analysis



There are broadly three insurtech segments in China (Exhibit 12), which are projected to grow at different rates:

Online distribution of traditional insurance products (e.g. online auto insurance sales). According to Oliver Wyman estimates, GWP for this segment will grow from about 207 billion yuan in 2015 to about 747 billion yuan in 2020. And within this segment, non-life insurance products will grow at a faster pace than life products.

Technology enabled upgrades of existing insurance products (e.g. new health insurance policies or prices based on wearable devices, telematics). GWP for this segment is expected to grow from about 28 billion yuan in 2015 to about 197 billion yuan in 2020. Auto insurance will be the highest contributor to this growth, followed by health insurance products.

Ecosystem-oriented innovation of new insurance products (e.g. shipping return insurance, flight delay insurance). Estimates show that GWP in this segment will grow from 12 billion yuan to 202 billion yuan between 2015 and 2020. The key contributors to this growth being the e-commerce and travel ecosystems because of their large market size and the growing desire among consumers to protect themselves against risks related to these ecosystems.

RISKS AND UNCERTAINTIES FACING THE INSURTECH INDUSTRY

Notwithstanding the tremendous scope and opportunity for certain simple products – such as travel insurance and shipping return insurance – in the Chinese insurtech market, several products such auto insurance and universal life insurance face uncertainties owing to the following four factors:

Macro economy. A fall in Chinese GDP growth to 5 percent or lower would have an adverse impact on per capita disposable income, which in turn could negatively affect the demand for non-essentials such as automobiles, wearable devices and connected home devices. As a result, GWP in these sectors would fall.

Regulation. In general, the CIRC has been supportive of innovation, but there are times when it has been too conservative. For instance, the regulator may put a limit on guaranteed return of universal life insurance distributed online. Online universal life was recently stopped by the regulator (which is considered a temporary measure to curb increasing risk). In another case, we observed that the slow

adoption of telematics is caused by the tariff set by the regulator even after the recent pricing reform for auto insurance. In another case of regulatory back-and-forth, smog travel insurance, which compensates travelers during bad weather caused by smog, has been stopped by the regulator.

Technology. Future development of technologies such as big data, cloud computing, block chain and artificial intelligence are critical to insurtech. Therefore, technological failures of particular platforms can pose risks for companies, particularly when they are looking to ramp-up operations.

Competition. Traditional insurers and disruptors currently dominate the industry. Traditional insurers may set up joint ventures with tech companies to compete with disruptors, or they might set up subsidiaries to attack this market. New players could also emerge, increasing competition. For example, auto or 3C (computer, communication and consumer electronics) manufacturers could set up insurance companies to insure their own products. Similarly, peer-to-peer insurers may rise to cover online communities and large ecosystems might also self-insure.

Despite these uncertainties and possible risks, there is potential for the insurtech industry in China, with the forecasts clearly suggesting a growing opportunity set for businesses in this space. The question is whether it will meet or exceed expectations.

This article first appeared on BRINK on November 7, 2016.

CYBER RISK IN ASIA: INCREASING TRANSPARENCY TO LIMIT VULNERABILITY

Wolfram Hedrich
Executive Director of the Asia Pacific Risk Center and Partner in the Finance and Risk practice at Oliver Wyman

Jaclyn Yeo
Senior Research Analyst at the Asia Pacific Risk Center

Asia is an ideal environment for cybercriminals to thrive in due to high digital connectivity and the accelerating pace of digital transformation, contrasted with low cybersecurity awareness, growing cross-border data transfers and evolving but still weak regulations.

Compounding problems is a lack of transparency, which leads to the inaccurate general perception that the cyber threat level is lower in Asia than other regions.

According to the Global Risks Report 2017, concerns around the likelihood and impact of technological threats has sharpened among business executives in Asia, and cyberattacks are ranked among the top five risks of doing business in the region.

The need to combat cyber threats has never been more urgent in Asia, and many major industries in the region – including construction and engineering, financial, high-tech and electronics – are especially susceptible, according to a new report from Marsh & McLennan Companies' Asia Pacific Risk Center (APRC). A series of recent, high-profile cyberattacks have touched multiple countries and industries across the region, highlighting the issue.

The worrying factor is that although these breaches grab the headlines, there are deeper issues lurking. "The majority of cyberattacks in the region usually go unreported as companies are neither incentivized nor required to do so," said Cheah Wei Ying, an expert on non-financial risk at Oliver Wyman. "This lack of transparency underpins Asia's susceptibility to cyberattacks."

TRANSPARENCY TRENDS IN ASIA

We argue that there is still a lack of transparency in Asia that reduces visibility about the level and frequency of cyber attacks, resulting in the perception that cyber threat is lower in Asia than

EXHIBIT 13 RISING CYBER RISK TRENDS IN ASIA AND KEY CHALLENGES IN MANAGING CYBERSECURITY
Source: Asia-Pacific Risk Center, "Cyber Risk in Asia-Pacific: The Case for Greater Transparency"

THE SEVERITY OF CYBERATTACKS

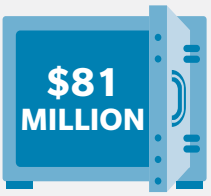
in business revenues lost to cyberattacks[1]

Ranked **5th** among **Asian** top risks[2]

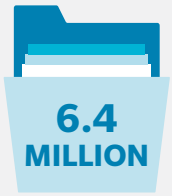
Ranked **6th** among **Global** top risks[2]

RECENT CYBERATTACKS EXAMPLES IN ASIA

personnel stolen from Singapore's defense ministry online database portal in Feb 2017[4]



stolen from cyberattack on a bank in Bangladesh in May 2016[5]



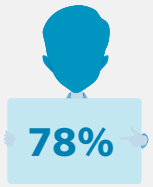
children's data stolen in Hong Kong hacking of a digital toymaker firm in in Dec 2015[7]

Philippine government websites **simultaneously hacked** in July 2016[6]

ASIAN FIRMS LAG IN CYBERSECURITY

Asian organisations take **1.7 times** longer than the global median to **discover a breach**[8]

Asian firms spent **47%** less on information security than North American firms[9]



of Internet users in Asia have **not received any education** on cybersecurity[10]

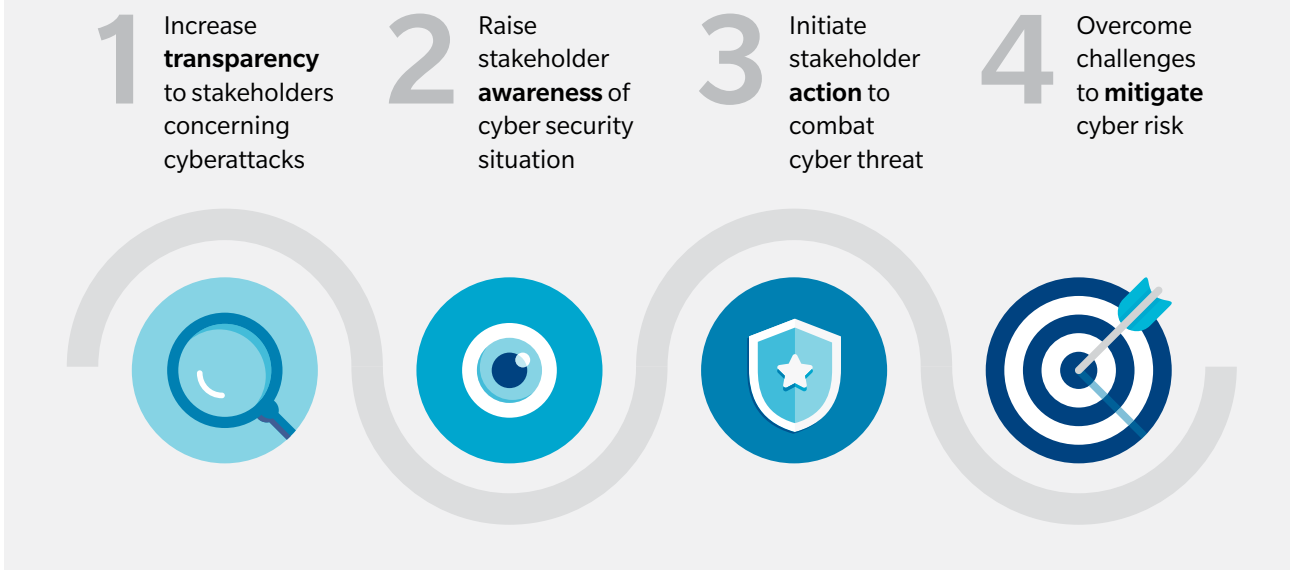
CHALLENGES FOR FIRMS IN MANAGING CYBERSECURITY

70% of firms do not have a strong understanding of their cyber posture

of organisations found it "difficult-to-extremely-difficult" to recruit cyber talent[11]

Primary insurers are reluctant to provide single coverage above **$100 MILLION**

EXHIBIT 14 THE ROLE OF TRANSPARENCY IN MITIGATING CYBER RISK
Source: Asia-Pacific Risk Center, "Cyber Risk in Asia-Pacific: The Case for Greater Transparency"



it actually is. That, in turn, leads to insufficient investment in cybersecurity among corporations and erodes the urgency for tighter cybersecurity among regulators.

The degree to which Asia lags behind the rest of the world is highlighted in recent research, which found the median time between a breach and its discovery for Asian organizations is almost double the global average – 172 versus 99 days.

Underpinning the region's transparency issue is its lack of data breach notification laws – which typically require companies that are compromised to inform regulators and stakeholders and take steps to remediate or face a heavy penalty, with the exception of Japan, Australia, South Korea and the Philippines, for example. In some countries, breach notification may be industry-specific; for example, the Monetary Authority of Singapore requires financial institutions to notify them of any breach of security or confidentiality of customer information, or any events that can potentially lead to prolonged service disruption.

This indicates that some governments and policymakers have yet to recognize the importance of transparency in the battle against cyberattacks, which shrouds perceptions and influences the behavior of corporations, resulting in inaction or inadequate mitigation efforts.

Detailed and clear data breach notification laws, supported by enforcement, and a culture of compliance within organizations are critical to improving transparency and improved risk mitigation.

Although this breaks the opacity that most organizations would prefer, such legislation keeps companies accountable to their stakeholders, allowing them to protect their reputations and also minimize losses that could result directly and indirectly from breaches in the cyber architecture.

Another challenge that Asian governments face is that even when willing to put in place legislation to ensure transparency, they have been slow in doing so, compared to the rapid pace of digital transformation in Asia. This is in contrast to the West, where digital progress was slightly more incremental and allowed regulators somewhat more time to adapt, assess and implement necessary safeguards.

GOVERNMENT ACTIONS TO ENHANCE CYBER TRANSPARENCY

Beyond legislation of detailed and clear data breach notification laws, governments in the region can further mitigate cyber risk through public-private information sharing, the development of cybersecurity knowledge hubs and growing the cybersecurity talent pool.

Public-private information sharing is a useful and necessary defense tool against cyberattacks; both the public and private sector hold critical information in the fight against cybercrime, and there is growing recognition of the need to consolidate this information to obtain a fuller view of the cyber-risk landscape.

Governments should also develop cybersecurity knowledge hubs, which go hand-in-hand with growing the cybersecurity talent pool. Building cyber resilience requires experience and technical expertise, and the development of cybersecurity hubs can act as central knowledge and talent repositories for cutting-edge innovation, technologies and personnel expertise to bridge the gap necessary to build an effective cyber defense.

THE NEED TO ACT

Asia has never been more vulnerable to cyber attacks, and the exposure to cyber threat is disproportionately large compared to the amount of investments in cybersecurity and risk management strategies by governments and corporations.

Clearly, a lot more work is required. Governments need to find ways to effectively implement and enforce breach disclosure laws, companies must renew long-entrenched approaches to cybersecurity and individuals have to play their part and practice good cybersecurity habits.

The progress towards transparency is currently piecemeal across stakeholders. The lack of convergence on breach notification regulations in the region suggests that governments have yet to recognize the key role that transparency plays in the fight against cyber risk. That needs to change urgently if the region wants to become more cybersecure.

This article first appeared on BRINK on March 31, 2017.

ASEAN: THERE CAN BE NO DIGITAL ECONOMY WITHOUT SECURITY

Naveen Menon
President, ASEAN of Cisco Systems, Singapore

Across the world, digital technologies are disrupting industries, improving lives and propelling progress. Similarly, we see these changes taking place in ASEAN (Association of Southeast Asian Nations) countries, building on the fundamentals for digitization that are in place – such as the growing economies of Thailand and Indonesia, which have highly digital and young populations (50 percent of ASEAN's population is under 30 years of age) and an extremely high literacy rate of 94 percent. Infrastructure is also well developed – 90 percent of people in the region have Internet access.

The conditions are ripe for ASEAN to become one of the world's top five digital economies and a major global economic player by 2025. To achieve this, the ASEAN needs to implement a comprehensive digital agenda and strategy. Doing so could add $1 trillion to ASEAN's GDP over the next decade.

This is why digitization is incredibly relevant for the region. By pioneering the development of new digital services and business models, ASEAN countries will create new areas for economic growth. The clearest example today is the tech sector – it's changing the way citizens work, live and play through businesses that are built on the sharing economy. But beyond that we are also seeing the rejuvenation of old sectors, such as manufacturing, which is moving toward "Industry 5.0" and reaping the benefits of improved efficiency, flexibility and widespread customization.

THE CORNERSTONE OF DIGITIZATION

While it's clear that digitization is paramount, there are many aspects to consider. But underlying all of that is security, which is absolutely fundamental. To fully realize the opportunities that are described above, security needs to be a core part of any digital transformation strategy. Today, we have a diverse and growing threat landscape. And as business goes digital, the number of external touchpoints will only grow, making them increasingly vulnerable.

Security is what protects businesses, allowing them to innovate and build new products and services.

Beyond a defensive role, security provides businesses with a strategic growth advantage. Here's an example: customer data – imagine you're a business like Go-Jek, an Indonesian transport, logistics and payments startup. Regardless of the value you add to the market, do you think customers would willingly use your service if they didn't trust you to handle their sensitive information? Trust creates widespread use of the service, which in turn generates valuable data, allowing Go-Jek to identify growth opportunities in terms of creating new services or improving existing ones.

This is just one example of the importance of security – Cisco has identified 414 security-enabled digital use cases that will drive $7.6 trillion in value over the next decade.

GETTING STARTED

There are three key areas for organizations to focus on when it comes to security: strategy/policy, technology and people.

Businesses need to look at security from a big picture perspective. It's about saying "let me have a security blueprint to enable the business" more so than worrying about the tactical aspect of "how do we detect where the vulnerabilities are within the environment?" This means thinking about security end-to-end, throughout the organization, from the network to the cloud to the customer endpoints.

An architectural approach allows products to be integrated and built to share context and information on threats. Such an approach takes advantage of investments and network infrastructure already in place, which means that scaling security alongside business growth is simple and straightforward. It creates a multiplier effect and reduces cost by over 30 percent vis-a-vis a point-product approach. For example, the western Australian education department is able to centrally manage security for 798 school sites without having to worry about scalability.

From a technology standpoint, a company needs technology that visualizes what's happening across the entire network. With that, a company can respond to threats before they occur. That said, when breaches do occur, security needs to be automated across physical, virtual and cloud touchpoints to reduce complexity and quickly remediate attacks.

Besides processes and technologies, organizations will also need to invest in people to become more resilient in the face of new attacks. It's evident that many high-profile security breaches in recent times began with a phishing attack on a single employee.

It should be the responsibility of tech industry players and government bodies to drive the cyber security agenda.

Only increased employee awareness could have prevented these events. Hence, personal responsibility with respect to security must become a business priority, too. And as the lines between personal and enterprise technology blur, organizations can also consider extending protection to employees in their personal use of technology.

BUILDING AWARENESS

Given that ASEAN is such a diverse and complex region, political and cultural differences and variations in economic behavior can make awareness-building a challenge. It should be the responsibility of industry players and government bodies to drive the security agenda through comprehensive awareness-building programs. By doing so, we empower ASEAN to achieve its potential and claim its rightful place as one of the leading lights of the global digital economy.

This article first appeared on the World Economic Forum Agenda blog and BRINK on May 16, 2017.

A GROWING CYBER VULNERABILITY: THE COMPETITION FOR TALENT

Tom Jacob
Senior Partner and Global Leader of Research & Insights in the Information Solutions group of Mercer's Talent Division

Karen Shellenback
Principal and Leader of Research and Insights for Mercer Select Intelligence

The rise of the Internet, data and communication technologies in concert with the proliferation of mobile and interconnected ecosystems has revolutionized every aspect of modern society. However, our never-ending reliance on technology has also created new vulnerabilities and avenues for harm for those who wish to capitalize on financial and otherwise nefarious schemes. The cyber vulnerabilities that organizations face today are pervasive and formidable.

But to view the challenges through only a technological lens is missing half of the equation.

Fundamentally, cybersecurity remains a human problem, and the solution to that problem lies with human beings. Thus, understanding the role of human capital is critical in the development of innovative security solutions. In 2015, competition for talent in this field is a make-or-break factor for organizational resiliency and competitiveness.

A CONVERGENCE OF CHALLENGING FACTORS: THE CYBERSECURITY LABOR POOL

The cybersecurity field is growing exponentially, and the demand for skilled tech workers exceeds the supply.

The supply of talent, however, is hampered by a convergence of factors that have placed an unintentional stranglehold on the workforce. Consider the following challenges organizations face in hiring cybersecurity talent in 2015:

- Exponential growth: Cybersecurity jobs postings have grown 74 percent between 2007 and 2013. This growth rate is more than two times faster than all other IT jobs. In particular, cloud computing and mobile connectivity are experiencing exceedingly rapid growth trajectories. These new globally adopted technologies are driving the need to address a new set of security concerns and are propelling cybersecurity job growth in the professional services, public administration, manufacturing, defense and retail sectors

- Demand exceeds supply: Although the cybersecurity field is growing rapidly and offers very competitive pay, demand for these IT specialists exceeds the supply of credentialed, experienced professionals. Research at Cisco Systems Inc. in 2014 linked recent high-profile security breaches to the shortage of nearly one million skilled cybersecurity professionals

- Supply is hampered by multiple interwoven challenges: There are many educational and experiential barriers for those interested in moving into cybersecurity roles, including the need for four years of education and four to five years of work experience or certification. Yet, only 186 institutions offer cybersecurity coursework, which accounts for less than 5 percent of all American colleges and universities. These requirements effectively eliminate new graduates and create a dearth of entry-level positions, which are necessary for building a robust pipeline. Finally, cybersecurity leadership requires a focus on the people issues, calling for executive communication skills, negotiation skills and gravitas along with operational, legal or line-of-business exposure. Finding talent with the right mix of these skills is extremely difficult

THE UNINTENDED CONSEQUENCES – LABOR MARKET RESULTS

The unintended consequences of the above educational, experiential and hiring requirements have, in part, resulted in the following:

Building your cybersecurity talent pool takes longer than other IT positions:
According to Burning Glass, cybersecurity job postings take, on average, 24 percent longer to fill than other IT job postings and 36 percent longer to fill than all other job postings. Senior level cybersecurity positions take even longer to fill: On average, filling a cybersecurity position at the senior level takes 9.2 months.

Cybersecurity talent costs more than other IT positions:
Cybersecurity jobs pay approximately $10,000 to $20,000 more annually than comparable IT jobs and salaries are increasing at a faster rate than the average IT position. In addition, 83 percent of cybersecurity new hires are receiving more-than-average pay increases.

Companies that have a hard time attracting and retaining cybersecurity talent risk falling behind in terms of competiveness and add more uncertainty to the ever-growing equation of holistic organizational risk. So, what can

Understanding the role of human capital is critical in the development of innovative security solutions.

organizations do to increase the flow of cybersecurity talent into their organization? Like any other job category with hard-to-find skills, companies must create a comprehensive talent strategy and action plan.

11 WAYS TO ATTRACT AND RETAIN CYBERSECURITY TALENT

In the 2015 marketplace, where demand is high and supply is low and cybersecurity professionals are poached daily, a well-executed talent strategy with progressive attraction and retention incentives is a must. A strategic cybersecurity talent action plan should include the following elements:

Evaluate your company brand.
What is it that makes the organization stand out from the rest and how is the company perceived in the larger arena of social media and the crowd-sourced blogosphere? If your organizational presence is nonexistent or negative, it is time to dedicate resources (financial and otherwise) to change that image.

Understand current engagement levels.
Engage cybersecurity staff in brainstorming solutions and action planning, so as to increase the excitement and engagement of your critical team members.

Harness strategic workforce planning and metrics.
Using data analytics and workforce planning applications, the human resources (HR) function must work with cybersecurity leadership to create a plan that lays out the anticipated ebbs and flows of talent streams, patterns of attrition, bench strength, career path mapping and avenues for bringing critical talent in the door.

Partner with universities to develop emerging curriculums and open up access to potential new hires.
Providing real-world curriculum challenges as well as on-site job rotations, networking opportunities, co-ops and internship opportunities allows young workers the development experience they need and the exposure hiring organizations require.

Provide training and more training.
Companies must make the most out of the talent already in place. Providing specific training opportunities to current staff on emerging technologies is a requirement that cannot be overlooked.

Create enticing career path trajectories.
In a field where talent is in short supply and one can jump ship for added responsibilities and pay, having a visible, enticing, attainable and tangible internal career map is essential.

Focus on creative career growth opportunities.
Create opportunities to highlight significant accomplishments and provide a clear line of sight and accelerated growth paths that align with career goals, passions and personal aspirations.

Improve processes, communication and productivity.
Increase the productivity among the cybersecurity team by using new technologies to manage day-to-day workflow processes and efficiencies.

Increase the use of open-source collaboration and external networks.
Consider the use of community collaboration models, including design challenges, hackathons and open-source community platforms to tap into external networks and locate potential talent.

Build line-of-business experience.
Provide training opportunities to IT staff on business strategy, negotiation, legal considerations and communications, along with stronger ties to senior management, to enable cybersecurity leaders to translate corporate business strategy into risk and cybersecurity resource plans.

Open the door to all talent.
Increase talent acquisition channels to look beyond what HR and recruiters may deem as the appropriate experiential requirements (B.S. degree, four years of experience and certifications).

The cybersecurity field is growing by leaps and bounds. The need to stay in front of a rapid and exponential technological landscape with astounding opportunities and vulnerabilities is simply... daunting.

The demand is exceedingly high and the pressure to find critically specialized talent to address the inherent challenges and vulnerabilities is not about to go away. Organizations that want to remain competitive and reduce substantial organizational risk must invest in cybersecurity talent practices to open up, energize and direct the flow of essential talent into and within the organization.

This article first appeared on BRINK on October 22, 2015.

ARE ASIAN SMEs PREPARED FOR GROWING CYBER THREAT?

Wolfram Hedrich
Executive Director of the Asia Pacific Risk Center and Partner in the Finance and Risk practice at Oliver Wyman

Jaclyn Yeo
Senior Research Analyst at the Asia Pacific Risk Center

A recent cybersecurity investigation conducted by Singapore-based Interpol Global Complex for Innovation revealed significant cyber threats across the Association of Southeast Asian Nations (ASEAN) – approximately 9,000 servers across the region were laden with malware, which compromised several websites and government portals.

A more significant cyber event took place in February, when the Singapore Ministry of Defence reported a security breach resulting in the theft of the staff's personal data.

ASIA ALMOST TWICE AS LIKELY TO BE TARGETED BY CYBER ATTACKERS

The revelation by Interpol is one of the many investigations that confirms the growing cyber threat in the region. Asia-Pacific (APAC) is becoming a prime target for cybercrime due to its higher threat potential and weaker cyber risk mitigation efforts, as detailed in the recent cyber risk report published by the Asia Pacific Risk Center.

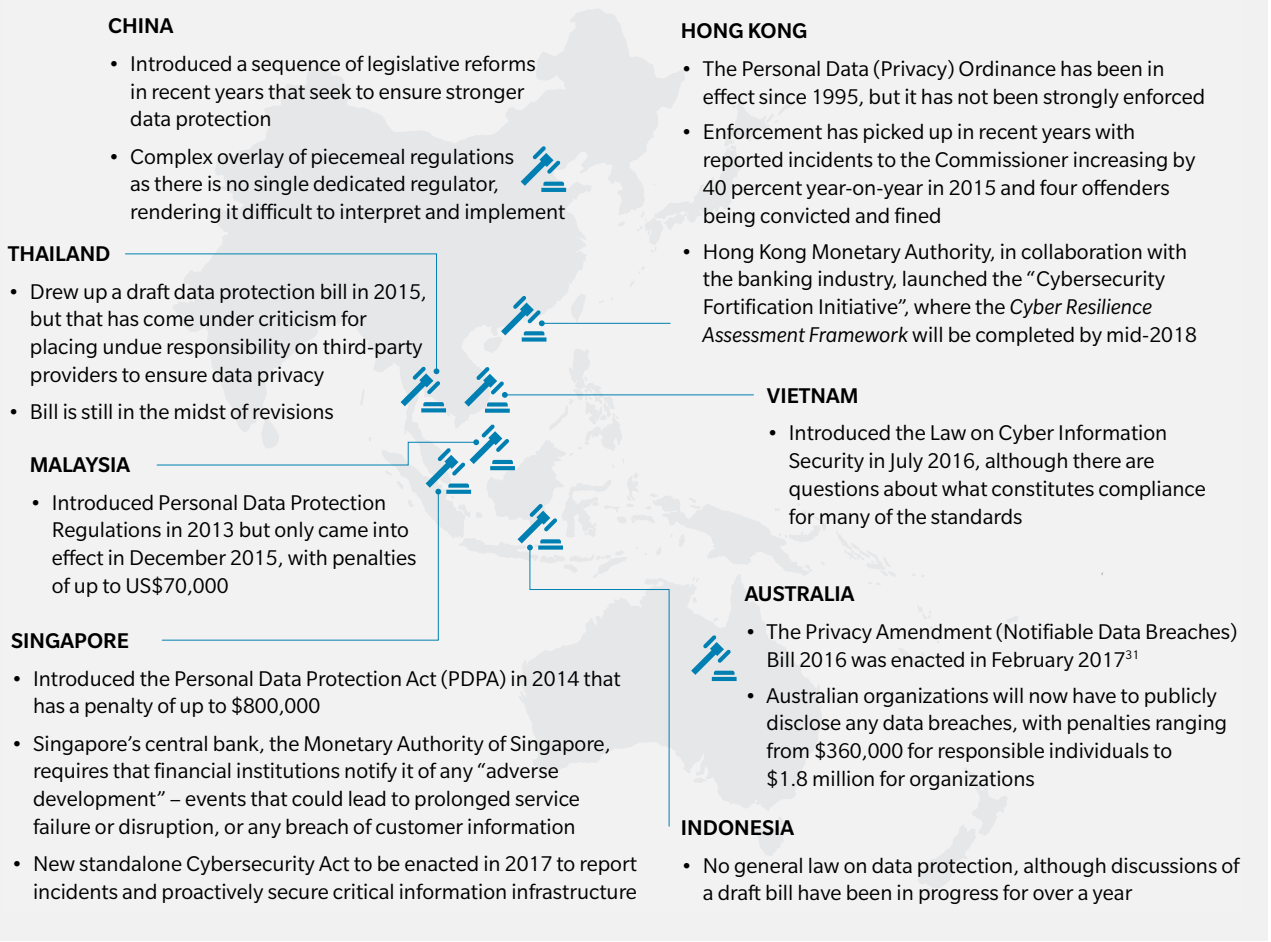
The speed of digital transformation has evolved, enabling cyber attacks to become more sophisticated and increase in frequency, with attackers becoming bolder with every successful attempt on relatively easy targets.

The worrying cyber-risk trend in recent years has caught the attention of several APAC lawmakers; Singapore, Malaysia, China and Australia have either introduced or updated their data privacy laws to ensure better management, security and control of data (Exhibit 15).

In Singapore, apart from updating the existing Computer Misuse and Cybersecurity Act in March 2017, a new stand-alone Cybersecurity Act will be introduced later this year that will mandate Critical Information Infrastructure (CII) facilities to report any cybersecurity breach and incidents.

The bill is currently in discussion and debate in the Parliament; it remains uncertain whether the legislation will ultimately cover sectors beyond CII.

EXHIBIT 15 RECENT DEVELOPMENTS IN THE APAC REGION IN TERMS OF DATA PRIVACY AND BREACH DISCLOSURE REGULATIONS
Source: Asia-Pacific Risk Center, "Cyber Risk in Asia-Pacific: The Case for Greater Transparency"



However, what is clear is the recognition by authorities and governments of the growing cyber risk in the region and the proactive steps already taken in the region's battle against cybercrime.

CYBERSECURITY A GROWING RISK CONCERN FOR SMEs

While cyber is a growing risk for large companies, it may be a relatively more elevated risk concern for small- or medium-sized enterprises (SMEs), which may be less resilient than their larger counterparts. Less sophisticated systems and technology, a lack of internal cybersecurity resources, potentially relying on less-than-cutting-edge outsourcing partners, and greater dependence on a smaller number of customers all highlight the heightened risk and overall resilience requirements for SMEs to better protect themselves and recover quickly in the event of a cybersecurity breach.

According to a recent survey, cybersecurity is one of the biggest concerns to Singapore-based SMEs. While 25 percent of respondents have either experienced an attempted or actual data breach or cyber attack in 2016, a fifth of the respondents were uncertain about whether they had experienced any compromise (Exhibit 16).

Despite the rising vulnerability to cybersecurity breaches, a lack of awareness and high investment costs remain the two immense challenges faced by SMEs. Cybercrime poses a greater threat to SMEs, since they have significantly fewer resources as a buffer, unlike larger organizations.

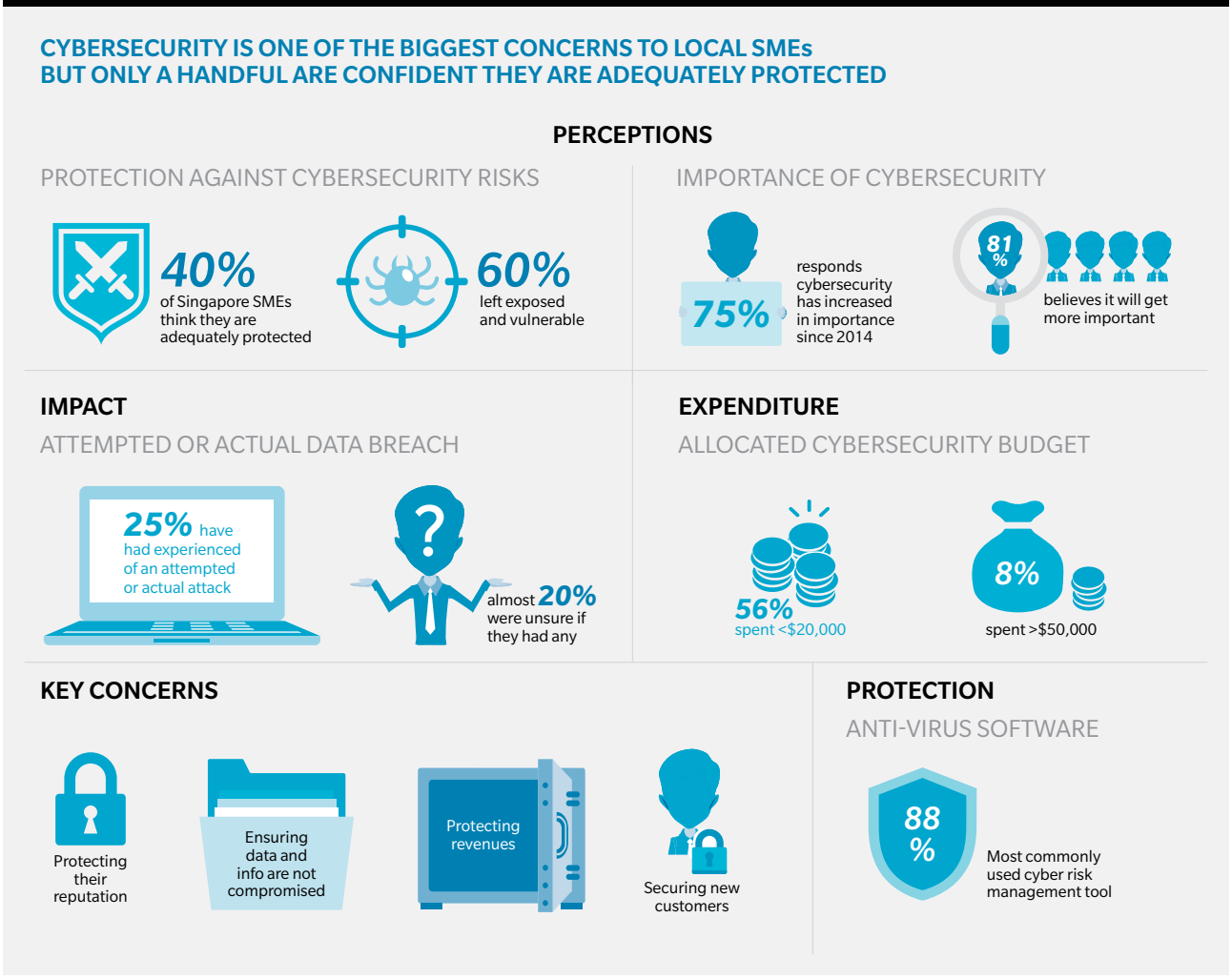
HOW CAN SMEs ADDRESS CYBER THREATS?

To address cybersecurity concerns, SMEs will first have to understand the types of cyber threats confronting them. They can start by making use of available resources and support platforms provided by the government, such as the Employee Cybersecurity Kit and the Cyber Security Awareness Alliance, which were both launched in 2015 to help local businesses enhance awareness and adopt essential cybersecurity practices.

In fact, identifying potential cyber threats is the crucial first step that businesses should undertake, and it is part of integrating cybersecurity into the enterprise-wide risk management plans.

Finally, besides putting in place the appropriate cyber risk management processes, SMEs must also consider the extent of risk transfer cover they need in response to a cyber attack since cyber risk cannot be fully eliminated and the question will often remain: when and not *if*.

EXHIBIT 16 INSIGHTS FROM THE BEAZLEY-SBF (SINGAPORE BUSINESS FEDERATION) SURVEY ON THE PERCEPTION OF CYBER SECURITY RISK BASED UPON 76 SINGAPORE-BASED SMEs
Source: Asia-Pacific Risk Center adaptation of the Beazley-SBF survey results



CONSIDER RISK TRANSFER VIA INSURANCE COVERAGE

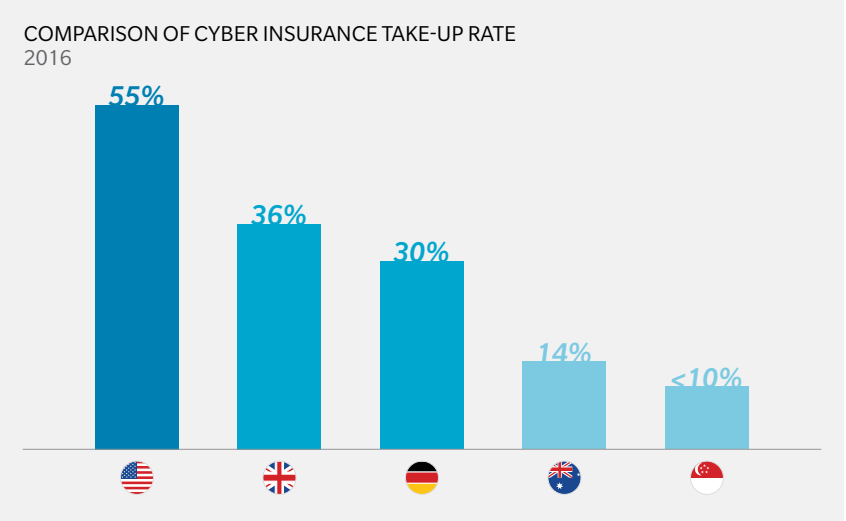
SMEs may be overwhelmed by the accelerated pace of technological change, the extent of investment needed to protect against increasingly sophisticated attacks, and ensuring comprehensive cyber-risk management strategies are implemented.

As such, insurance is being seen as a complementary and valuable risk-management tool for SMEs, with some Asia-based insurers (such as AIG and Beazley) developing tailored products for the SME segment. Cyber insurance premiums and coverage will vary, dependent on industry, risk profile and risk controls.

Nonetheless, cyber insurance adoption among Singapore SMEs generally remains below 10 percent, with less than 5 percent of manufacturing companies holding such policies, compared to 35 percent or more companies in the financial services, technology, and telecommunications sectors. Similar to Singapore, only 14 percent of Australian small businesses held cyber insurance policies in 2016, although 19 percent surveyed are looking to purchase cyber insurance in 2017.

These statistics are a far cry from the cyber insurance market in Western economies such as the US, the UK and Germany (Exhibit 17).

EXHIBIT 17 COMPARISON OF SELECTED COUNTRIES' CYBER INSURANCE TAKE-UP RATES
Source: Asia-Pacific Risk Center analysis of data from Security Brief AU 2016, Hiscox 2017, and Marsh 2017



MOVING AHEAD WITH RESILIENCE

There's no doubt that insurance plays a key role in cyber risk management. However, SMEs as well as large corporations need to be cognizant that a cyber insurance policy is just one of the many strategic response tools that form a holistic cybersecurity management framework.

In the fight against cybercrime, the government is more than just a regulator – it holds the authority to create and shape a more conducive environment to mitigate cyber risks. In the APAC region, we have seen most governments step-up efforts to put in place law enforcement on cybersecurity.

Business leaders will also need to find the right balance between cybersecurity investments and securing the appropriate insurance plans suitable to the unique needs of their industry or organization amidst changing cyber legislations and a changing risk landscape.

This article first appeared on BRINK on May 4, 2017.

ASIA IN FOCUS

CHALLENGES AROUND THE CYBERSECURITY REGULATORY ENVIRONMENT IN SOUTHEAST ASIA

Simon Piff
Vice President of IDC Asia/Pacific's IT Security Practice Business

Barely a day goes past that the international press does not carry a story of a massive data breach – whether it is about a billion records taken from a tech company, a health insurer's 80 million records, or a bank's small but significant 9,000. And yet, rarely do we hear of breaches from Asian organizations.

Could it be that the information technology (IT) security of Asian organizations is ahead of those of our Western counterparts, or, as many in the region think, that Asian organizations are either below or do not figure on the radar of the cybercriminals who steal this information?

Sadly, this is far from the truth.

In 2015 and 2016, the International Data Corporation (IDC) undertook a study of the maturity of the IT security of organizations in the US and across the Asia-Pacific region, and the comparison provides deep cause for concern. The evidence indicates that very few organizations in Asia embrace anywhere near the level of sophistication or general awareness, and have not invested in the technologies that secure their organizations to the degree their Western counterparts have.

A recent report pointed out that the global average number of days taken to discover malware inside an organization is 146 days, but in Asia-Pacific the number jumps to over 500. This means that many Asian organizations have malware sitting within their network environments, for well over a year. Traditional burglars could retire if they could wander around their target environments, unnoticed, for that long.

So why do we not hear of breaches in Asia? We could assume they are not happening, but that would be naïve. In reality, the lack of notification is due, almost entirely, to a lack of breach notification legislation. Aside from a few countries in the region, breach notification legislation is non-existent, and as such, even if an organization knows of a data breach (and the above statistics would imply that this is unlikely), there is no motivation to

go public with such news. And why would any organization want to in the first place? There is no benefit to telling the world at large that you are unable to secure your IT security systems... or is there.

ORGANIZATIONAL CHALLENGES

Although personal data privacy laws are on the books in numerous countries, for the most part the legislation covers the use of such data in terms of marketing outreach. Organizations cannot, without the individual's express permission, re-use or sell the data they have collected for any other purpose than that which it was originally collected for. This makes for a challenge to IT managers, who focus on the issue or storing a wealth of data.

Business users have a different understanding of the regulations for using this data, but are unlikely to know how or where it is being stored within IT systems. So, the promise of big data – the ability to mine the data we own and can obtain to gain critical insights to accelerate business growth (or whatever the premise is) – becomes a regulatory challenge for many, if indeed they understand the legislation and also accept that the cost of contravening such personal privacy legislation is too much of a business risk to take.

But this is not always the case. Some countries do have strong legislation around the protection of personal data, but they don't have a way to enforce this legislation, making it ineffective at best or totally ignored at worst. And as it has been mentioned, even if such personal identifiable information is misused, leaked, lost or stolen, there is no motivation to inform anyone, leaving the individual to blow the whistle on any misuse or data loss they become aware of.

WILL STRONGER REGULATION MAKE A DIFFERENCE?

On the horizon is a piece of legislation coming out of Europe that will have an impact on a sub-segment of companies in these under-legislated markets, including in Asia. The General Data Protection Regulation (GDPR) coming from the EU will potentially apply a huge fine to anyone losing data on a European citizen or resident. The criteria an organization needs to consider here is whether they own any such data and have an operation in Europe. If the answer is "yes" then an organization will fall under this legislation, regardless of where the data is lost (so organizations need to look closely at their developing country operations).

Hackers, too, are aware that legislation is missing for the most part, and they are leveraging such laws as the EU GDPR to hold data to ransom. An emerging crime is that of data theft from organizations – cybercriminals steal data that can be clearly attributed to the organization and threaten to post the data to a public site and "name and shame" the business unless a ransom is paid.

TO TELL OR NOT TO TELL

So, to the question of "why tell the world about your data loss?" The issue is that hackers get away with far more if their "modus operandi" is unknown. If a perfect theft is one where nobody realizes anything is stolen, then data theft is likely at the top of that list, since the victim still retains a copy of the data and potentially has no knowledge of the theft. But, if the details of how such crimes are committed get shared with the broader community, then the chances of evading the next hack are much greater.

If details of cybercrime are shared more broadly, the chances of evading future hacks are much greater.

This, perhaps, is where government legislation should focus itself. Issuing a punitive fine because a better-funded, better-organized criminal with access to more financing and computer resources than the average CIO is able to steal data is perhaps not the best approach to take. Encouraging organizations to share details of any data breach or hack into their environment, perhaps even offering some form of amnesty program, will provide countries with far better knowledge that can be used to better protect their IT infrastructure in the future.

Whether or not a newspaper headline is required is very much a cultural question. The concept of "face" carries far more value in Asia than elsewhere, and so perhaps we will never see these headlines... but the data loss and hacks will continue regardless.

This article first appeared on BRINK on March 30, 2017.

ASIA IN FOCUS

BANKING THE UNBANKED IN SOUTHEAST ASIA: HOW CAN DIGITAL FINANCE HELP?

Duncan Woods
Partner in the Retail & Business Banking Practice, Asia Pacific at Oliver Wyman

Ritwik Ghosh
Principal, Retail and Business Banking Practice, Asia Pacific at Oliver Wyman

Worldwide bank account ownership rocketed by 700 million between 2011 and 2014, and as of 2014, 62 percent of adults globally reported having a bank account with a formal financial institution. This represents significant success in extending access to formal financial services. However, promoting the use of formal financial services continues to be a challenge across developing economies (including a number of ASEAN markets), and the depth of engagement varies with different financial products.

For example, a recent study of four Southeast Asian markets shows that only 18 percent of adults use a bank account to receive wages or pay utility bills, and only 11 percent borrow from formal sources.

The study, which is focused on financial inclusion, finds that digital financial solutions can play a significant role in closing these gaps in financial inclusion by promoting regular use of various financial services products. Digital applications can address 40 percent of the volume of unmet demand for payment services and 20 percent of unmet credit needs in the "Base of Pyramid" and the micro, small, and medium enterprise (MSMEs) segments, according to the study, which assesses the impact of digital finance in Cambodia, Indonesia, Myanmar and the Philippines.

BANKING ON TECHNOLOGY

The effect of leveraging digital technology to bank the unbanked could boost GDP by 2-3 percent in markets such as Indonesia and the Philippines, and by 6 percent in Cambodia.

Making the most of this opportunity could shape the future growth trajectory of the financial services industry, particularly in smaller markets such as Cambodia and Myanmar, where only a small percentage of the current needs for financial services are met by formal providers.

Digital financial solutions will have the most significant impact on financial inclusion in five key areas:

1. They can enable fast, low-cost and convenient customer identification and verification processes – especially when powered by unique national identification numbers, a real-time verification infrastructure and supporting regulatory frameworks such as tiered know-your-customer (KYC) schemes.

2. They can meaningfully alter the economics of the supply side by addressing last-mile distribution and servicing issues through low-cost, widespread, digitally enabled points of physical access such as mobile phones and point-of-sale devices.

3. They can become prevalent throughout the payments value chain and ecosystem. Digital government-to-person payments – such as employee payments (wages and pensions) and social transfers – and remittance flows can create the initial momentum for electronic payments, thereby supporting the development of viable supply-side business cases. These can be sustained and further developed through person-to-all payment systems (which include all payments made by individuals, including to businesses or the government), combined with interoperable networks and open application programming interface platforms.

4. They can significantly enhance access to credit by using alternative sources of data, such as payment transactions and telecoms data, as well as analytics. These improve customer profiling, credit risk assessment and fraud detection.

5. Savings can be mobilized digitally through alternative, lower-cost origination and distribution channels and more-convenient product designs, such as mobile wallets connected to savings accounts and intuitive goal-based savings products. An easy KYC and on-boarding process can also contribute to savings.

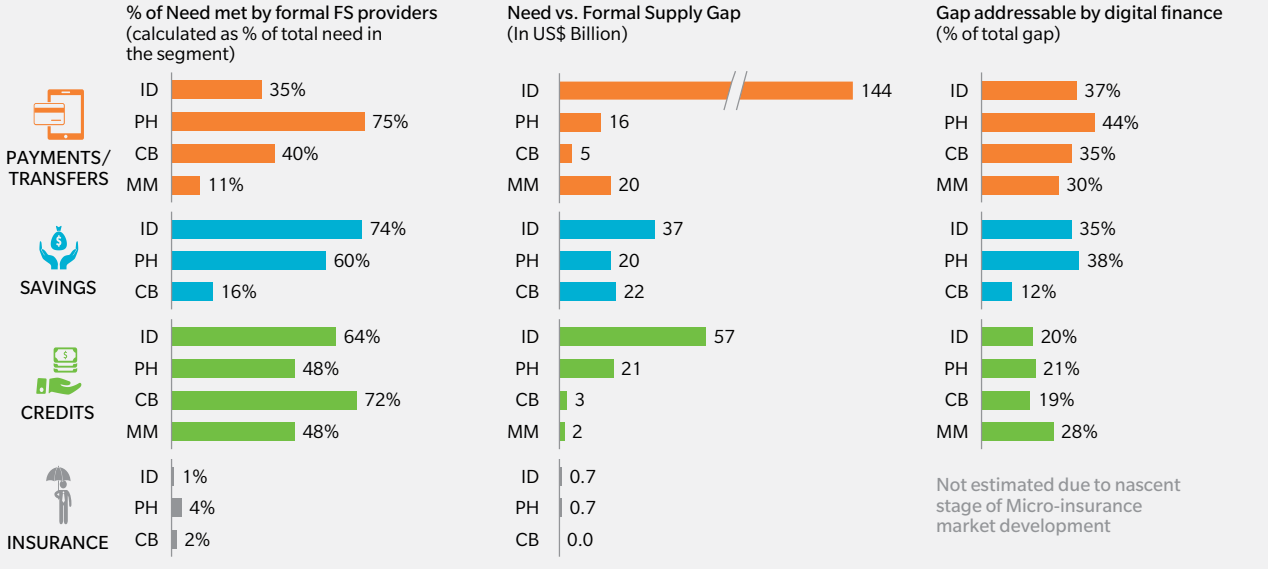
Exhibit 18 provides an assessment of the financial inclusion gap across four focus markets and the potential impact of digital finance across different need categories.

THE NEED FOR REGULATORY SUPPORT

Since much of the digital enablement will be driven by the supply side, regulatory and public policy actions will play a significant role in creating a favorable environment. There is a need for action in the following three areas.

Supply-side entry barriers. Create a level playing field by allowing collaboration and competition between traditional financial

EXHIBIT 18 GAP BETWEEN DEMAND AND FORMAL SUPPLY, AND IMPACT OF DIGITAL APPLICATIONS
Note: We were not able to reliably estimate formal savings and insurance supply in Myanmar that targets financial inclusion sub-segments
Source: Oliver Wyman analysis



services players and new types of supply-side participants such as mobile network operators.

Suitable solution design and delivery. Develop a "safe space" for businesses to test new ideas in a live environment with more permissive regulations that provide clear guidance on the development and role of agent networks, and allows different supply-side operators to use these alternative channels; and promote low cost and more convenient payment channels and network infrastructure, for example, by advocating and mandating transfer of money between mobile money platforms.

Shared vision. Produce a unified roadmap for financial inclusion to focus the efforts of various stakeholders; and put in place a governance mechanism to facilitate coordination and ensure accountability for action in all relevant government departments.

A DIGITAL FUTURE?

When all of these elements fall in place in a mutually reinforcing manner, rapid change in the level of financial access and usage can be achieved. The graphic below illustrates how such a digitally enabled solution can take shape in customer identification and verification. The user possesses a universal unique ID that is verifiable with biometric information stored in a public utility database. This is accessed in real time by various service providers via different channels, ranging from agents to fully digital customer-initiated requests.

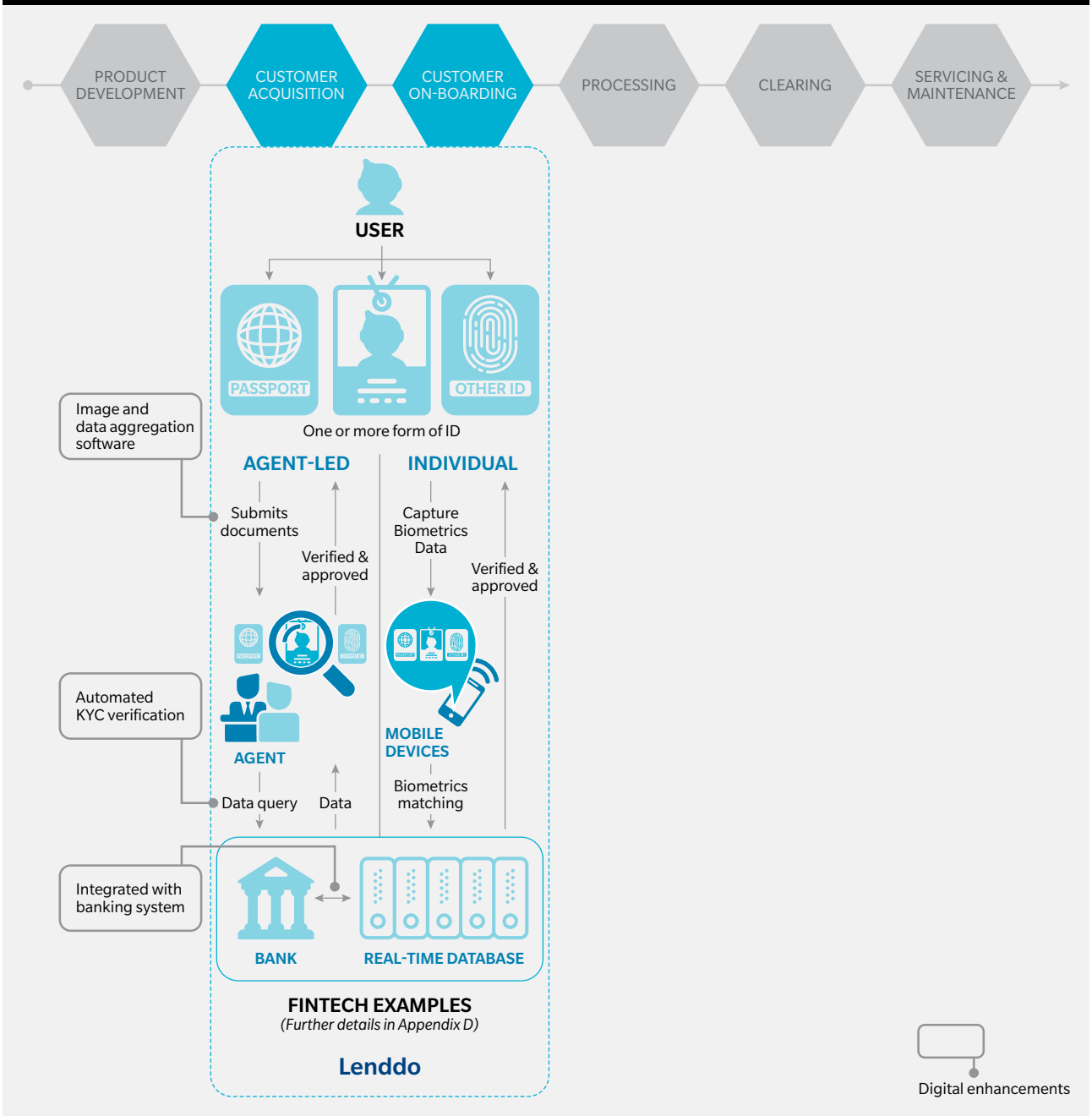
The end result is the ability to extend access to the unbanked/under-banked population by significantly reducing the cost of KYC, customer due diligence and on-boarding processes.

This is not a pipe dream of a digital future. India is a case in point where much of this is now being realized on the back of a universal national ID project (called Aadhaar). Indonesia's national ID program (e-KTP) is also being developed to enable a similar end-state solution.

The opportunity to accelerate financial inclusion through digital finance is clear, and the impact would be significant on both the lives of financially excluded people and the broader economy. Regulators and policymakers have critical roles to play in supporting and enabling this digital innovation.

This article first appeared on BRINK on February 3, 2017.

EXHIBIT 19 MAPPING DIGITAL KYC ENHANCEMENTS TO PRODUCT VALUE CHAINS CAPTURE
Source: Oliver Wyman analysis



ASIA IN FOCUS

HERE'S HOW ASIA'S CITIES CAN BE SMART AND SUSTAINABLE

Todd Ashton
President of Ericsson Malaysia and Sri Lanka

A quick online search of the world's top 10 most populous cities will reveal that more than half are in Asia. If you were to walk down the busy streets of Jakarta, Tokyo, Manila or Seoul, you might think that everyone has moved to the city – and you wouldn't be far from the truth.

We are undergoing a major rural-to-urban demographic shift. There are already more people living in cities than in rural areas, and the United Nations estimates that by 2050, almost 70 percent of the world's population will be city dwellers.

With so many people moving to cities, the way these cities are structured will impact the lives of billions of people.

In some respects, this elevates cities above nation states as significant incubators of innovation, enterprise and social progress. At the same time, the required pace of change – especially now where we face global economic, environmental and social uncertainty – creates a raft of challenges to sustainable development.

CONNECTING THE CITY

It's crucial that cities adopt smart, sustainable development practices. Harnessing the potential of information and communication technology (ICT) will enable cities to thrive without their development taking a major toll on already-scarce resources. ICT allows people, knowledge and devices to be networked in new ways, and cities that embrace ICT's potential can create new value, operate efficiently and benefit from significant return on investments. All this adds up to more livable, more attractive and ultimately more competitive cities, as well as the potential for people to pursue a more sustainable urban future.

The significance of cities is well recognized in the UN Sustainable Development Goal 11 about sustainable cities and communities. If we go back to considering the most populous cities in Asia, each city faces many complex problems that require different types of action – but we see that a common enabler across the board is ICT.

A paper published in 2015 by the Earth Institute at Columbia University and Ericsson states that ICT can accelerate the achievement of these Sustainable Development Goals. Higher ICT maturity levels for cities are associated with more opportunities to transform lifestyles and economic prospects.

For ASEAN countries, broadband, based on a combination of both fixed and wireless technologies, can help significantly accelerate sustainable growth in cities. Therefore, there should be a national agenda when it comes to broadband and concerted efforts to improve the business case for these investments. By releasing more spectrum with sustainable economics to the key players in the market, governments will be able to better enable broadband investment from private industry. Education in terms of digital literacy and new technologies is also needed. This combination of infrastructure and capability will help create smart cities.

CAN SMART CITIES ALSO BE SUSTAINABLE?

So, what of sustainability? ICT projects alone won't necessarily make cities more sustainable.

Our experience has shown that to successfully transform into a smart, sustainable city, five critical considerations are necessary:

- Defining an agreed-upon vision, strategy and targets
- Creating informed networked governance structures
- Developing organizational capacity
- Engaging with all relevant stakeholders
- Forging and fostering long-term partnerships

Partnership, planning and engagement can make all the difference between a city that owns and controls its transformation and one that is a victim of fragmented, unsustainable change.

Forming strong partnerships with ICT companies and non-governmental organizations (NGOs) with a global presence and high levels of expertise, particularly in systems integration, can allow cities to accelerate their transformation journey.

Early last year, we announced our partnership with Arup, an independent firm of planners, designers, engineers, consultants and technical specialists working across the built environment to transform a pilot district in Hong Kong into a smart and sustainable neighborhood. The feasibility study focuses on transforming the 488-hectare Kowloon East into an additional Central Business District of Hong Kong, which will further support economic growth and strengthen global competitiveness.

Investment in information and communication technology will make cities smarter and more sustainable.

The scope of the study spans a wide range of subjects that include formulating a smart city framework, an implementation strategy and a business model that later can be expanded to cover the rest of Hong Kong. It will also advise on centralized digital infrastructure and cybersecurity to support the Internet of Things (IoT) and big data applications.

While Hong Kong's ICT maturity more easily enables ICT-based transformations with social, economic and environmental benefits, ICT-based solutions can be created to match cities' levels of development, as long as the right partnerships are in place.

The use of IoT technology to enhance bike-sharing in China is another example of how technology is transforming cities. Our partnership with China Mobile Shanghai and Mobike, the popular bike-sharing service, gave us the opportunity to trial the latest cellular IoT technologies on a live network.

The trial provided a more convenient and enhanced bike-sharing experience to Mobike users using new cellular IoT technologies, allowing users to locate bikes more accurately and extending service to areas that traditional coverage could not reach, such as basement parking spaces. In a country like China, where cities are more densely populated compared to other cities in Asia, the convenience of bike-sharing – powered by mobile and IoT technology – will help not only to decongest roads, but will also help to address challenges from the pollution that heavy road traffic brings.

These are just two examples of how ICT can help transform cities into becoming smarter and more sustainable, but the possibilities are endless with public and private sector collaboration, broadband infrastructure and the right investment in capability.

This article first appeared on the World Economic Forum Agenda and BRINK on May 29, 2017.

ASIA IN FOCUS

ELECTRIFYING EMERGING ASEAN THROUGH OFF-GRID DISTRIBUTED RENEWABLE ENERGY SYSTEMS

Han Phoumin
Energy Economist at the Economic Research Institute for ASEAN and East Asia

Some 134 million people in the Association of Southeast Asian Nations (ASEAN) region do not have access to electricity. At the end of 2015, the ASEAN community declared that lack of power and energy access could threaten the region's economic growth and its economic transition.

Many industrial and commercial economic zones, and remote areas in ASEAN's emerging countries that contribute to economic growth, are sometimes faced with an unstable energy supply. This can prevent companies and households from investing and providing economic activities, such as goods and services.

Off-grid distributed energy systems (DES) using renewable energy could be a solution to this problem, thanks to the increasing availability of small power generation and renewable energy technologies.

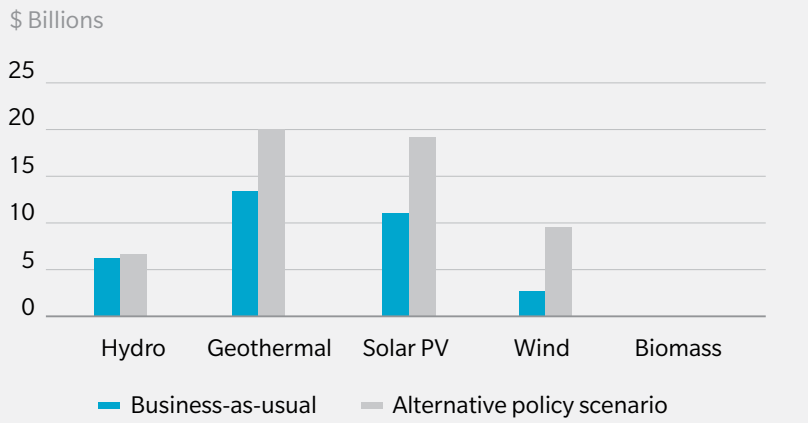
Off-grid DES-related renewable energy sources include biomass, solar, and hydro, with generating capacities ranging from a few kilowatts to as much as 50 megawatts. Such renewable energy technologies can either be integrated into local distribution grids or used as stand-alone systems in areas where the extension of transmission lines is not economically viable.

As energy supply from off-grid DES-related renewable sources has a large potential to increase in emerging ASEAN countries, the Economic Research Institute for ASEAN and East Asia has attempted to estimate the off-grid DES-related renewable energy potential using both a business-as-usual scenario and an alternative policy scenario.

A business-as-usual scenario was developed for each ASEAN country to outline the current energy policies and the expected foreseeable future of energy policies and economy-wide energy consumption, assuming no significant changes in government policies. An alternative policy scenario was set to examine the potential impacts of additional energy efficiency goals, action plans, or policies that are currently, or likely to be, under consideration.

The results show that the electricity supply from off-grid DES-related renewable sources would increase from 65,608 gigawatt-hours under the business-as-usual scenario to 91,854 gigawatt-hours in the alternative policy scenario (Exhibit 20).

EXHIBIT 20 ESTIMATES OF OFF-GRID DISTRIBUTED RENEWABLE ENERGY SYSTEM INVESTMENT OPPORTUNITIES BY 2040
Source: Han (2016)



The investment opportunity estimated for the combined use of solar, wind, biomass, hydropower, and geothermal is about $34 billion for the business-as-usual scenario and about $56 billion under the alternative policy scenario.

Among the DES-related renewable energy sources, investments in solar and geothermal power are expected to double under the alternative policy scenario compared with the business-as-usual scenario, while investment in wind energy is expected to increase more than threefold to meet the expected generation output by 2040.

POLICY OPTIONS TO PROMOTE OFF-GRID DES

From the potential increase in off-grid DES-related renewable energy sources in ASEAN, it is also estimated that the CO_2-emissions reduction in the ASEAN region as a result of the application of off-grid DES-related solar, wind, biomass, geothermal, and hydropower would be about 46.1 million metric tons in the business-as-usual scenario and 64.6 million metric tons under the alternative policy scenario.

But to realize the potential of off-grid DES-related renewable capacity and investment, an enabling policy framework that provides a long-term government commitment and credible targets will be needed. ASEAN may need to consider a wide range of policy options and instruments, although it is already targeting a 23 percent share of renewable energy in primary energy supply by 2025.

The following framework of policy options is worth considering:

- National policy design aims to provide a trajectory for the future energy mix. It includes a renewable energy target; a renewable energy law or strategy; a biomass and biofuels law or program; and a solar heating, solar power, wind, and geothermal law or program
- Fiscal incentives aim to reduce the upfront cost by introducing fiscal policy instruments, such as exemptions of value-added tax, income tax, import and export duties, and local taxes; and the introduction of a carbon tax and accelerated depreciation
- Grid access aims to give project developers confidence to invest through grid access priority and a transmission discount policy if electricity is produced from renewable energy
- Regulatory instruments aim to provide incentives for investing in renewables through the implementation of energy policies, such as feed-in tariffs, feed-in premiums, auctions, net metering, and quotas
- Finance aims to reduce risk for investors through the implementation of currency hedging, dedicated funds, eligible funds, and guarantees

In conclusion, the increase in off-grid DES-related renewable energy supply in the ASEAN region will have multiple benefits for people and the environment.

Its expansion and application could promote lower-cost, more efficient energy access, and it could also address the challenging issue of electricity access for about 134 million people whose rights have been denied. Its application would also contribute to CO_2 reduction at the ASEAN level by reducing emissions by as much as nearly 65 million metric tons in the alternative policy scenario.

ASEAN will enjoy quality growth by investing more in off-grid DES-related renewable energy sources.

This article first appeared on Asia Pathways, the blog of the Asian Development Bank Institute and BRINK on July 3, 2017.

WHAT'S NEXT?

THE END-TO-END AUTONOMOUS SUPPLY CHAIN… IS HERE

Wolfgang Lehmacher
Head of Supply Chain and Transport Industries at World Economic Forum

From Amazon's delivery drones to self-driving cars, autonomous factory equipment to Elon Musk's vacuum tubes that will transport items at 760 miles per hour – automated vehicles are on the rise.

Even beyond the realm of private companies, automated transport has been successfully tested. Six convoys of platoons, in groups of two or three trucks – communicating wirelessly and driving closely behind one another – arrived by public road in Rotterdam in April 2016. The Ministry of Transport in Singapore and the port operator, PSA, seek proposals to develop an autonomous truck platooning system. Airbus is pursuing an autonomous air taxi project to deliver parcels to ships in the port of Singapore.

As an alternative to drones and surface transportation on roads or through tubes, experts in Switzerland have presented a plan to move goods across the country in a gigantic underground tunnel. On the waters, the cargo ships of the future are expected to be crewless and remote-controlled.

COMPLEXITY OF 'THE LAST MILE'

The so-called last mile, the delivery to the doors of businesses and consumers, is probably the most complex task in the supply chain – in particular in the diverse urban universe of cars, bicycles and children playing on the streets. As an alternative to drones, the start-up, Dispatch, has developed an autonomous last-mile solution that can move a total of 100 pounds. In order to learn to move safely alongside other vehicles and citizens, the robot is equipped with sensors and artificial intelligence technology.

In Paris, two entrepreneurs are building a river shuttle that will essentially fly above the Seine to avoid congestion on the busy streets. Another startup, Parcelhome, has developed intelligent lockers and boxes to complete the autonomous supply chain.

In parallel, engineers are working on building the software to coordinate thousands of autonomous units on, under and above the ground, on the rivers, lakes and oceans – to move passengers and cargo.

In summary, the autonomous end-to-end supply chain is almost complete. Raw materials extracted in automated mines reach the smart industry 4.0 and from there are transported by truck platoons or long-distance drones to purchasers, or the automated distribution centers of wholesalers, retailers or e-commerce warehouses. Drones, robots, or urban tubes deliver the products directly into homes or smart boxes – or via self-driving cars, sent to pick up goods from local sorting centers.

A SAFER, MORE EFFICIENT SUPPLY CHAIN ... AND ITS CHALLENGES

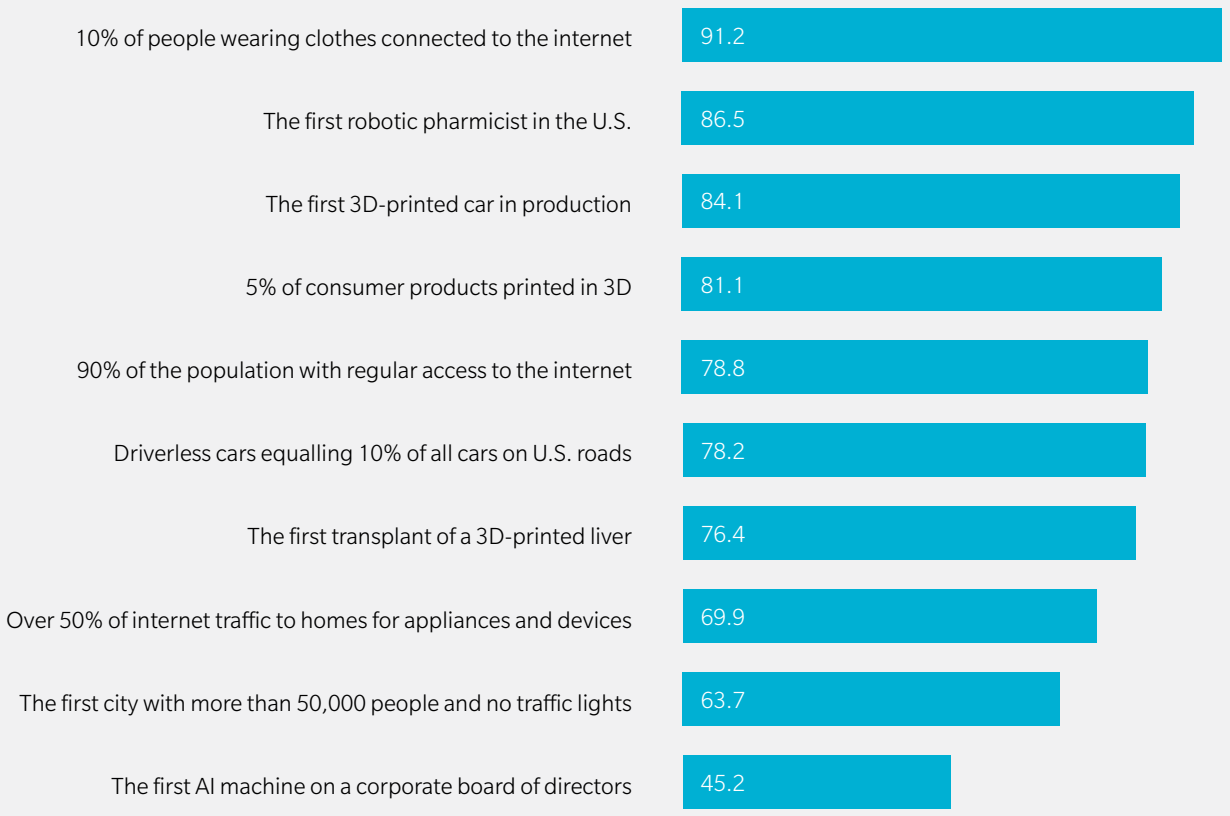
The autonomous supply chain will create enormous opportunities to make the flow of goods safer, more efficient and environmentally friendly: self-driving cars alone would reduce accidents by 70 percent, improve fuel-efficiency by 20 percent, and save about 1.2 billion hours of pure driving time over a period of ten years.

Less congestion will make the flow of goods and people faster – and those countries with driver shortages, such as the US, the UK and Germany will find relief.

These improvements do not come without their challenges. One key concern is cyber risk. We need to ensure that autonomous units cannot be hacked. Ethical questions must also be answered. How should we decide who a vehicle should save in the case of an accident? Policymakers need to consider where to drive

EXHIBIT 21 WHEN WILL THE FUTURE ARRIVE?
800 technology executives and experts from the information and communications technology sector were surveyed as part of our *Technology Tipping Points and Societal Impact* report

Source: World Economic Forum, Technology Tipping Points and Societal Impact report, 2015



innovation and where to slow down the autonomous economy to avoid unwanted consequences, such as job losses.

The autonomous movement, which started in the early 1950s, is now in full swing. Some 70 percent of 1,433 consumers surveyed in the US think they will order their first drone-delivered package within the next five years. Almost 90 percent of policymakers expect autonomous vehicles to gradually become reality within the next 10 years, according to a 2015 World Economic Forum study. Many of the cities interviewed consider goods delivery as one of the key applications for autonomous transportation in their city.

Some 60 percent of policymakers in the study expect a ban for private cars in a significant part of the city over the next 15 years. Will this stay limited to private vehicles? Probably not. Over time, cities will further regulate goods deliveries. One of the pain points for citizens today is daytime deliveries, which regularly come with double parking and add to the city's overall congestion. Therefore, shippers, in addition to transportation companies, need to prepare for the autonomous future.

Capturing the full potential of the automated supply chain requires rethinking and transforming the mainstream logistics systems: from the fixed "collect in the evening and deliver during the morning" approach to a fluid system of continuous movement and supply.

Platoons, drones, tunnels, tubes, rolling robots and automated warehouses will make that constant flow possible. This requires flexibility and innovation on operator level and investments in technology and infrastructure.

The realization of the autonomous supply chain requires close collaboration between manufacturers, operators, retailers, developers, policymakers and citizens.

The global self-driving vehicle study yielded hopes in respect to the environment and our health: 66 percent of the 5,500 consumers surveyed said that, to their minds, self-driving cars would be electric or hybrid. In light of all the benefits and challenges of the autonomous supply chain, creating a pilot program somewhere in the world with fully-fledged autonomous mobility of goods and people would be a major step toward cleaner, safer and more efficient cities.

This piece first appeared in The Agenda from the World Economic Forum and BRINK on March 24, 2017.

WHAT'S NEXT?

FACTORIES OF THE PAST ARE THE DATA CENTERS OF THE FUTURE

Graham Pickren
Assistant Professor of Sustainability Studies at Roosevelt University

We live in a data-driven world. From social media to smart cities to the Internet of Things, we now generate huge volumes of information about nearly every detail of life. This has revolutionized everything from business to government to the pursuit of romance.

We tend to focus our attention on what is new about the era of big data. But our digital present is in fact deeply connected to our industrial past.

In Chicago, where I teach and do research, I've been looking at the transformation of the city's industrial building stock to serve the needs of the data industry.

Buildings where workers once processed checks, baked bread and printed Sears catalogs now stream Netflix and host servers engaged in financial trading.

The buildings themselves are a kind of witness to how the US economy has changed. By observing these changes in the landscape, we get a better sense of how data exist in the physical realm. We are also struck with new questions about what the rise of an information-based economy means for the physical, social and economic development of cities. The decline of industry can actually create conditions ripe for growth – but the benefits of that growth may not reach everyone in the city.

Data is crucial to innovation, but also enables the displacement of workers through offshoring and automation.

FACTORIES OF THE 21st CENTURY

Data centers have been described as the factories of the 21st century. These facilities contain servers that store and process digital information. When we hear about data being stored "in the cloud," those data are really being stored in a data center.

But contrary to the ephemeral-sounding term "cloud," data centers are actually incredibly energy- and capital-intensive infrastructure. Servers use tremendous amounts of electricity and generate large amounts of heat, which in turn requires extensive investments in cooling systems to keep servers operating. These facilities also need to be connected to fiber-optic cables, which deliver information via beams of light. In most places, these cables – the "highway" part of the "information superhighway" – are buried along the rights of way provided by existing road and railroad networks. In other words, the pathways of the internet are shaped by previous rounds of development.

An economy based on information, just like one based on manufacturing, still requires a human-made environment. For the data industry, taking advantage of the places that have the power capacity, the building stock, the fiber optic connectivity and the proximity to both customers and other data centers is often central to their real estate strategy.

FROM ANALOG TO DIGITAL

As this real estate strategy plays out, what is particularly fascinating is the way in which infrastructure constructed to meet the needs of a different era is now being repurposed for the data sector.

In Chicago's South Loop sits the former R.R. Donnelley & Sons printing factory. At one time, it was one of the largest printers in the US, producing everything from Bibles to Sears catalogs. Now, it is the Lakeside Technology Center, one of the largest data centers in the world, and the second-largest consumer of electricity in the state of Illinois.

The eight-story Gothic-style building is well-suited to the needs of a massive data center. Its vertical shafts, formerly used to haul heavy stacks of printed material between floors, are now used to run fiber-optic cabling through the building. (Those cables come in from the railroad spur outside.) Heavy floors built to withstand the weight of printing presses are now used to support rack upon rack of server equipment. What was once the pinnacle of the analog world is now a central node in global financial networks.

Just a few miles south of Lakeside Technology Center is the former home of Schulze Baking Company in the South Side neighborhood of Washington Park. Once famous for its butternut bread, the five-story terra-cotta bakery is currently being renovated into the Midway Technology Centre, a data center. Like the South Loop printing factory, the Schulze bakery contains features useful to the data industry. The building also has heavy-load bearing floors as well as louvered windows designed to dissipate the heat from bread ovens – or, in this case, servers.

It isn't just the building itself that makes Schulze desirable, but the neighborhood as a whole. A developer working on the Schulze redevelopment project told me that, because the surrounding area had been deindustrialized, and because a large public housing project had closed down in recent decades, the nearby power substations actually had plenty of idle capacity to meet the data center's needs.

Examples of this "adaptive reuse" of industrial building stock abound. The former Chicago Sun-Times printing facility became a 320,000-square-foot data center in early 2016. A Motorola office building and former television factory in the suburbs has been bought by one of the large data center companies. Even the once mighty retailer Sears, which has one of the largest real estate portfolios in the country, has created a real estate division tasked with spinning off some of its stores into data center properties. Beyond Chicago, Amazon is in the process of turning an old biscuit factory in Ireland into a data center, and in New York, some of the world's most significant data center properties are housed in the former homes of Western Union and the Port Authority, two giants of 20th-century modernity.

What we see here in these stories is the seesaw of urban development. As certain industries and regions decline, some of the infrastructure retains its value. That provides an opportunity for future savvy investors to seize upon.

DATA CENTERS AND PUBLIC POLICY

What broader lessons can be drawn from the way our data-rich lives are transforming our physical and social landscape?

First, there is the issue of labor and employment. Data centers generate tax revenues but don't employ many people, so their relocation to places like Washington Park is unlikely to change the economic fortunes of local residents.

If the data center is the "factory of the 21st century," what will that mean for the working class?

Data centers are crucial to innovations such as machine learning, which threatens to automate many routine tasks in both high- and low-skilled jobs. By one measure, as much as 47 percent of US employment is at risk of being automated. Both low- and high-skilled jobs that are non-routine – in other words, difficult to automate – are growing in the US. Some of these jobs will be supported by data centers, freeing up workers from repetitive tasks so that they can focus on other skills.

On the flip side, employment in the manufacturing sector – which has provided so many people with a ladder into the middle class – is in decline in terms of employment. The data center embodies that economic shift, as data management enables the displacement of workers through offshoring and automation.

So buried within the question of what these facilities will mean for working people is the larger issue of the relationship between automation and the polarization of incomes. To paraphrase Joseph Schumpeter, data centers seem likely to both create and destroy.

Second, data centers present a public policy dilemma for local and state governments. Public officials around the world are eager to grease the skids of data center development.

In many locations, generous tax incentives are often used to entice new data centers. As the Associated Press reported last year, state governments across the US extended nearly $1.5 billion in tax incentives to hundreds of data center projects nationwide during the past decade.

For example, an Oregon law targeting data centers provides property tax relief on facilities, equipment, and employment for up to five years in exchange for creating one job. The costs and benefits of these kinds of subsidies have not been systematically studied.

More philosophically, as a geographer, I've been influenced by people like David Harvey and Neil Smith, who have theorized capitalist development as inherently uneven across time and space. Boom and bust, growth and decline: They are two sides of the same coin.

The implication is that the landscapes we construct to serve the needs of today are always temporary. The smells of butternut bread defined part of everyday life in Washington Park for nearly a century. Today, data is in the ascendancy, constructing landscapes suitable to its needs. But those landscapes will also be impermanent, and predicting what comes next is difficult. Whatever the future holds for cities, we can be sure that what comes next will be a reflection of what came before it.

This piece first appeared on *The Conversation and BRINK on February 6, 2017.*

WHAT'S NEXT?

HOW DATA AND TECH WILL FUEL MEGACITIES OF THE FUTURE

Terry D. Bennett
Senior Industry Strategist for Civil Infrastructure at Autodesk

What will cities look like by the year 2050? Will they be like those in South Korea, centered on a digitally connected retrofit of existing society? Will they parallel the shiny new cities of Dubai or Singapore? Or could they possibly move underground or under the oceans?

Today, innovative cities, such as Curitiba, Brazil, are rethinking entire mass-transportation strategies while debating visions of autonomous cars and drones. The most basic infrastructure needs have always been about how people want to live and move around.

It's also about how things move around. FedEx sees e-commerce increasing by 26 percent from 2016 to $2.4 trillion worldwide by 2018, which adds pressure to upgrade roads, highways, and port/airport infrastructure for vehicle use – autonomous or otherwise.

Add to this mix myriad technology disruptions, such as sensors, big data, and the Internet of Things (IoT), which can help adjacent cities work together like cogs in a bigger machine.

But why is that important? Planners have been considering urbanization pressures, often in areas with little room to increase building or infrastructure capacity. One alternative is analyzing collected data to determine how to densify corridors of population between neighboring cities, with mass transit creating megaregions that could easily become home to millions more.

Big Data collected through the Internet of Things will play a key role in growing the megacities of 2050.

The challenge for cities around the world is: How do they grow? How do they perform and transform simultaneously?

DATA AND THE MEGACITIES OF THE FUTURE

Neighboring cities are coalescing in their shared infrastructure and mutual impact of their economies. Power lines, roads, transit, water systems, and safety don't stop at city limits, and municipalities are facing transformation at unprecedented rates. As a result, there's a lot of debate about who decides the way forward and what that looks like.

When it comes to designing infrastructure, one thing is for sure: Big data collected through the IoT will play a key role in growing the megacities of 2050. "Big Data is all the information around us that is being collected in various streams," says Steph Stoppenhagen, smart cities business development director for Black & Veatch. "If you use a metrocard to get on a subway, then the system knows when you entered, where you went, and the route you took. How is this helpful? By recognizing if the subway service worked. Was it successful? If so, you will do it again and again. That is one example of using data to watch people's movements – creating smarter mobility."

Not all data easily translates into useful or actionable information, though. To address the changing urban landscape, information itself should be seen as a form of infrastructure – one that can be used for better planning to connect cities within a bigger system.

The starting point is people, not technology. Planning, design, and investment decisions – along with supportive policymaking – can be informed and expedited via infrastructure visualization, simulation, and analysis. The rise of big data and advanced modeling technology make it possible to plan and prioritize infrastructure investment with greater foresight, better communicate potential outcomes, and yield measurably better results.

Creating smart cities means more than using the IoT to optimize services or communicate information to residents. It should be a construct used to frame local government decision-making around city transformation. While 2050 seems far off, for existing cities that must perform, transform, and compete with brand-new cities, it's pretty close at hand. Cities need to evolve to develop sustainably; improve resilience; meet citizens' rising expectations; and attract investment, new businesses, and talent. The good news is that data and technology will make work and life better by creating a well-connected community.

But smart investment and policy decisions are crucial to planning, and moving to long-term investment (versus grant funding) is key. To achieve that, cities must connect:

- Projects: Developments that build toward the unified city vision and meet broader economic objectives, such as accessibility, jobs, affordable housing, and healthy environments
- Teams: Collaborative efforts functioning across all levels of government to unlock public and private infrastructure investment, leveraging big data to track the performance of infrastructure
- Insights: New technologies that revolutionize how cities are planned, function, and grow the economy by connecting everyone at the beginning of project planning
- Outcomes: Projects that meet planning/business-case measures and use cost-benefit analyses to meet economic objectives

THE FUTURE OF PLANNING IS 3-D

Building Information Modeling (BIM) gives meaning to the vast information available to architects and engineers, urban citizens, and decision-makers. Advanced 3-D modeling allows people to analyze complex information, including risks and problems at a system-versus-asset level. What that means is thinking about what the whole infrastructure system is trying to accomplish versus goals of its individual components. That information helps architects and engineers enhance designs so individuals, firms, and cities can meet their "smart" connected goals, bringing neighboring cities together.

Consistent use of 3-D in-context models coupled with simulation software can create a hypothetical but realistic scenario of the physical infrastructure's performance. It establishes a concrete vision in 3-D, setting the context for discussing goals and performance measures that everyone can understand.

Technology lets people see with both eyes open – gaining perspective and depth – rather than with one eye closed, which gives perspective but no depth. The depth comes from information streaming through technology: Information-rich models can help stretch infrastructure investment dollars throughout the design and construction phases.

Going forward, using 2-D designs in an ever-changing 3-D world won't work. Using 3-D BIM processes will be a critical skill set to build the right infrastructure for a megacities-of-the-future vision.

CREATING SMART FOUNDATIONS TOGETHER

Cities are often overwhelmed by big data and lack the ability to make the information actionable. A benefit of BIM is that it can manage connections among all the data useful for complex city design projects – from the micro to macro level.

Through an immersive collaboration, the general public will better understand the future of infrastructure design. This way of stepping into, around, and through infrastructure virtually is becoming the norm. It aids in faster design-concept creation, vetting, and approval, and it reduces stakeholder pushback.

In this era of connected BIM – where information forms the infrastructure for planning, designing, and maintaining manufactured and natural systems – the objective is to create integrated and resilient infrastructure. Then, cities will be able to withstand and recover more quickly from natural and human-caused disasters – and grow to support their future.

By collecting and analyzing more information, civil engineers will better predict what's needed to manage bridges, roads, and other infrastructure assets, prolonging their lifecycles. As populations increase and demand for infrastructure rises, future-proofing assets must take into account true lifecycle costs.

Smart infrastructure connections at a personal, community, metropolitan, or even national level – underpinned by technology – provide the capability for monitoring and measuring data. Then the analysis of data feedback can yield positive steps to address issues (whether through human or machine actions).

This changes the vision of cities and provides the foundation for more holistic planning. In the connected cities of 2050, all kinds of infrastructure – energy, water, transportation, buildings, and governance – will "talk" to each other to prioritize needs, optimize performance, minimize energy use, and make life more enjoyable and productive for the people who live in and travel between cities.

This article originally appeared on Autodesk's Redshift, a site dedicated to inspiring designers, engineers, builders and makers, and BRINK on May 3, 2017.

2050 seems far off, but data and technology will soon make work and life better through a well-connected community.

About Marsh & McLennan Companies

MARSH & McLENNAN COMPANIES (NYSE: MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy and people. Marsh is a leader in insurance broking and risk management; Guy Carpenter is a leader in providing risk and reinsurance intermediary services; Mercer is a leader in talent, health, retirement and investment consulting; and Oliver Wyman is a leader in management consulting. With annual revenue of more than $13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies provides analysis, advice and transactional capabilities to clients in more than 130 countries. The Company is committed to being a responsible corporate citizen and making a positive impact in the communities in which it operates. Visit www.mmc.com for more information and follow us on LinkedIn and Twitter @MMC_Global.

About Asia Pacific Risk Center

Marsh & McLennan Companies' Asia Pacific Risk Center addresses the major threats facing industries, governments, and societies in the Asia Pacific Region and serves as the regional hub for our Global Risk Center. Our research staff in Singapore draws on the resources of Marsh, Guy Carpenter, Mercer, Oliver Wyman, and leading independent research partners around the world. We gather leaders from different sectors around critical challenges to stimulate new thinking and solutions vital to Asian markets. Our digital news service, BRINK Asia, keeps decision makers current on developing risk issues in the region.

Economy • Environment • Geopolitics •
Society • Technology

BRINK Asia gathers timely perspectives from experts on risk and resilience to inform business and policy decisions on critical challenges in the region. It is the online news service of Marsh & McLennan Companies' Asia Pacific Risk Center, managed by Atlantic Media Strategies, the digital consultancy of The Atlantic.

contact@brinkasia.com
www.brinknews.com/asia
Follow BRINK Asia on Twitter
Follow BRINK Asia on Linkedin

www.mmc.com