

# *Financial Services Technology 2020 and Beyond: Embracing disruption*



*To succeed in this rapidly changing landscape, IT executives will need to agree with the rest of the management team on the posture they wish to adopt. Will they try to be industry leaders, fast followers, or will they just react? Whichever direction they choose, they will need to devise a clear strategy to move forward.*

[pwc.co.nz/fstech2020](https://pwc.co.nz/fstech2020)



## Contents

### **Foreword**

**3**

### **Executive Summary**

**5**

### **The ten technology forces that matter: how to compete in the financial services industry in 2020 and beyond**

**7**

- 1** FinTech will drive the new business model 8
- 2** The sharing economy will be embedded in every part of the financial system 11
- 3** Blockchain will shake things up 12
- 4** Digital becomes mainstream 15
- 5** 'Customer intelligence' will be the most important predictor of revenue growth and profitability 17
- 6** Advances in robotics and AI will start a wave of 're-shoring' and localisation 20
- 7** The public cloud will become the dominant infrastructure model 22
- 8** Cyber-security will be one of the top risks facing financial institutions 23
- 9** Asia will emerge as a key centre of technology-driven innovation 25
- 10** Regulators will turn to technology, too 27

### **Six priorities for 2020**

**28**

- 1** Update your IT operating model to get ready for the 'new normal' 29
- 2** Slash costs by simplifying legacy systems, taking SaaS beyond the cloud, and adopting robotics/AI 32
- 3** Build the technology capabilities to get more intelligent about your customers' needs 35
- 4** Prepare your architecture to connect to anything, anywhere 37
- 5** You can't pay enough attention to cyber-security 40
- 6** Make sure you have access to the necessary talent and skills to execute and win 42

### **Conclusion**

**45**

# Foreword

## *Is your business equipped to compete?*

*We are pleased to introduce Financial Services Technology 2020 and Beyond: Embracing disruption.*

This paper complements PwC's Project Blue<sup>1</sup> and the PwC Megatrends framework<sup>2</sup>, which examines the forces that are disrupting the role, structure, and competitive environment for financial institutions and the markets and societies in which they operate. It also continues our series of publications examining the future of financial services, including:

- Retail Banking 2020: Evolution or Revolution?<sup>3</sup>
- Capital Markets 2020: Will it Change for Good?<sup>4</sup>
- Asset Management 2020: A Brave New World<sup>5</sup>

Can you envision branches and operation centres staffed by sophisticated robots instead of human tellers? Or picture everyone from high net worth investors to high school teachers taking financial advice from artificially intelligent apps – and then investing across asset classes, currencies and geographies on a real-time basis? Or imagine if launching a bank, an asset manager or an insurance company was as simple as plugging in an appliance?

We can. This is not fantasy; it is where things are headed. We have been looking at the financial services landscape and asking some tough questions about what comes next. These are some agenda items for the leaders who operate and supervise the

global financial system: Will blockchain be as significant to the future of banking as the Internet was to physical stores? Or will fraud and technical complications marginalise its application? Will the public cloud be safe and reliable enough to outcompete on-premises solutions? Could cyber-attacks really cause worldwide panic and loss of confidence in the financial system?

The post-crisis regulatory frameworks have been gradually settling into place, and financial institutions have been adjusting their business models accordingly. It is now becoming obvious that the accelerating pace of technological change is the most creative force – and also the most destructive – in the financial services ecosystem today. In this paper, we set out to capture the real world implications of these technological advances on the financial services industry and those who must supervise and use it.



**Julien Courbe**

Global FS Technology Leader  
PwC US  
+1 646 471 4771  
julien.courbe@us.pwc.com

- 1 <http://www.pwc.com/gx/en/financial-services/projectblue>
- 2 <http://www.pwc.com/gx/en/issues/megatrends>
- 3 <https://www.pwc.com/gx/en/industries/financial-services/banking-capital-markets/banking-2020.html>
- 4 <https://www.pwc.com/gx/en/industries/financial-services/banking-capital-markets/capital-markets-2020.html>
- 5 <https://www.pwc.com/gx/en/industries/financial-services/asset-management/publications/asset-management-2020-a-brave-new-world.html>



### ***Project Blue***

There are huge forces at work in the global economy today – from a shift in global economic power and climate change to urbanisation, demographic shifts, and more. Many of our clients have been using our Project Blue framework to help assess how these megatrends will affect their strategies and business models for 2020 and beyond. Project Blue offers a structured process for adapting to these changes. Seeing the future clearly and developing a proactive, strategic response – rather than simply reacting to events – will set apart the winners from the losers in a fast-evolving market. There is no single ‘best answer’; whether these developments are threats or opportunities depends on the nature of the organisation and where in the world it sits. The results will help your institution better target investment, identify talent requirements and develop the necessary operational capabilities needed to make the most of its competitive potential.

Each of these forces will shape our lives in many ways. But for the financial services industry, as the post-Financial Crisis regulatory wave retreats, technology stands above the rest. In this paper, we look at these changes, and offer some suggestions on how to prepare for the opportunities and threats ahead.



# Executive Summary

**You are a bank executive. Imagine that you are competing against a truly global, multi-service, low-cost, digital bank: customers accessing their accounts through their mobile phones, paying with a tap on their wearables, sweeping savings to an ETF portfolio**

## ***A glimpse of what is to come***

Let's say you are a bank executive. Imagine that you are competing against a truly global, multi-service, low-cost, digital bank: customers accessing their accounts through their mobile phones, paying with a tap on their wearables, sweeping savings to an ETF portfolio (designed by an AI (artificial intelligence) engine based on their savings goals and risk appetite profile) offering no-fee, cross-border payments. Imagine if you faced a competitor bank like this, with a low and nimble footprint, prototyping new services quickly, managing regulatory compliance transparently, using an AI system to limit fraud losses, and hedging currency risk using cryptocurrencies.

This competitor does not exist today. But in the next few years, it is a very real possibility. Now what?

The financial services industry has seen drastic technology-led changes over the past few years. Many executives look to their IT departments to improve efficiency and facilitate game-changing innovation – while somehow also lowering costs and continuing to support legacy systems. Meanwhile, FinTech start-ups are encroaching upon established markets, leading with customer-friendly solutions developed from the ground up and unencumbered by legacy systems. Customers have had their expectations set by other industries; they are now demanding better services, seamless experiences regardless of channel, and more value for their money. Regulators demand more from the industry too, and have started to adopt new technologies that will revolutionise their ability to collect and analyse information. And the pace of change shows no signs of slowing.

In our latest Global CEO Survey, across all sectors business leaders told us the speed of technological change is one of their biggest concerns. In fact, in financial services, 70% of the leaders told us the speed of change in technology was a concern.<sup>6</sup> One factor is that the time it takes to go from breakthrough technology to mass-market application is collapsing. For example, in the United States, it took the telephone 76 years to be adopted by half the population. By contrast, the smartphone did it in under ten years. We are now watching blockchain move from a notebook sketch to an established technology in a tiny fraction of the time it took for the Internet to be accepted as a standard tool. Indeed, technology-driven change is so pervasive that no financial institution is immune. In Section 2, we address how these and other global megatrends are affecting the financial services industry, with a particular focus on the IT department.

<sup>6</sup> Source: PwC's 19th Annual Global CEO Survey, Jan 2016

## **Ten competitive technology-driven influencers for 2020**

It is clear that technology is affecting financial services in a multitude of ways. In the following section, we discuss ten key themes that we believe IT executives will need to address as they begin their strategic planning for 2020 and beyond. These ten themes include:

- FinTech will drive the new business model
- The sharing economy will be embedded in every part of the financial system
- Blockchain will shake things up
- Digital becomes mainstream
- ‘Customer intelligence’ will be the most important predictor of revenue growth and profitability
- Advances in robotics and AI will start a wave of ‘re-shoring’ and localisation
- The public cloud will become the dominant infrastructure model
- Cyber-security will be one of the top risks facing financial institutions
- Asia will emerge as a key centre of technology-driven innovation
- Regulators will turn to technology as well

Each of these themes is likely to affect financial services companies and their leadership teams in far-reaching ways. And while each may have a disproportionately strong effect on a given geography, customer set or industry segment, they all present opportunities for the thinking executive to get ahead. When you know a robotics movement is coming, for example, you have a choice: to lead the charge, to make sure your organisation has the right listening capabilities and agile architecture to be a ‘fast follower’, or to watch others take advantage of a generational shift. This section sets up a challenge around the ten themes: to understand them, prepare for them and see how to use them to get a competitive advantage.

## **Priorities for 2020**

The pace of change is increasing and shows no sign of slowing. Financial institutions are looking to the IT organisation to do more to help make sure they are well-positioned to succeed in the future. There are macroeconomic trends sweeping the world, and technology-driven influences buffeting the industry. What is the best approach to moving forward?

We see six priorities for success for 2020 and beyond, based on our research and our experience in the field:

- 1.** Update your IT operating model to get ready for the new normal
- 2.** Slash costs by simplifying legacy systems, taking SaaS beyond the cloud, and adopting robotics/AI
- 3.** Build the technology capabilities to get more intelligent about your customers’ needs
- 4.** Prepare your architecture to connect to anything, anywhere
- 5.** You can’t pay enough attention to cyber-security
- 6.** Make sure you have access to the talent and skills necessary to execute and win

To succeed in this rapidly changing landscape, IT executives will need to agree with the rest of the management team on the posture they wish to adopt. Will they try to be industry leaders, fast followers, or will they just react? Whichever direction they choose, they will need to devise a clear strategy to move forward. Most likely, there will be a need to partner with innovative FinTech start-ups and change their business practices based on lessons

from other industries. They will certainly need to maintain laser-sharp focus on their customers’ preferences, both stated and unstated.

Frankly, each priority is important. The good news is that each one is also achievable. The answer: combining tactical short-term actions with long-term initiatives that tie to a larger, strategic vision. This is how financial services firms will succeed in 2020 and beyond.

# *The ten technology forces that matter: how to compete in the financial services industry in 2020 and beyond*

*There are many large forces sweeping society, from demographic and social changes to shifts in global economic power. But one force in particular – namely, technological breakthroughs – is having a disproportionate affect on financial services. Here we look at the ten most important technology-driven influencers that will shape competition in this industry by the decade's end.*



## FinTech will drive the new business model

For a long time, new market entrants found it difficult to break into the financial services industry. The large, well-established financial institution that we call 'incumbents' had advantages in size, and their networks added a multiplier effect. They had strong compliance systems in place to manage ever-increasing regulations, and they had the client base and resources to prosper even in tough economic conditions.

### Where is the epicentre of disruption?

#### Most disrupted FS sectors



Source: PwC Global FinTech Survey 2016



Well, not any more. FinTech disruptors have been finding a way in. Disruptors are fast-moving companies, often start-ups, focused on a particular innovative technology or process in everything from mobile payments to insurance. And, they have been attacking some of the most profitable elements of the financial services value chain. This has been particularly damaging to the incumbents who have historically subsidised important but less profitable service offerings. In our recent PwC Global FinTech Survey, industry respondents told us that a quarter of their business, or more, could be at risk of being lost to standalone FinTech companies within five years.<sup>7</sup>

Global investments in FinTech more than tripled in 2014, reaching more than \$12 billion. In comparison, banks spent an estimated \$215 billion on IT worldwide in 2014, including hardware, software, and internal and external services.<sup>8</sup> This is a material number, and because it is so highly targeted, the FinTech spending will really make an impact.

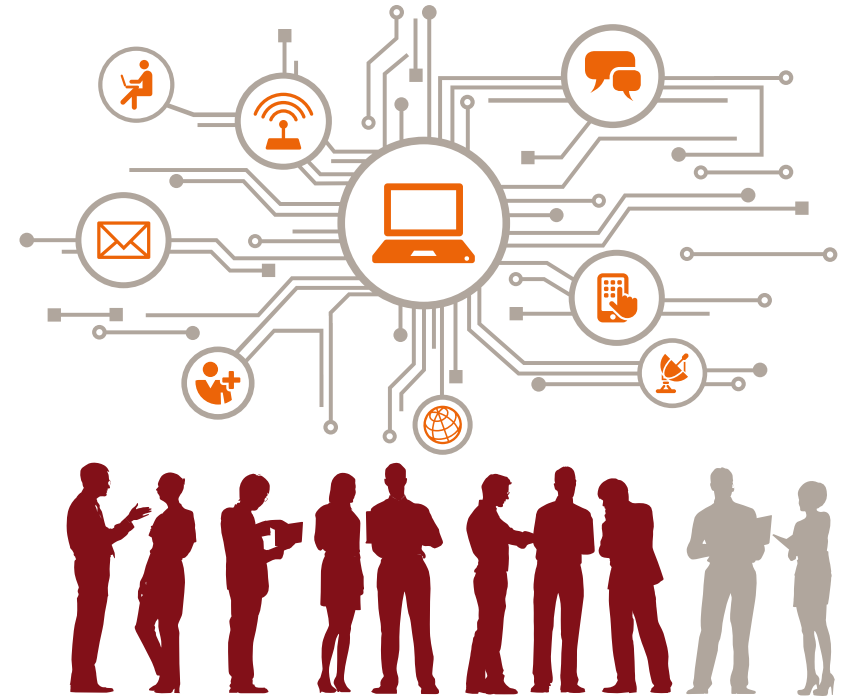
### **A cast of thousands (of start-ups)**

PwC created a tool to allow ourselves (and others) to analyse the size and complexity of the challenge to incumbents and the speed of change facing the industry.<sup>9</sup> Our online platform, which we call DeNovo, defines approximately 40 different value chains for

the financial services industry. We identified several thousand companies that are new market entrants to various components of these chains. Here is what we have seen so far:

- Successful disruptors typically offer a better customer experience and greater convenience at a much lower price.
- The effects of disruptors vary significantly across countries and value chains, largely because of differences in regulatory barriers and the robustness of local FinTech ecosystems.
- Regulatory authorities are caught between wanting to encourage competition and innovation and wanting to provide meaningful oversight of these disruptors.

Despite regulation and other potential barriers to entry, we see tremendous demand for FinTech-related services in areas such as consumer banking and wealth management. This will open up new opportunities for both incumbents and disruptors. For example, consider the rise of ‘robo-investing platforms’ offered by both online-only and traditional wealth management companies. New players are using the online-only model to reach millennials and increasingly other segments too. Meanwhile, traditional players are employing this approach to significantly



**81%**

*of banking CEOs are concerned about the speed of technological change, more than any other industry sector.<sup>10</sup>*

<sup>7</sup> PwC Global FinTech Survey 2016

<sup>8</sup> [http://www.banktech.com/management-strategies/bank-it-spend-projected-to-reach-\\$215-billion-in-2014/d/d-id/1296655?](http://www.banktech.com/management-strategies/bank-it-spend-projected-to-reach-$215-billion-in-2014/d/d-id/1296655?)

<sup>9</sup> <http://www.strategyand.pwc.com/denovo>

<sup>10</sup> PwC's 19th Annual Global CEO Survey

## The DeNovo™ platform

DeNovo is a new platform to help leading financial institutions get better strategic advice about the disruptive technologies, new business models, and other FinTech forces that are shaking up the industry. It is a resource for financial services CEOs, CTOs, business unit heads, heads of strategy, and other key decision makers who need a trusted, objective resource to help them make better strategic and operational decisions.

The platform includes a dashboard with regular updates to explain developments in key industry segments; dossiers that provide information on companies' differentiations, strategic focus, leadership, and investment information; technical information; a comprehensive view of where innovation is most aggressive (or not); competitive considerations; and other resources.

The content is developed and curated by PwC's Strategy& FinTech subject matter specialists, leading a dedicated team of over 50 strategists, equity analysts, engineers, and technologists. Using both public and proprietary data from over 40,000 sources, as well as research from across PwC's global network of over 200,000 professionals, DeNovo helps clients determine which startups, technologies, trends, and new market entrants are most relevant to them – and why.



reduce their operational costs. They are also using it to find more cost-effective ways to comply with regulatory mandates such as the UK Retail Distribution Review rules. In Asia, a new wealth-management app was launched with almost one thousand products, all without commissions or fees.

This experience is being repeated across virtually every sector within financial services. Disruptors in retail banking are using this online-only model to grow market share by offering a highly customised user experience combined with lower fixed costs. We have also seen emerging FinTech companies targeting customers using so-called “closed-loop interactions” (bi-directional messaging between institutions and their clients) that avoid the costs of larger public-facing platforms. There are new high-tech, low-footprint companies with huge potential to drive down costs and offer better customer experience in the marketplace lending arena. And we are seeing upstarts jumping into the global payments and foreign exchange sectors, sidestepping existing costly networks by leveraging innovations such as digital currencies. In one such example, an increasingly well-known start-up is using a

proprietary blockchain-based cryptocurrency and the cross-border payments model to route foreign-exchange payments between virtually any currency pair for free. And the disruption is just beginning in capital markets.

The bottom line: there are many smart people with good ideas and abundant funding trying to disrupt and improve the industry. If you work for an incumbent, scanning the market for new competitors, studying how they think about infrastructure and regulation, and considering what defense or collaboration approaches make sense are all business imperatives.

## The sharing economy will be embedded in every part of the financial system

*By 2020, consumers will need banking services, but they may not turn to a bank to get them. Or, at least, maybe not what we think of as a bank today. The so-called sharing economy may have started with cars, taxis, and hotel rooms, but financial services will follow soon enough. In this case, the sharing economy refers to decentralised asset ownership and using information technology to find efficient matches between providers and users of capital, rather than automatically turning to a bank as an intermediary.*

Today, we tend to think of financial institutions as the entities that initiate and manage transactions from end to end, typically putting their own capital at risk. Increasingly, financial institutions may play either an intermediary role, with less at stake, or just be one node in a network. This evolution will be driven by peer-to-peer transactions, enabled by partnerships between today's financial services firms and a new breed of FinTech companies. We have already witnessed this with peer-to-peer lending platforms, often in partnership with traditional banks, which exist today in places such as the UK, US and China. Many of these new companies are designing and building services that focus on a specific sliver of the value chain, or a specific subset of customers. Consumers are getting smarter about their options, too. Recent PwC research shows that 44% of those who earn less than \$75,000 per year would trust a technology company for peer-to-peer payments, and this rises to 68% among earners making more than \$100,000.<sup>11</sup>

A number of enabler companies target specific verticals like student debt, or connecting debtors and investors. They are building platforms that enable ordinary individuals to raise funds and draw credit lines from retail investors. Apple has filed a patent application for "person-to-person payments using electronic devices" that could allow iPhone users to transfer money more easily. This could potentially commoditise retail banking even further. Instead of using relatively high cost bankers to broker the connection between those who have and those who want, the disruptors are using technology to make the match: faster, cheaper, and maybe even better.

In developing markets, where branch networks are typically less dense, particularly in rural areas, physical distribution will continue to evolve, and banks are more likely to partner with new entrants to create alternative distribution channels. For example, M-PESA in Kenya, handles deposits and payments using customers' cellphones and a network of agents. According to a recent report, the service is now being used by 90% of the adult population in the country.<sup>12</sup>

Financial institutions should seriously consider sharing economy opportunities such as partnerships with digital intermediaries or even end users with an eye towards how they might deliver services at much lower costs. With their relatively informal profiles, start-ups may not, at first, seem like a threat. But in the new digital age, when businesses as well as individuals are increasingly tech-savvy, new customers will gravitate toward lower fees, convenience, and ease-of-use. And once there is enough critical mass and liquidity, the network effect takes over, and the disruptors' market share could grow exponentially, as it has in Kenya.

<sup>11</sup> PwC's 2015 Consumer Banking Survey

<sup>12</sup> "The Future of Money" which aired on Nov. 22, 2015, 60 Minutes, CBS.

## Blockchain will shake things up

*In the late 1990s, when companies began to realise the Internet's potential power, e-commerce investment and experimentation soared. And despite the 'dot com crash,' it is unlikely that anyone would deny just how revolutionary the technology has proved to be. Today, there are curious similarities with blockchain—both in how companies are being funded and how they are exploring use cases.*

<sup>13</sup> <http://letstalkpayments.com/13-blockchain-bitcoin-companies-that-raised-serious-funding-in-2015/>

<sup>14</sup> <http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/>

Last year alone, 13 blockchain companies obtained over \$365 million in funding.<sup>13</sup> According to multiple sources, by the start of 2016, blockchain companies had raised well over a billion dollars to fund their development and operations.<sup>14</sup>

### **Is the impact of blockchain technology taken into account?**

**56%**

*of survey respondents recognise its importance, but...*

**57%**

*say they are unsure about or unlikely to respond to this trend*

Source: PwC Global FinTech Survey 2016

3

We have written primers to explain what blockchain is<sup>15</sup> and how strategists see it<sup>16</sup>, and even some thoughts on our own approach to the technology. But we are hardly alone. Many major financial institutions have some form of blockchain research effort underway. In our recent PwC Global FinTech Survey, we found that 56% of survey respondents recognised the importance of blockchain. At the same time, however, 57% say that they are unsure or unlikely to respond to this trend. So, what should you do?

Several industry groups have come together to commercialise technology and apply it to real financial services scenarios. We expect this surge in funding and innovation to continue as blockchain and FinTech move from a largely retail focus to include more institutional uses. And while many of these companies may not survive the next three to five years, we believe the use of the blockchain ‘public ledger’ will go on to become an integral part of financial institutions’ technology and operational infrastructure.

### **Why blockchain matters**

There are two aspects of blockchain technology that have captivated so many C-level executives, start-up founders and private equity firms around the world. First, blockchain could make the financial services industry’s infrastructure much less expensive. And second, the list of potential

uses is almost limitless, from financial transactions to automated contractual agreements and more.

Blockchain systems could be far cheaper than existing platforms because they remove an entire layer of overhead dedicated to confirming authenticity. In a distributed ledger system, confirmation is effectively performed by everyone on the network, simultaneously. This so-called ‘consensus’ process reduces the need for existing intermediaries who touch the transaction and extract a toll in the process. In financial services, that includes those who move money, adjudicate contracts, tax transactions, store information and so on.

The sheer range of applications has attracted FinTech providers and legacy firms who hope to develop solutions both narrow and broad. In the next three to five years, we see transaction volumes and the associated profit pools shifting from intermediaries toward the owners of new highly efficient blockchain platforms. These transactions could include transferring digital or physical assets, protecting intellectual property, and verifying the chain of custody. In an era of cyber-crime and stringent regulatory requirements, a highly fraud-resistant system for protecting and authenticating almost any kind of transaction could have a revolutionary impact on the financial services industry.

### **In blockchain we trust?**

Of course, trust does not occur overnight. This is the challenge facing both individual institutions and the industry as a whole. For blockchain to be adopted on a large scale, we will need to experience a migration of trust from today’s effective-yet-expensive central counterparty utilities to the distributed model. The business benefits for many players, or even the industry, will not materialise if the ‘trust issue’ is not addressed effectively. Some of the hurdles that lie ahead: understanding whether or not the public ledger can be hacked, addressing Bitcoin’s negative reputation, and navigating potential regulatory challenges related to blockchain’s adoption. For example, while confirmation is effectively performed by everyone on the network simultaneously, if a majority of the participants forming the network consensus model were to collude to transact a fraud, a ledger might be manipulated. This might be an issue in a relatively small network without proper vetting procedures. We also see a need to address security limitations with linked technologies, like the external systems that monitor events to trigger blockchain transactions once conditions have been met.

Still, this is a participatory sport and there is a lot to lose from sitting on the sidelines. Now is the time for testing, planning and learning. Given the extraordinary range of options and potential technology partners, one of the bigger challenges is to sort through the hype. Once you have a clear vision of where to apply the technology and why, it will be easier to create a workable implementation plan for building blockchain into your infrastructure.

15 <https://www.pwc.com/us/en/financial-services/publications/qa-what-is-blockchain.html>

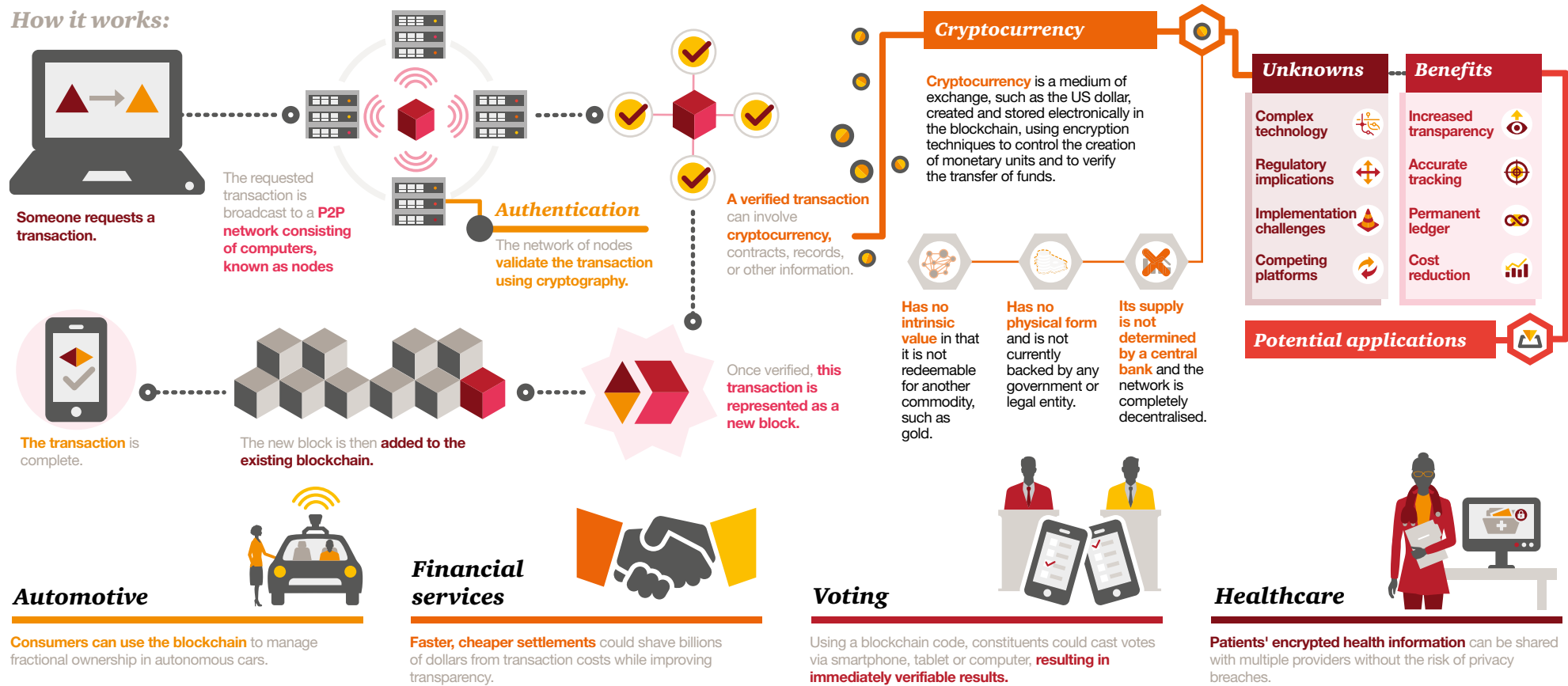
16 <http://www.strategy-business.com/article/A-Strategists-Guide-to-Blockchain>



## A look at blockchain technology

**What is it?** The blockchain is a decentralised ledger, or list, of all transactions across a peer-to-peer network. Using this technology, participants can transfer value across the Internet without the need for a central third party.

### How it works:



Sources: "Money is no object: Understanding the evolving cryptocurrency market," PwC, 2015/"A Strategist's Guide to Blockchain," strategy+business, January, 2016/"How Blockchain Technology Is Disrupting Everything," TechDay, 2016

## Digital becomes mainstream

*Two decades ago, many large financial institutions built ‘e-business’ units to ride a wave of e-commerce interest. Eventually, the initial ‘e’ went away, and this became the new normal. Internet development and large technology investments drove unprecedented advances in efficiency.*

Today’s digital wave has the same markers: separate teams, budgets and resources to advance a digital agenda. This agenda extends from customer experience and operational efficiency to big data and analytics. In financial services, we have seen this approach applied to payments, retail banking, insurance and wealth management, and migrating toward institutional areas such as capital markets and commercial banking.

### **The digital wallet: a case study**

Consider the evolution of the digital wallet, which is rapidly just becoming ‘the wallet’. Digital wallets – typically housed within a mobile phone – are now at the core of a battle between traditional financial services providers and disruptors. They give consumers a fast, secure, low-cost method to use, store and send money over the Internet. It is a service they value as well as a front-door to many lucrative bank offerings.

Should banks care? Well, the trend toward greater acceptance of the mobile device as a banking channel also converges with the billions of payment cards issued globally and the transactions they generate. Ironically, given the expense of deploying EMV chips

to replace magnetic stripe technology, many consumers are now turning to the smartphone as the preferred tool for making online and proximity payments. Mobile devices offer more convenience and greater security than plastic cards, many of which still include magnetic stripes. The tap-and-pay mobile payment user experience can also be faster and easier than typical plastic card transactions.

Who is using digital wallet technology? Most studies show that millennials are the key early adopters of mobile payments.<sup>17</sup> In a recent study, roughly half of millennials said they would rather pay for small items with their mobile phone than with cash; a similar share want to use mobile tools to split bills with their peers and track spending.<sup>18</sup> This is a new generation of consumers, and they are growing up associating core transactional services with technology and start-up brands, neither of which have historically been associated with financial services.

### **Who wins?**

In recent years, the banking sector has seen a rapid rise of non-traditional competitors, through alternative payment methods such as gift cards and contactless payments built

into mobile operating systems. Now that adoption has grown, banks want greater control over alternative channels. They want to manage the security, user experience, and customer connectivity at the point of purchase. Of course, controlling the digital wallet also gives a bank a better chance of protecting top-of-wallet status for its card products, and the interchange fees that follow. And this matters: for most banks, even a modest 3%–5% reduction (or increase) of interchange fees from debit and credit cards would represent a material change.

And then there is the data. A wallet creates real-time connectivity that the bank can use to send valuable information like balances and alerts. If handled properly, it can also successfully present revenue-generating, point-of-sale offers and promotions to customers. For example, real-time financing offers could be directed to debit card only customers who have expressed interest in building their credit profiles but who do not want to carry credit card debt. Fee income from these offers could be worth twice as much as average deposit revenue, making this a very lucrative source of income for

<sup>17</sup> Incidentally, high net worth consumers are early adopters too: another group that financial institutions cannot afford to lose.

<sup>18</sup> <http://www.adweek.com/news/advertising-branding/why-mobile-payments-are-millennial-must-161163>



banks. Non-standard providers also hope to use point-of-sale data to get valuable insights into consumer behaviour.

Finally, there are other security benefits from owning and controlling the digital wallet. By setting the terms of engagement, banks can demand stronger authentication, identification and verification processes. Without this, they are at the mercy of partners who may not have the same priorities. User data also helps banks to improve real-time fraud detection.

***‘Change the bank’ becomes the bank***

Over the next three to five years, digital efforts will advance in areas as diverse as robo-investing, automation of consumer lending and clearing and settlement of cash and securities transactions. As they do, they will stop being exotic, and will just be

‘how we do things’. Institutions will need to balance the need for separate ‘change the bank’ transformation teams with the inevitability that digital will become the platform. Practically, this means you have to keep the change-the-bank and the run-the-bank teams on the same page, operationally and strategically. At the same time, we know all organisations have a natural resistance to change, especially after years of a relatively protected status. To ward off a determined FinTech opponent, consider ‘challenger’ models in banking, insurance and wealth management that try to anticipate what a fierce competitor would look like.

***Institutions will need to balance the need for separate ‘change the bank’ transformation teams with the inevitability that digital will become the platform.***

## Customer intelligence will be the most important predictor of revenue growth and profitability

*Do you know what your customers value? Are you sure? Customer intelligence used to be based on some relatively simple heuristics, built from focus groups and surveys. These were proxies for real, individualised data about consumer behaviour, and the results were pretty hazy. Now, technology advances have given businesses access to exponentially more data about what users do and want. It is an amazing opportunity for whomever can use analytics to unlock the information inside, to give customers what they really want.*

For example, consider millennials: a key demographic, and one that banks generally have targeted through digital channels. Financial institutions should look below the surface to examine the behavioural attributes that drive consumer decisions. The following are key to millennial behaviour: they tend to build wealth as a result of owning a small business, investments, or real estate; they turn to social networks for content, product reviews, opinions and referrals; and they look for opportunities to improve their financial 'health'. Financial institutions that sift through available data can engage millennials by being ready with the right offer when relevant life events present buying opportunities.

The data is everywhere, and over the next five years, hyper-connectivity will give financial institutions the opportunity to use it. It will not only be computers and smart devices that record and communicate data, but everything from cars to coffee machines. This is referred to as the 'Internet of Things'. Customers are learning more about the value of their personal data. We expect to see them tendering out their information to banks, insurers and asset managers in return

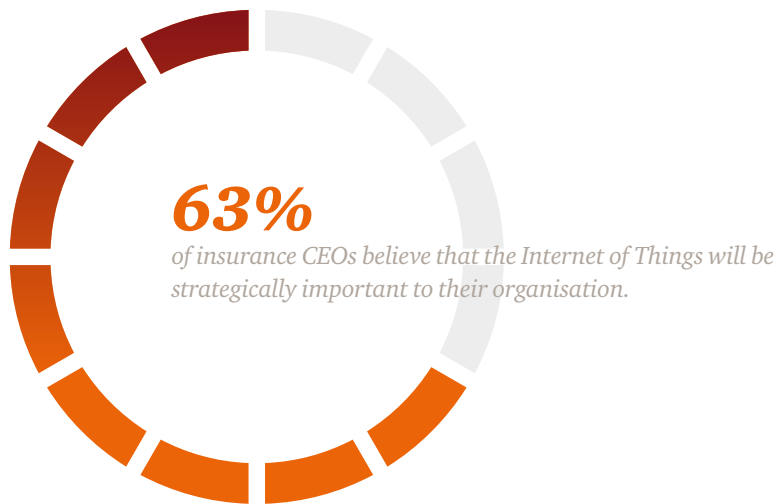
for the best deal, much as affinity groups already do. Within asset management, hyper-connectivity will also pave the way for greater product customisation. For life and health insurers, wearable computing (building on the technology already widely used in fitness sensors), could make the underwriting process more collaborative. For example, insurers may use the real-time insights into policyholder health and behaviour to offer discounts, eliminate the need for lengthy medical checks and simplify the contract process.

With other developments, this will also intensify price competition and pressure on cost. Big data analytics, sensor technology and the communicating networks that make up the Internet of Things will allow insurers to anticipate risks and customer demands

with far greater precision than ever before. The benefits would include not only keener pricing and sharper customer targeting, but a decisive shift in insurers' value model from reactive claims payer to preventative risk advisor. But it also implies that we will see a divergence between companies who use data to their advantage and those who do not. The winners will be able to price products based on a deeper understanding of risk; the losers will merely compete on price, compressing their margins with lower revenues and proportionately higher payouts.

**By 2020**  
there will be **20** times more useable data than today.<sup>19</sup>

<sup>19</sup> 'The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East', International Data Corporation, December 2012



Source: PwC's 18th Annual Global CEO Survey

### **The era of mass customisation**

As customers become more connected through social media, they are becoming more demanding and less loyal. Easier comparison and faster switching mean that relationships can be brief and largely transactional. We are already seeing one-click transfer, which moves all funds, direct debit instructions and other services to the new provider with very little effort on behalf of the customer. And the demographic trends have scary implications for conventional financial services companies because the youngest users are the least loyal. Recent research has found that one in three millennials in the United States are open to switching banks in the next 90 days and a similar proportion believe they will not even need a bank in the future.<sup>20</sup> What explains this decline in customer 'stickiness'? Service offerings that feel generic and tools that have made switching less painful.

Consumers now compare financial institutions to digital leaders across all industries, as well as to their industry peers, and they are falling short. Customers have experienced first-hand that digital commerce delivers speed and personalisation, and this shapes their expectation of financial services, too. Instead of a mortgage, insurance policy, or investment plan that broadly meets their needs, buyers want customised, adaptive solutions that evolve and deliver specified outcomes. For example, target-date funds automatically adjust the asset mix to a user's expected retirement age. Personalised service and tailored solutions were once the preserve of high net worth clients. Now, technology is opening it up to mass affluent consumers, and beyond.

In the insurance industry, advances in processing capacity, customer profiling, and risk analytics are now opening the way for a new generation of 'smart' policies. While being as affordable and easy to understand and compare as today's off-the-shelf products, these policies could be both fully customised to individuals and able to adapt to their changing needs. Crucially, the technological developments that are making this new generation of policies possible would also making it easier for new entrants to break into the market at relatively little cost.

**One in three millennials in the United States are open to switching banks in the next 90 days and a similar proportion believe they will not even need a bank in the future.**

Source: Viacom Media Networks – The Millennial Disruption Index

<sup>20</sup> Viacom Media Networks – The Millennial Disruption Index



### Smarter service, smarter sales

Financial institutions are already using artificial intelligence (AI) to experiment with service that is far more personalised. Many banks in the United States are piloting AI-based client advisors, where the AI engine is primed with the entire product manual, past call history, policy and procedures guidelines, and more, to provide context-based service to their customers.

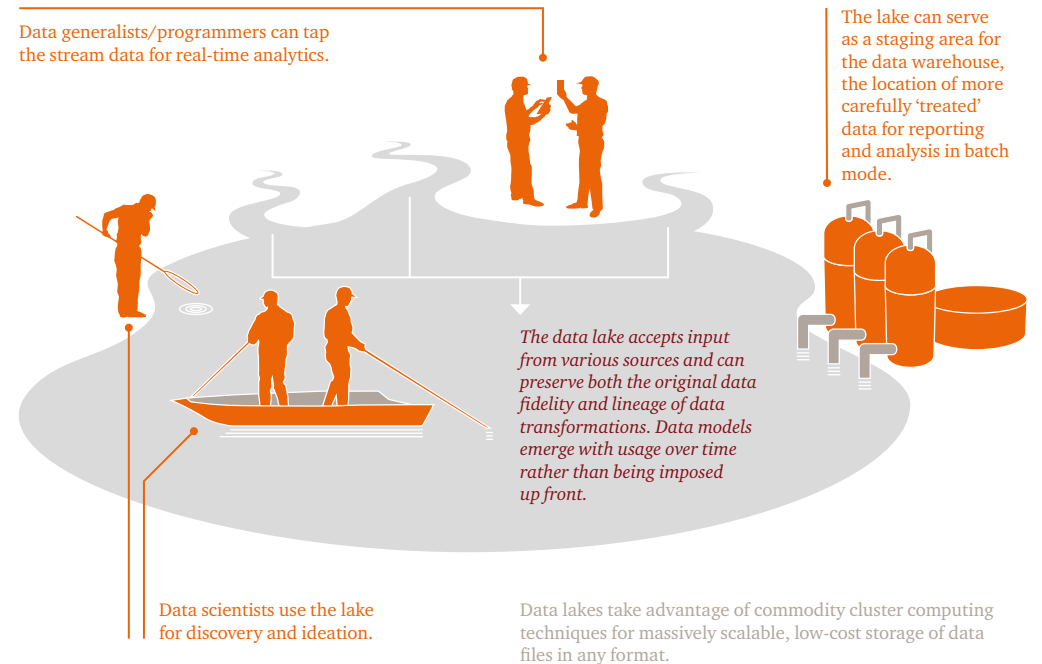
We expect AI, machine learning, and customer analytics to become the driver of client engagement over the next decade. Certainly, financial institutions will need to deliver instantaneous, seamless transactions, but speed is just the baseline requirement. Smart businesses will develop new forms of virtual engagement capable of integrating themselves into customers' lives. They will stick because they will be personal: informed by intelligence gathered from data about consumer behaviours, choices, and volunteered preferences.

### Rethinking the service architecture

Before firms can engage customers like this, they will have to make sense of a torrent of data that defies human comprehension and that will require gathering, interpreting and presenting massive quantities of data in real-time. Few firms are ready. In fact, most will need to change many aspects

of how they have traditionally managed IT. There are four building blocks for this emerging solution architecture. At the visualisation layer, the customer interacts with a self-service dashboard and search capabilities, displayed through advanced visualisation tools that generate and present rapid insights. In the application layer, the visualisation layer is integrated into the business processes management with capabilities such as case management, alerting and reporting. The analytics layer does the thinking, using advanced AI techniques to profile and predict behaviour, detect anomalies and discover hidden relationships. And, data lakes will form the key layer of the solution, acquiring data rapidly from disparate sources and ingesting it so it can be used productively. Data lakes are a new take on data warehousing, taking advantage of cheaper tools to distribute storage and processing. They offer a scalable platform that can store a wide range of data models, enabling analysis of both structured and unstructured data. Unlike the existing systems that many firms use today, they won't buckle under the much larger volumes that will soon arrive.

### A repository for large quantities and varieties of data, both structured and unstructured



Source: PwC Technology Forecast (Issue 1, 2014); "The enterprise data lake: Better integration and deeper analytics"

## Advances in robotics and AI will start a wave of ‘re-shoring’ and localisation

*When ATMs were first introduced, many customers refused to use them. Gradually though, after time and training, they came to see that ATMs could offer a better service experience. And trust followed.*

ATMs are robots. They are very simplistic, purpose-built robots – but they provide consistent, convenient, low-cost service and customers have grown to trust them. The same principles will apply to other, more sophisticated financial services applications. There have been astonishing advances in robotics and AI, machine learning and pattern recognition in recent years. Over the next five years, we will see a shift from standalone uses to full integration into a company’s business-as-usual activities.

### **What robots can do**

We are already seeing alliances between leading incumbent financial services and technology companies, using robotics and AI to address key pressure points, reduce costs and mitigate risks. They are targeting a specific combination of capabilities such as social and emotional intelligence, natural language processing, logical reasoning, identification of patterns and self-supervised learning, physical sensors, mobility, navigation and more. And they are looking far beyond replacing the bank teller.

Here are some of the capabilities shaping these sophisticated machines:

- **Cognition:** The robot’s ability to perceive, understand, plan and navigate in the real world. Better cognitive ability means robots can work autonomously in diverse, dynamic and complex environments.
- **Manipulation:** Precise control and dexterity for manipulating objects in the environment. With improvements in manipulation, robots will take on a greater diversity of tasks and use cases.
- **Interaction:** The robot’s ability to learn from and collaborate with humans. Progress here – such as support for verbal and nonverbal communications, observing and copying human behaviour, and learning from experiences – means robots will increasingly be able to work alongside humans.

Already, some robots can sense the details of their environments, recognise objects, and respond to information and objects with safe, useful behaviours. Over time, they will be able to perform not only more tasks, but more complex tasks. Service robots are in the early stages of a long development cycle, and they still face some big technological

hurdles. In the next three to five years, we expect modest, evolutionary gains. After that, though, we anticipate rapid gains, as new models combine increasingly powerful and standard modular platforms with the ability to learn. To take an even broader view, robotic process automation is already making inroads in financial services digital operations, too. There are whole categories of work that had not been seen as cost-effective to automate. However, with lightweight software ‘bots’, workers are freed up to focus on higher value activities.

### **Talented people, talented machines**

In the last 20 years, US companies have ‘offshored’ repetitive tasks to lower-cost locations such as India, China and Poland. However, relative costs for labour in those regions have started to rise. Combine this with improvements in robotics and AI capabilities and machines will soon become credible substitutes for many human workers. As the capabilities continue to improve and technology continues to drive down the cost of machines, these forces will combine to spur re-shoring, as more tasks can now be performed at a competitive cost on-shore. Even functions that seem dependent on human input, such as product

design, fraud prevention and underwriting, will be affected. At the same time, the need for software engineering talent will continue to expand.

### ***The B2B robot that is already down the hall***

AI already plays a prominent role in the capital markets sector, starting with algorithmic triggers in high-speed trading. Next generation algorithmic trading systems are already moving from descriptive and predictive to prescriptive analysis, improving their ability to anticipate and respond to emerging trends. And while ‘algo’ trading programs were once limited to hedge funds and institutional investors, private investors can now get access to them too.

AI is also prominent in investment activity. The technology will become a core component of the fund design process, particularly around trading authorisations and hand-offs with human investors. AI systems already drive investment strategies that complement active management, governing the decisions of passive funds and driving greater returns in active ones. This, along with the increasing body of research citing the relative advantages of passive funds, could force asset managers to radically rethink active fund management.

By 2020, AI will also automate a considerable amount of underwriting, especially in mature markets where data is

readily available. Even in situations where AI does not completely replace an underwriter, greater automation would allow humans to concentrate on assessing and pricing risks in the less data-rich emerging markets. It would also free up underwriters to provide more risk management, product development advice and other higher value support for clients.

Of course, banks already use AI to detect payments fraud. Now, they are using AI’s ability to spot abnormal behaviour to detect market abuse and rogue trading. As hyper-connectivity accelerates and more business moves over to digital channels, the risk of fraud, hacking, data compromise and other cyber-vulnerabilities will continue to grow. In response, firms will use AI to fight back with methods like predictive analytics (past and forecast spending behaviour) and location data from customers’ smart phones and wearables.

### ***Thinking machines***

We urge financial institutions to rapidly ramp up their efforts to understand and develop a vision for their use of robotics and AI. They will need to find and integrate more industrial engineers into their talent plan. And they will need to learn from industries such as manufacturing and technology that have used robots extensively for decades.

***A core component of the fund design process, particularly around trading authorisations and hand-offs with human investors.***

***Banks already use AI to detect payments fraud. Now, they are using AI’s ability to spot abnormal behaviour to detect market abuse and rogue trading.***

## The public cloud will become the dominant infrastructure model

*As significant as the shift toward cloud-based computing has been, it is just getting started.*



*...believe that cloud computing will be strategically important to their organisation.<sup>21</sup>*

<sup>21</sup> 155 asset management CEOs interviewed for PwC's 18th Annual Global CEO Survey: A marketplace without boundaries? Responding to disruption ([www.pwc.com/ceosurvey](http://www.pwc.com/ceosurvey))

<sup>22</sup> <http://www.fiercecio.com/story/cloud-adoption-costs-are-down-real-savings-can-be-had-smart-negotiators/2015-07-23>

Today, many financial institutions use cloud-based software-as-a-service (SaaS) applications for business processes that might be considered non-core, such as CRM, HR and financial accounting. They also turn to SaaS for 'point solutions' on the fringes of their operations, including security analytics and KYC verification. But as application offerings improve and as COOs and CIOs get comfortable with the arrangements, the technology is rapidly becoming the way that core activity is processed. By 2020, core service infrastructures in areas such as consumer payments, credit scoring, and statements and billings for asset managers' basic current account functions will be well on the way to becoming utilities.

### Using the cloud to scale

What is behind this shift? Data storage costs have plummeted, facilitated by cloud-based infrastructure. This has made it easier to manage 'big data' and apply sophisticated analytics, and it has also reduced the barriers to entry for new FinTech disruptors. According to the International Data Corporation (IDC), public cloud investments are growing quickly, spending on private cloud is increasing, and traditional infrastructure spending has plateaued. IDC

estimates that public cloud investments increased by 32% in 2015 to US\$21.7 billion and private cloud investments grew in 2015 by 17%, reaching US\$11.7 billion. Overall, total cloud IT infrastructure spending grew 26% in 2015, reaching US\$33.4 billion. To put that in perspective, this is approximately one-third of all IT spending.<sup>22</sup>

Curiously, the sharing economy also plays a role here. After all, some companies that have a demonstrated competence in an area are choosing to sell it to others who need it. For example, the payments infrastructure of many industrial, healthcare and smaller FinTech institutions are being provided by conventional banks. These banks are selling their infrastructure as a service to others, and leveraging the cloud to do it. In our view, this provides an important source of revenue to these institutions.

### Bring an umbrella, just in case

With customers demanding a flexible, personalised system experience, and with costs continuing to drop, the cloud is here to stay. It is the sensible way to deliver innovation within a target return on equity. But there are many challenges in shifting from an on-premises model to a cloud-based

model. What are the best ways to manage an architecture that is more diffused and fragmented than ever? How can you juggle security, data protection and commercial confidentiality? There are even regulatory ramifications, as some countries have imposed considerable restrictions on the transfer of client data to the public cloud. As a result of this, many financial institutions today are leaning towards adoption of a private-cloud solution.

Despite the cautionary note, we expect that the next several years will result in an increasing adoption of the public cloud within the financial services industry. Like FinTech, robotics and digital, this will require new ways of thinking for organisations and IT departments. But the benefits will certainly be significant too.



## Cyber-security will be one of the top risks facing financial institutions

Financial services executives are already depressingly familiar with the impact that cyber-threats have had on their industry. In PwC's 19th Annual Global CEO Survey, 69% of financial services' CEOs reported that they are either somewhat or extremely concerned about cyber-threats, compared to 61% of CEOs across all sectors.

Unfortunately, it is not likely to change for the better in the coming years, due to the following forces:

- Use of third-party vendors
- Rapidly evolving, sophisticated and complex technologies
- Cross-border data exchanges
- Increased use of mobile technologies by customers, including the rapid growth of the Internet of Things
- Heightened cross-border information security threats

### **The Internet of Things (IoT): a case study**

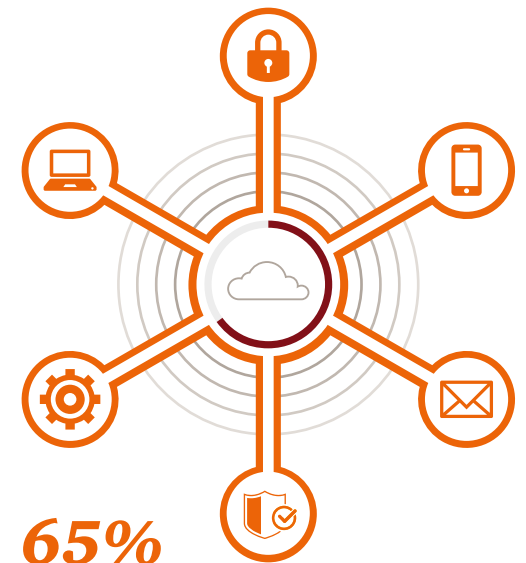
Expected IoT growth introduces a new set of security risks and challenges that will require serious attention. IoT refers to the proliferation of physical objects (devices, cars, houses, wearables) that contain sensors, software and the ability to communicate. The opportunities are fascinating, like dishwashers that can schedule a repair visit at the sense of an impending part failure. But every chain has its weakest link, and the company

that maintains the dishwasher may not be as passionate about patching software vulnerabilities as you are.

Some industry sources see the number of IoT devices deployed across the world reaching about 25 billion by 2020.<sup>23</sup> Until now, IoT growth in financial services has primarily occurred in payments, insurance and banking. Banks are forming partnerships with wearable technology manufacturers to allow customers to make mobile payments using watches or fitness trackers. Insurers are using telematics technology to monitor driving habits and provide discounts to safe drivers.

Cyber-security is the leading challenge to the adoption of IoT technology because insecure interfaces increase the risk of unauthorised access. Here are some of the concerns:

- **Attack surface:** Hackers can gain entry to a corporate network through an IoT device.
- **Perimeter security:** IoT technology relies on cloud-based services, so it will be challenging to implement effective perimeter defenses.



## 65%

of FS companies said they have adopted cloud-based security.<sup>24</sup>

<sup>23</sup> <http://www.gartner.com/newsroom/id/2905717>

<sup>24</sup> PwC's Global State of Information Security Survey 2016: <https://www.pwc.com/gsis>





- **Privacy concerns:** The pervasiveness of IoT data collection coupled with advanced analytic capabilities could potentially result in consumer privacy violations.
- **Device management:** Many IoT devices currently do not support implementation of strong security controls, and maintaining a security baseline will only get harder as IoT devices proliferate.

### **Fighting back**

As guardians of value, financial institutions have long dealt with sophisticated threats. However, cyber-crime is making the targets more appealing than ever. Earlier this year, hackers made off with tens of millions of dollars from Bangladesh's central bank by using malware to gain access to accounts. With incentives like these, criminals will continue to look for similar vulnerabilities in the future. And there are ominous signs that things could get worse, as certain threat actors now appear to be working together to carry out attacks.

Fortunately, the same capabilities that make networks more vulnerable can strengthen defenses as well. Financial institutions can use big data analytics to monitor for covert threats. This helps them identify evolving

external and internal security risks and react much more quickly. And the miniaturisation of technology that has driven smartphone growth has also made biometric security more practical. For example, some banks allow customers to access their accounts using thumbprints, or even voice and facial recognition – an approach that is more convenient for consumers and improves security.

Cyber-security is already important, and it will become even more significant for institutions and their regulators in the future. The challenge will be to balance safety with customer convenience. For full-scale providers who are trying to maintain visibility across channels, this is harder than it looks. But there are guidelines which can help financial institutions identify and prioritise threats, quickly detect and mitigate risks and understand security gaps. With a risk-based framework, companies can communicate and collaborate as necessary, decide how to design, monitor and measure their cyber-security goals, and keep their data safe.



## Asia will emerge as a key centre of technology-driven innovation

America's reputation (and Silicon Valley's, in particular) as a technology juggernaut is so ingrained that it can be easy to miss the globalisation of innovation. But if you happen to look behind the social network or the router that sends your email, you will quickly see how rapidly things are changing everywhere.

### Asia's rising demographics

Around the world, the middle class is projected to grow by 180% between 2010 and 2040; Asia's middle class is already larger than Europe's. By 2020, the majority share of the population considered 'middle class' is expected to shift from North America and Europe to Asia-Pacific. And over the next 30 years, some 1.8 billion people will move into cities, mostly in Africa and Asia, creating one of the most important new opportunities for financial institutions.<sup>25</sup>

These trends are directly linked to technology-driven innovation. Initially, as developments in agricultural technology improved labour productivity, rural workers began migrating to cities in search of better opportunities. At first they found jobs in capital-intensive industries like manufacturing for the local market – and then, as technology drove quality improvements, for the global market. Meanwhile, advances in computing and telecommunications made it possible for Western companies to offshore certain support functions to places like the Philippines and India, creating relatively well-paying jobs. Over time, the trend has

Global middle class statistics – population in millions

	2009		2020		2030	
North America	338	18%	333	10%	322	7%
Europe	664	36%	703	22%	680	14%
Central and South America	181	10%	251	8%	313	6%
Asia Pacific	525	28%	1740	54%	3228	66%
Sub-Saharan Africa	32	2%	57	2%	107	2%
Middle East and North Africa	105	6%	165	5%	234	5%
World	1845	100%	3249	100%	4884	100%

Source: Organisation for Economic Cooperation and Development

**The middle class in Asia-Pacific countries is expanding rapidly as incomes rise across the region<sup>26</sup>**

become self-reinforcing: more jobs in cities have led to better technology infrastructures in cities, which has attracted employers who can now serve global markets. The result: more urbanisation and a growing middle class across the emerging markets.

A rapidly growing middle class tends to drive higher consumption: scooters,

televisions, mobile phones and more. Asia-Pacific countries, with the world's largest middle class growth, will also see the largest demand for technology-driven innovation. There are other demographic shifts to support this growth. Asia has a comparatively young population of 'digital natives', the post-millennials who have grown up in a world in which digital

25 PwC's Retail Banking 2020: Evolution or revolution

26 Source: PwC's "Retailing 2020: Winning in a polarized world", <https://www.pwc.com/us/en/retail-consumer/publications/retailing-2020.html>

**China now has the world's largest peer-to-peer (P2P) lending market, and has more mobile smartphone users than any other country in the world.**

technology was already prevalent. Asia also has the largest inter-connectivity of flows with other emerging economies, and an average GDP growth that outperforms its peers in the West. As consumption grows, people become more sophisticated buyers of services, and they learn to continuously evaluate the price vs. value equation. For consumer-oriented companies, including those in financial services, any 'free ride' in the Asia-Pacific countries is now over; they will need to rely on technology innovations to get and keep customers.

**Many US financial institutions will have fully functional Asian hubs that can act as a catalyst for technology innovations, for both local and global deployment.**

### **Where the venture capitalists go**

Here are two statistics that may surprise some readers: China now has the world's largest peer-to-peer (P2P) lending market, and has more mobile smartphone users than any other country in the world. In fact, across Asia, we are seeing companies jumping to meet their customers' rapidly rising expectations for

financial services offerings – often, ahead of other markets. This includes embracing mobile innovations and creating a seamless, omnichannel customer experience. They are using mobile analytics to serve customers in context of their transactions. Cloud computing is gaining traction as a top

technology priority across the Asia region, with more than 50% of institutions reporting public cloud as a critical or high priority.<sup>27</sup> They are not necessarily doing it on their own, though; banks in the region typically partner with third parties to develop, implement, and integrate mobile payment technologies.

Investors have been quick to follow, and investments in AsiaPac FinTech grew faster in 2015 than previously predicted.<sup>28</sup> There were four times as many investments in FinTech companies in the region relative to the previous year. In the first nine months of 2015, investors poured in a staggering US\$3.5 billion. Payments and lending account for nearly two out of every three dollars invested in AsiaPac FinTech companies, and they drove much of this growth. But while payments and lending have dominated the scene thus far, Asian start-ups are now starting to focus on blockchain, cloud, and cyber-security as untapped niches in the FinTech industry – much like their counterparts in Silicon Valley.

### **Why Asia FinTech matters**

According to our research, Asia has now become the global leader in research and development across all industries, accounting for about one of every three dollars spent on corporate R&D spending.

And in FinTech, the market is second only to the United States in investors' interest. As we have noted elsewhere, Asia offers some key advantages to Western-based companies looking for innovation, including lower-cost but highly skilled resources (arguably on a level with those in the West), and a large market for testing and launching new products and services. Disruptive innovations typically begin as low-cost products and services that target the most price sensitive customers. Asia, with its wealth constraints, vast population and favourable regulatory environment, represents an ideal fertile ground for disruptive innovation, as many industries have discovered.<sup>29</sup>

By 2020, we expect that many US financial institutions will have fully functional Asian hubs that can act as a catalyst for technology innovations, for both local and global deployment. As specialised technology skills become harder to find, companies that have a foothold in Asia may see recruiting advantages, too.

<sup>27</sup> Source: Forrester Research, <https://www.forrester.com/The+Asia+Pacific+Public+Cloud+Market+Will+Reach+238+Billion+By+2020/-/E-PRE8912>

<sup>28</sup> <http://www.moneysedge.com/newsimage?id=646>

<sup>29</sup> <http://usblogs.pwc.com/growthleaders/to-launch-disruptive-innovation-head-east/>

## Regulators will turn to technology, too

*The use of technology and its implications are not limited to financial institutions.*

Regulators are rapidly adopting a wide range of data gathering and analytical tools too. They are trying to learn more about individual institutions' activities and overall systemic activity. They also hope to monitor the industry more effectively and to predict potential problems instead of regulating after the fact. Examples of this include the supervisory procedures and data requests tied to 'stress tests', asset quality reviews and enhanced reporting requirements coming out of Washington, London and Basel. Using sophisticated analytical tools on large volumes of data, regulators can compare scenarios and address potential issues before they become full-scale market problems.

### **The US regulators plug in...**

In United States, the Consumer Financial Protection Bureau (CFPB), which focuses on consumer protection, has invested heavily in analytics and digital technology. For example, the agency created eRegulations, an online tool to help users find, research, and understand regulations.<sup>30</sup> Also from the CFPB, Project Qu is an open source data platform that lets users query complex data about mortgage loans, combine it with other data, and then summarise it. The

SEC's Office of Compliance Inspections and Examinations (OCIE) has invested significant resources to enhance its data mining and analysis capabilities, such as its National Exam Analytics Tool. This tool, known as NEAT, combs through data to identify potential insider trading, improper allocation of investment opportunities, and other infractions.

### **...as do the Europeans**

In Europe, the regulators have put quite a bit of emphasis on how technology is used. In the UK, the Financial Conduct Authority (FCA) is stepping in to make sure that financial institutions do not abuse their newfound 'big data power'. For example, the FCA is looking into how insurance firms use their own large data collections with web analytics and social media data. Other EU regulators are looking into the 'opportunities and challenges' related to the use of big data to see if current regulations and supervisory measures are sufficient.

### **Financial institutions can do their part**

This is only the beginning. As financial institutions themselves continue to automate controls and monitoring in KYC/AML, trade surveillance, reconciliations and other areas, regulators will seek direct access to these tools – either on an ongoing basis or during supervisory reviews. As a result, firms will need to make data and control transparency priorities as they implement these tools and comply with data requests. It is shortsighted to focus solely on compliance with current regulations. Rather, firms should develop a better understanding of where their data and associated controls live. This will let them work with a growing range of interested regulatory bodies more quickly, easily and accurately, on everything from stress tests and periodic exams to individual requests. By doing so, they will improve their credibility with regulators today and be ready for the future.

<sup>30</sup> <http://www.consumerfinance.gov/eregulations/>



# *Six priorities for 2020*

To benefit from these technology developments, we recommend that financial institutions focus on six key priorities:

1. Update your IT operating model to get ready for the 'new normal'
2. Slash costs by simplifying legacy systems, taking SaaS beyond the cloud and adopting robotics/AI
3. Build the technology capabilities to get more intelligent about your customers' needs
4. Prepare your architecture to connect to anything, anywhere
5. Pay more attention to cyber-security before it becomes urgent
6. Make sure you have access to the talent and skills necessary to execute and win

You may feel that you have already seen this movie. After all, in broad terms, these have always been good things to do. But it is not a rerun; how you will do it, and why, is quite different from what you may have thought about until now. What worked for the client-server world will not work for cloud. What worked to secure card-not-present transactions will not work with the Internet of Things. And while any given institution will find some priorities more urgent than others, they all matter if you want to stay ahead of the changes sweeping through the industry. The alternative – playing catch-up in the very different financial services marketplace of 2020 – is a bad plan for anyone.





## Update your IT operating model to get ready for the 'new normal'

*By 2020, your operating model is probably going to look quite stale, even if it is serving you well today. That is because what your financial institution offers to your customers is almost certain to change, in ways both large and small. This will require important changes across, and around, the entire IT stack.*

You may need different hardware, software, or storage technology. You may also need to rethink the way you network the components. Of course, that is just a start. Will you build or buy? Does location matter? How will you make decisions on what to do, as well as what not to do? Do you have the proper organisation to fit the new program, now and as it continues to evolve? How will you know if you are getting it right?

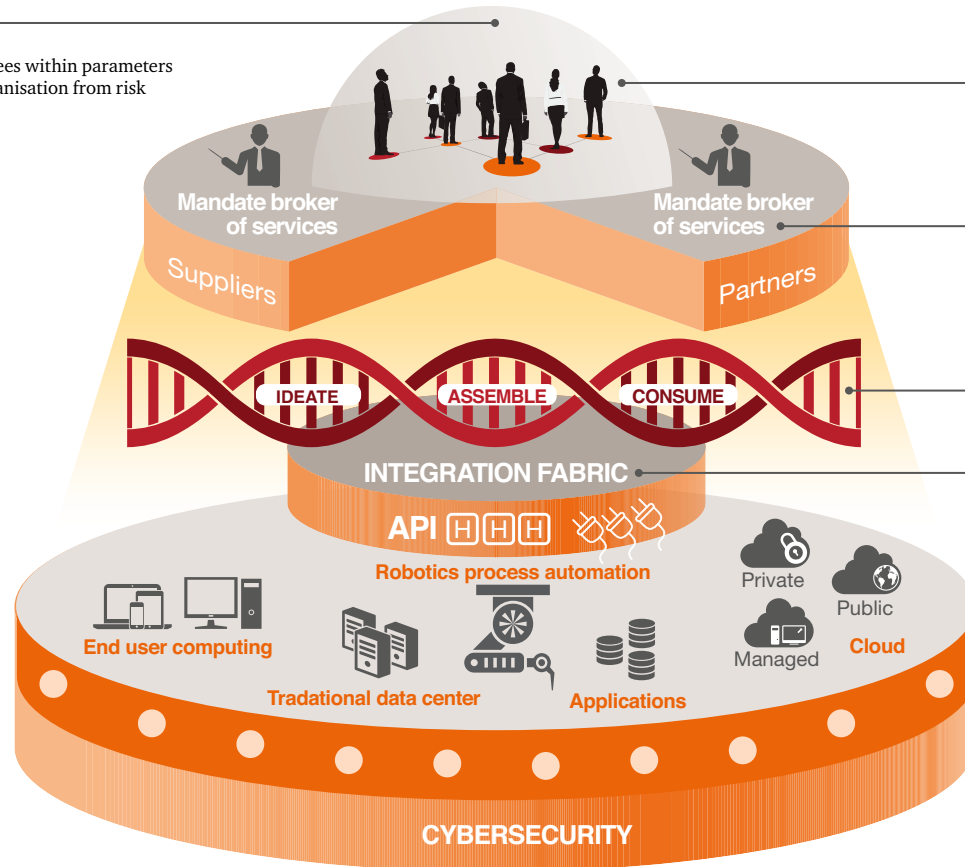
All companies have to balance where they are with where they are going. In IT, this means supporting both core 'keep-the-lights-on' functions and large transformation initiatives. Financial institutions have a unique struggle though. Among other things, these are IT-heavy companies, built over generations of technology. They have often grown through acquisition, operating with relatively static products and geographies. Typically, these operating models just are not nimble enough to support where things are headed.

The overriding principle is that financial institutions and their IT organisations must be prepared for a world where change is constant – and where digital comes first. For this to happen, it is time to really put legacy assumptions on the table. It may appear logical to continue to support core mainframe systems, given the potential disruption and perceived cost of transition to something different. But if the existing platform could be replicated at half the cost, would the logic still apply? Or at one tenth the cost?

***All companies have to balance where they are with where they are going. In IT, this means supporting both core 'keep-the-lights-on' functions and large transformation initiatives.***

### Governance

Empower employees within parameters to protect the organisation from risk



### Organisation

Professional services organisation with versatile generalists

### Mandate

Broker and orchestration with focus on innovation

### Process

Fluid and iterative assemble-to-order approach

### Architecture

Secure integration fabric with architectural guardrails and guidance

### Governance

Now more than ever, IT is expected to understand business issues and help the broader organisation achieve its goals – reshaping the brand, creating new markets, and outperforming rivals. But poor governance can get in the way. Governance is not just a control or compliance function. Ideally, it looks at how IT can support the organisation’s strategy: how decisions are made, what should be worked on and why. It helps everyone understand how much value IT creates (and for whom), measure day-to-day performance, and improve how risks and resources are managed. The right governance program keeps both business and IT initiatives on track. Finally, it provides a framework for dialogue that links business and technology capabilities, furthering organisation-wide goals. An effective IT governance program will not make up for a bad strategy, but it can help everyone work together to get the most out of IT investments.<sup>31</sup>

<sup>31</sup> We have discussed IT governance in greater detail in our FS Viewpoint, “Great by Governance: Improve IT performance and value while managing risk” (<https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/information-technology-governance-improvement-pwc.pdf>)

## **Mandate**

Even the nature of the 'keep-the-lights-on' vs. reinvention distinction is changing, because business-as-usual is no longer usual. The traditional IT group will keep existing capabilities moving, but this will start to look more like a sophisticated supply chain function than a manufacturing operation. In this view, IT success will depend on brokering and orchestration. Because information will increasingly be processed anywhere, financial institutions will need to manage the flows and processes that occur within your facilities as well as across domains. Switching can be automated, but humans will need to think through the exception handling, provisioning, billing and more.

## **Organisation**

Increasingly, financial services and FinTech are becoming inseparable, putting IT into a critical position. A product team may want to build visualisation and AI logic into its customer service function, but it is not qualified to assess how to do it, let alone how this would work with the rest of the IT infrastructure. So, along with its new revised supply chain mandate, your IT team will also need to advise marketing, sales, operations, product management and other business functions, either by embedding or aligning facilitators. IT will require specialists with expertise in everything from data analytics, robotics, and user-experience design to

cyber-security and integration. These specialists will need to be able to consult with the business in order to better understand what the business is trying to accomplish and agree on the best way forward. Similarly, IT will likely be the ones who help business teams become more comfortable with new forms of AI-driven decision making. Huge amounts of data will be available, but it will not help you without the resources to extract meaningful conclusions. Firms will turn to IT teams for non-IT skills too; there is no way to separate out project management and risk management. And, of course, all individual projects will need to be consistent with the overall IT and business strategy.

## **Process**

It is no surprise that the rate of IT change is rising quickly – or that FinTech has raised the ante. Expect even more by 2020, as deployment gets cheaper and connectivity continues to scale. Unfortunately, most financial institutions already struggle to keep up, and process is a key part of the problem. Fortunately, there are ways to work faster across the full range of steps that convert ideas into technology services, by borrowing the same techniques that first sped up the development process. We encourage teams to look at four broad areas where processes often break down under pressure.

- **Flow:** are the tasks, activities and outcomes clearly defined, staged and delivered?
- **Resilience:** have you anticipated how you will need to flex as a result of mistakes, faults, attacks or failures?
- **Insight:** do you have adequate visibility into everything that you are doing? Is how your services are actually being used tied into real-time visibility?
- **Culture:** are you oriented in a way that promotes collaboration and trust with your stakeholders?

## **Architecture**

In 2020, hardware, software and data could reside anywhere. You will be expected to make a virtually limitless combination of inputs and work together, quickly and securely. For this to happen, you will need to (1) anticipate it, (2) make sure that your infrastructure is aligned with applications so it can scale up or down in real time, and (3) be prepared to integrate anything. We have come a long way from the early days of middleware; we now have higher expectations and demands for systems integration. This allows new flexibility in how financial institutions interact beyond their traditional borders, and it is a key part of updating the operating model. We cover this in more detail in #4, Prepare your architecture to connect to anything, anywhere.

## Slash costs by simplifying legacy systems, taking SaaS beyond the cloud, and adopting robotics/AI

*One of the starkest differences between a legacy financial services institution and a FinTech upstart comes down to fixed assets. Incumbents carry a huge burden of IT operating costs, stemming from layer upon layer of systems and code. They have bolted on a range of one-time regulatory fixes, fraud prevention and cyber-security efforts, too.*

The ever-spreading cost base leaves less budget available for capital investment into new technology, driving a vicious cycle of increased operating costs. This is in clear contrast to the would-be disruptors, who typically have far lower operating costs, only buying what they need when they need it.

It does not have to be that way. In fact, from our experience working with a wide variety of clients in banking and capital markets, insurance and asset management, we think many financial institutions are spending up to twice as much as they need to on IT.

While every company is different, we generally see large savings opportunities for firms that do the following: simplify legacy systems, adopt an aggressive SaaS-based model and deploy robotics and AI-based automation.

### **Simplify legacy systems**

Legacy core systems and their related integration architecture are expensive to maintain and complex to modify. They also make it hard to stay ahead of changing market needs, given how long it takes to develop and release functionality changes and upgrades. At financial institutions, this is made worse because of the need to maintain

extensive branches and sales forces. So, legacy systems may be limiting your ability to roll out new competitive features or service offerings, and they are also limiting the ability to compete on cost.

The key question for core systems and infrastructure executives: how to offer the best services to the business at the lowest cost? To stay competitive, this will invariably mean that they will selectively decommission legacy systems and integration infrastructure. They will also need to develop new capabilities that run in parallel. We are hardly suggesting that this is a trivial problem; at many larger financial institutions, this could involve a three-to-five year timetable. These initiatives are capital intensive and they force a firm to decide if they will be buyers or providers of core services. But this is all the more reason to act now, because waiting to start a three-to-five year transition until 2020 could be disastrous.

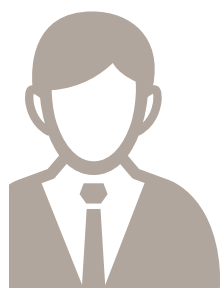
In some cases, FinTech will drive simplification. For example, as we discussed earlier, blockchain has the potential to shake up the financial services industry specifically because it eliminates entire categories

of work. By replacing outdated systems, blockchain could remove costs associated with an entire layer of overhead

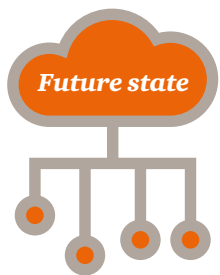
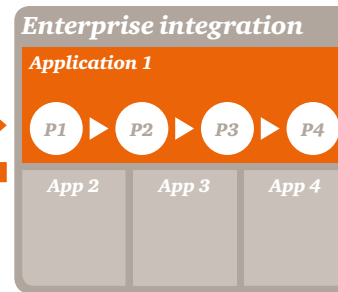
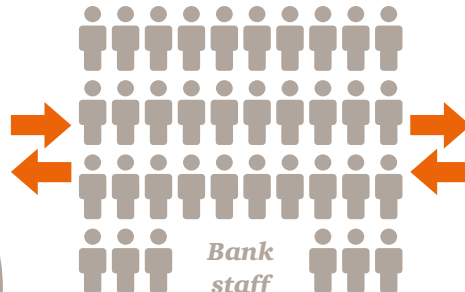
### **Adopt an aggressive SaaS-based model**

With the proliferation of network end-points, we now have access to an unprecedented amount of data. Enterprise architects see the cloud as a way to access actionable customer information on a large scale, providing insights across geographies, brands and products. And because the cloud can help break down data silos across customer channels and marketing service providers, companies often find that it reduces fragmentation and the overall cost of IT ownership. In theory, it allows a firm to break out of the organisational structures that legacy systems have helped create. But this can only happen if IT can make a disparate set of hardware, software, data and networks cooperate.

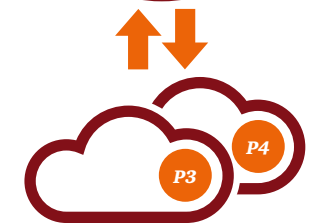
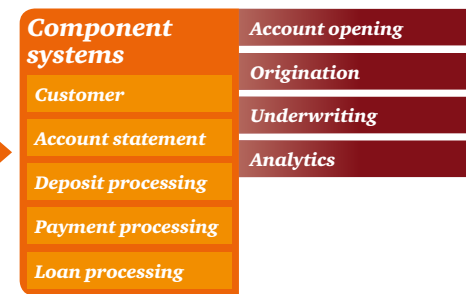
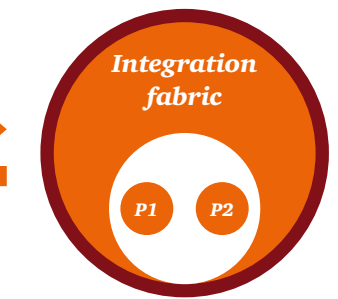
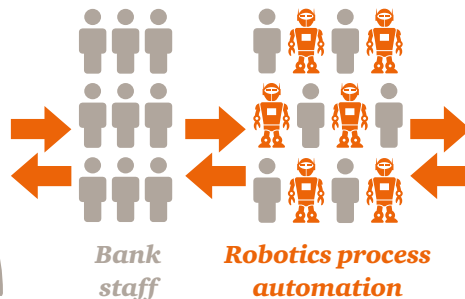
Fortunately, there has been a revolution underway, reshaping the way we think about systems integration. Better still: the cost-savings from switching to cloud-based computing can be dramatic. In fact, one of the drivers behind the public-cloud-becomes-



**Current state**  
Human-centric business processes contained within the walls of enterprise and constrained by monolithic and complex legacy core systems.



**Future state**  
Human and robotics-enabled business processes that reside within the enterprise or in cloud, liberated by component-based modern core system.



the-dominant-infrastructure-model trend is how much cheaper it is than maintaining a legacy, physical infrastructure.

These days, the concept of service-oriented architecture can be used more broadly than ever, starting with how systems are linked. We encourage you to think big: essentially, setting expectations for a systems design that allows IT to plug anything into anything. Core systems of record and processing will need to plug into an integrated architecture fabric. Cloud-based platforms will allow

financial institutions to bring innovations to market quickly and test and adapt as they go. These developments provide many opportunities to reduce costs, through economies of scale and new application support models.

**Deploy robotics and AI-based automation**

Our estimates suggest more than half of the activities people are paid to perform can be automated by adopting advanced robotics and AI – either now, or surprisingly soon.





In the United States, these activities represent about US\$2 trillion in annual wages. And while many observers think of automation primarily affecting low-skill, low-wage roles, we have seen that even the highest-paid occupations in our economy can be enhanced through automation. As we have said, these technologies are likely to unleash a wave of re-shoring, as firms discover that this approach is even cheaper than outsourcing or offshoring. (Indeed, this is also linked to Asia's rise as a centre of technology-driven innovation; the emergence of Asia's middle class may drive up costs, making Asian outsourcing less appealing to Western buyers.)

The growth of robotics and AI automation is not a matter of 'if'; it is a matter of 'when'. As such, we strongly urge financial institutions to act now. Look for opportunities to selectively pilot the

advances that are being made in robotics and AI technology. By learning now about the technical and culture issues, you will be able to gradually increase adoption across the enterprise, rather than doing it under duress.

Finally, we note that robotics and AI will require new skills in the teams that support them. You will need to find or develop people with enterprise and integration architecture skills who can bring together legacy systems with the new generation of cloud services in a flexible and resilient way. Similarly, teams with robotics and AI solution architecture skills to deploy automation effectively will be required. External contractors can be a way to augment internal staff, allowing companies to adjust headcount numbers as the legacy architecture is gradually replaced and resources are shared across the organisation.

***Our estimates suggest more than half of the activities people are paid to perform can be automated by adopting advanced robotics and AI—either now, or surprisingly soon.***

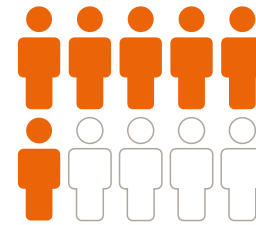
## Build the technology capabilities to get more intelligent about your customers' needs

As we have noted, customer intelligence – and the ability to act in real-time on that intelligence – is one of the key trends affecting the financial services industry, and it will drive revenue and profitability more directly in the future. As this happens, many of the attributes that drive today's brands, from design to delivery, could become less important.

By 2020, we expect that the 'new normal' operating model will be customer- and context-centred. That is, companies will change the way they interact with their customers based on the context of the exchange. They will offer a seamless omnichannel experience, through a smart balance of human and machines.

This will require the integration of massive amounts of situational data, much of it from mobile sources – smartphones, sensors, wearables and so on – and the ability to tie it to operational data such as transaction history and risk profiling. If that is not difficult enough, you will need to make these connections in (or near) real-time, so you can deliver 'next-action' recommendations and advice. Until now, most financial institutions have focused on building their mobile presence. Going forward, we expect market leaders to build on this foundation to deliver in-the-moment information, advice and decision-making power to their customers. This represents an important shift. Mobile originally developed as a nice-to-have add-on to electronic banking. However, advances in networks and mobile devices have flipped the hierarchy. Now, you need to adopt a mobile-first view of features and development.

*PwC's Retail Banking 2020 survey indicates a growing awareness to develop a more customer-centric business model, but a significant gap in preparedness remains.*



**61%**

of bank executives say that a customer-centric model is "very important"



**75%**

of banks are making investments in this area (this pattern is consistent globally)



**17%**

Only feel "very prepared"

## Understand the natural limits of artificial intelligence

Artificial intelligence will transform customer interactions, and all users – across companies, market segments, and individual customers – will value different things. But two issues will be common to everyone, regardless of where they fall in the financial services industry: privacy and risk. For financial institutions that integrate AI into business processes, these need to be at the top of any priority list.

AI has huge potential because of its ability to learn and adapt. But this introduces new kinds of risk, depending on how much autonomy the systems are given when they make decisions. Accordingly, it is critical to have a clear strategy on what role AI will have and what checks and balances to maintain over your systems. This raises some important questions: Will humans need to make ultimate decisions outside of certain parameters? Will there be spot checks on AI decisions? How will AI systems be iteratively tested and upgraded? From circuit-breakers to configurators, systems can spiral out of control quickly without proper rules. These are complex issues; to strike the right

balance between AIs risks and rewards, you will want to engage executives across the business.

### ***Protect privacy, or else***

Privacy is another critical concern.

Customers must feel their information will be used to benefit them, and not in a way that intrudes upon their private lives. This is a sensitive topic; in fact, if handled poorly, privacy violations could invite a heavy-handed regulatory response. Companies will need strong operational controls in place so data is not being misused in – or across – business units. In fact, as we have seen, regulators are getting more comfortable with how they use technology to enhance supervision. The US CFPB, for example, recently announced its first enforcement action (against a FinTech payment company) related to privacy and cyber-security, and regulators are likely to step up these efforts in the future.

### ***Use the power of analytics to give a customer more***

As data proliferates, we encourage executives to explore how to get the most value out of what they hold: what information is already being collected, what form it is in, how (or if) it is being analysed today, how it can be adapted to address customer needs and reduce costs and more. These are key and ongoing questions for any business, and

it is why many financial services firms are appointing chief data officers (CDOs).<sup>32</sup>

When used properly, AI and data analytics together can help financial institutions understand their customers more than ever before. (And this matters, because FinTech start-ups will be going down the same path, and the first one to get it right will earn the customer's loyalty.) These new tools provide access to rich, compelling and personal service to customers. The service is personal because it draws on individualised data about a consumer's behaviours, which is then used to customise product offerings for that specific user. The days of designing products based on broad demographics or survey groups are fading fast.

This user experience will occur anywhere: either in a branch, online, or through a customer's mobile and wearable devices. In fact, because digital has become mainstream, we now see consumers starting to turn to mobile devices as their preferred tool for making online and proximity payments, rather than credit cards or banks. These new capabilities, with seamless transitions among them, are the essence of what we mean by an omnichannel experience: customers will be able to start a transaction in a browser on their laptop, continue it on a mobile device, walk into a branch with their tablet, and be greeted by name without needing to explain why they have come in.

These tools go far beyond the customer interface; they even have implications for existing physical infrastructure. For example, as a bank, it is important to consider which locations will house your 'flagship' and full-service branches and where to locate the assisted, self-service (or even robot-enabled) branches. The long leases on many branch sites mean that this service map needs to be drawn up today to be ready by 2020.

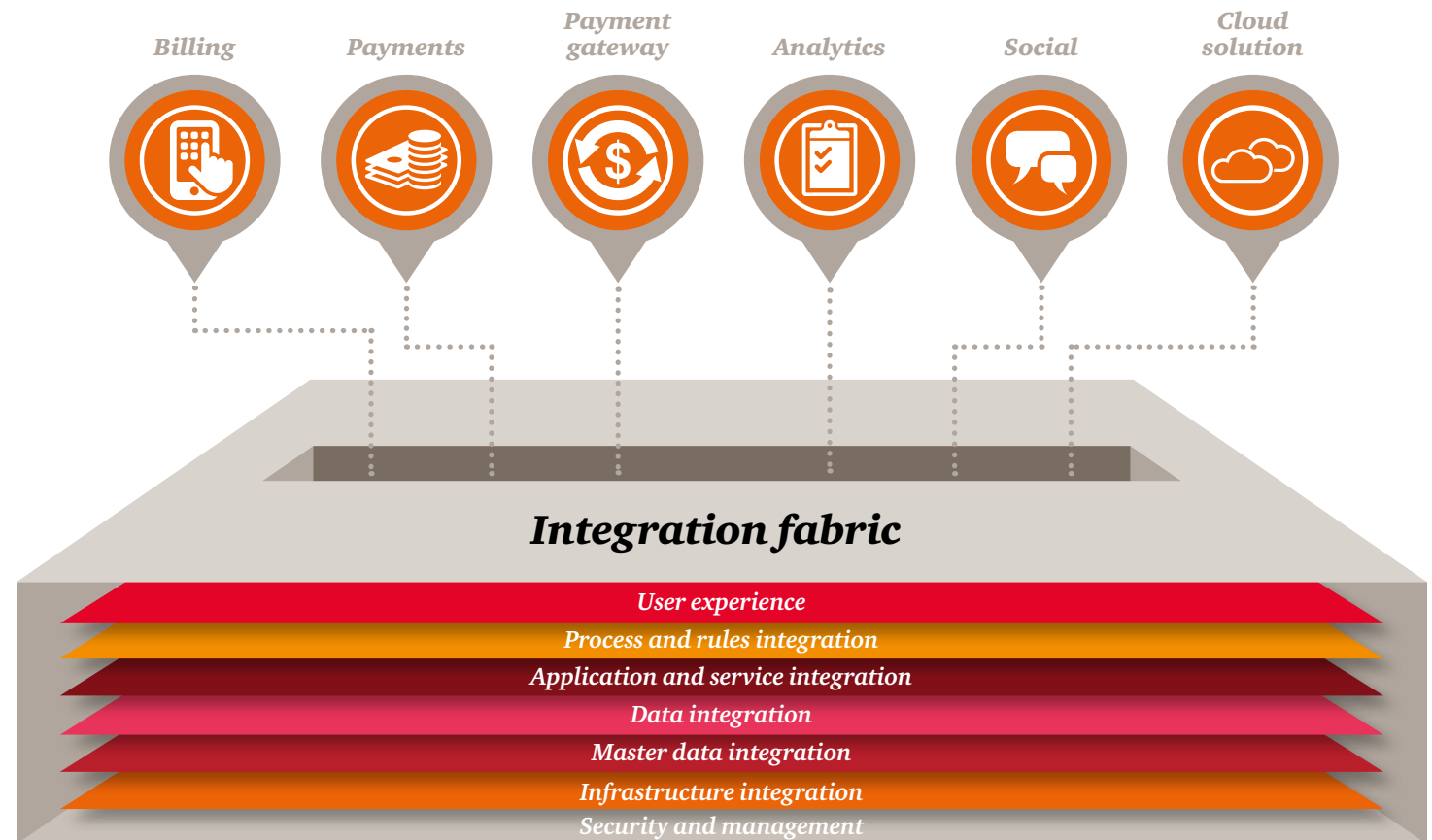
Finally, as these technologies advance, financial institutions will quickly bump into some human capital limitations. AI already has practical implications and companies need to be investing in it today. We are already seeing a high demand for AI experts. Companies will need to consider how they will address this talent gap in the short-term, even as they develop strategies for the long-term.

---

<sup>32</sup> See our recent paper, "Great Expectations: the evolution of the chief data officer," for more information on this trend. <https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-chief-data-officer-cdo.pdf>

## Prepare your architecture to connect to anything, anywhere

The FinTech trends that we have discussed in this paper, from the cloud and peer-to-peer transactions to customer intelligence and cyber-security concerns, all rely on the rapid transmission and assimilation of data. Today's systems do this too, of course, but without the scale or resilience that the future will require. To stay cost-competitive, and to have the flexibility that innovation requires, financial institutions will need to update their infrastructure to make it more agile and responsive. You will need an architecture that can bend as requirements change and interact with data and systems that could be anywhere – because they will be. And at most financial institutions we know, this will require a significant reorientation.





Here are just a few of the endpoints that will need to coexist and cooperate:

- Enterprise databases, data warehouses, applications and legacy systems
- Cloud services
- Business-to-Business (B2B) connections, linking to comparable systems at partners and suppliers
- Business-to-Consumer (B2C) connections, linking to apps, wearables and mobile devices at an individual user level
- Bring-Your-Own-Device (BYOD) connections, using an enterprise mobility strategy to link to employees and contractors
- Third party 'big data' sources
- IoT sensors

The systems are diverse, and they are getting more complex by the week. Now, financial institutions will need to layer on a more sophisticated view of federated identity management, because companies will be dealing with new classes of users. Systems architecture can be the key to balancing control and accessibility. That is, the way you assemble the technical building blocks can protect your institution against cyber-threats without adding needless barriers to discourage interaction.

### **Work with the cloud**

To work this way, you will need to manage a lot of different forms of data, and much of it will be beyond your control, in forms and locations that you have not anticipated. The cloud offers a good use case. For example, you may turn to hybrid cloud brokers to help you improve the way you aggregate data, analyse activity, and react to user behaviour through a single customer view for customer banking. This integration is essential for front office applications and channel architecture domains that expose such services to your customers. This is another reason that cloud computing is becoming so dominant: it makes it much easier to manage and analyse 'big data'. Internally, this also allows technology teams to develop and test solutions in the cloud without having to rewrite and test code on dedicated machines. It allows businesses to design and deliver their products more quickly. For CIOs, this also significantly reduces capital and operating expenditures: a perennial challenge for all IT departments.

### **Make an API plan**

Application programming interfaces (APIs) have come of age in financial services. Similar to online or mobile banking today, nearly all financial institutions will provide external APIs in the future. (In fact, directives from regulators in Europe and the UK mandate access to customer data and accounts under certain circumstances.)

For example, banks will rely heavily on payment APIs to facilitate e-commerce. The global industry has been standardising the way it handles payments messaging and remittance meta-data. These standards will define consistent structures for individual messages, promoting interoperability and helping developers define API requirements.

But APIs require that financial institutions think differently about strategy, given that the transactions that call them may come from third parties. The payment transaction may become more of a commodity, but the data itself that is captured in the process could drive drastically different business models. New business models will influence how firms think about the data models they use, how they aggregate information from other sources, the support structures they implement and more. This is not just an issue for business strategists; it has clear technical implications for the teams who are responsible for doing the work.

### **Issues in planning a hybrid integration strategy**

As financial institutions move to adopt more of a hybrid integration strategy, there are several factors to consider, including how hand-offs works, how data moves and how to address security concerns.

- **SaaS data policies:** Financial institutions should work with their vendors to understand the data policies and limitations of APIs. This will let you consider what services can be exposed and consumed, at the user interface (UI) level and beyond.
- **Transitioning data to the cloud:** There are various ways to move data into a public or private cloud environment and financial institutions should understand the advantages of each strategy. There are cost, risk, and time trade-offs involved, whether you choose a parallel, incremental, or external cross-referencing transition method.
- **Security:** There is always an element of risk when exposing data for system consumption. Under most circumstances, we recommend that financial institutions only use an integration approach where data is exposed to trusted systems using a private cloud infrastructure.

Of course, if you want to implement a hybrid integration strategy effectively, you have to decide what your end-state application landscape will look like. This is true even during a transition period, where some banking services will come from cloud-based SaaS providers and others will come from in-house. So, for example, a bank might invest in an enterprise service bus



(ESB) infrastructure as it starts to open up its systems; this alone can offer material reductions in cost and time for a digital banking upgrade project.

Given the FinTech trends we have discussed, we think you will want to build your hybrid integration platform assuming true interoperability across multiple products or suites. By 2020, this will be the most effective way to share common infrastructures and maintain architectural integrity with native, on-premises data integration.



## You can not pay enough attention to cyber-security

*Financial institutions have been addressing information security and technology risks for decades. But a growing number of cybersecurity 'events' in recent years has shown that the traditional approach is no longer good enough. In fact, in PwC's Global State of Information Security Survey 2016, we found that there were 38% more security incidents detected in 2015 than the year before.<sup>33</sup>*

Many financial institutions still rely on the same information security model that they have used for years: one that is controls- and compliance-based, perimeter-oriented, and aimed at securing data and the back office. But information security risks have evolved dramatically over the past few decades, and the approach that financial institutions use to manage them has not kept pace.

### **Finding the weakest link**

The Internet of Things (IoT) presents a good example of the pending challenges. On the one hand, IoT will play an increasingly important role in the way that businesses collect and aggregate previously inaccessible data, leading to growth and innovation. In financial services, we have already seen IoT growth in payments (wearable technology that allows customers to make mobile payments via watches or fitness trackers), insurance (telematics technology that enables insurers to monitor customer driving habits and provide discounts to safe drivers) and banking. At the same time, IoT presents some 'weakest link' challenges, because many IoT devices do not support the implementation of strong security controls. These insecure interfaces, with billions of potentially vulnerable devices connecting

to a corporate network, can increase the security risk for your critical data and infrastructure.

And IoT is just one way in. There are more layers than ever, and this has expanded the attack surface – the points through which adversaries attempt to access data. In a sharing economy, there may be many different providers touching a disaggregated transaction that once would have been handled by a single bank. And because digital has become mainstream, the technology perimeter has moved far beyond traditional control boundaries, making information security exponentially more difficult. Meanwhile, well-funded threat actors are launching technically sophisticated assaults that, when successful, can siphon off valuable data undetected for months, or even years.

### **Do not forget physical security**

With all the risks posed by new, virtual entry points, it is easy to get distracted and neglect the importance of physical security management. Physical and virtual security must be considered together. While information is virtual, it is stored in a physical location, and skilled hackers will find the weakest link, either physical

or virtual. We have found that a surprising number of firms do not put enough effort into identifying their infrastructure weaknesses, let alone remediating them; this compromises even the best cybersecurity program.

### **The role of management**

Cyber-risk management is complex and rapidly evolving. To stay ahead, you will need executive management engagement, ongoing governance, risk management techniques, threat correlation, collaboration throughout the organisation and adoption of a new operating model. You are not fighting off a single threat, or even a single class of threats; next week, you could see an entirely new attack vector. So, the true goal of cyber-risk management is to build resiliency. You need to make sure that your systems and operations are designed to detect cyber-threats and respond to cyber-events, so you can limit any business disruption or financial losses.

In the financial sector, this takes on an added dimension, because the perceived rewards for the hackers are so appealing. In fact, a financial institution's cyber-risk management program should be one of many components of the overall business risk environment that

<sup>33</sup> PwC Global State of Information Security Survey 2016, <https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>

feeds into the enterprise risk management framework. You may not be able to eliminate all cyber-risks, but you have to be able to manage those risks through an informed decision-making process. Instead of seeing a wire fraud incident or DDoS attack as an isolated incident, we encourage looking at them as tips of an iceberg. This is serious enough that executive management teams should use their leadership role to set the proper tone and structure to enable cyber-resiliency across their organisations. Frankly, if you do not mitigate cyber-risks effectively, you could jeopardise the ongoing success of your whole institution.

We recommend executive management focus on the following:

**Proactively manage cyber-risk and regulation:** Treat cyber-risk as a strategic business issue and focus on becoming cyber-resilient. Develop specific cyber-risk appetite, both corporate-wide and by business. Understand and incorporate baseline regulatory requirements into current environment, and include cyber-protection as a key priority in the organisation's overall regulatory program.

**Build and execute a strategic cyber-security roadmap:** Organisations should understand the evolution of cyber-threats and threat actors on an ongoing basis, leveraging cyber-threat intelligence from a number of internal and external sources. They should then develop and execute a plan to mitigate exposure to these threats, making adjustments to their risk control posture as the threat landscape changes.

**Establish a commercially reasonable cyber-security capability:** Cyber-protection programs should be tailored to the risk profile of the organisation as well as the expectations of clients, shareholders and regulators. Organisations should understand how they compare to their peers and relevant industry standards. In 2020, as more services will be provided by vendors, cyber-security programs will need pay more attention to third parties, too.<sup>34</sup>

**Develop a world class cyber-response:** Organisations should adopt an enterprise risk management approach, focusing on incident response and crisis management as a key priority. Scenario planning should take place with the executive management team and attack simulations should be conducted on an ongoing basis. The goal should be cyber-resiliency: being able to defend against and respond to cyber-risks that have become a fact of life.

**Acquire, develop and retain key talent:** The organisational model for cyber-protection should be adjusted to focus more on enterprise and business risk management. Organisations should then determine the required skills, capabilities and resource requirements before hiring the necessary talent to fill any gaps.

**Align cyber-security team with business risks:** Establish governance and reporting lines for cyber-security, reflecting its role as a technology risk function. Make the executive team accountable for making decisions about IT risks. Segregate broader budgeting and funding from the technology budget. Develop appropriate linkages to both the risk and technology functions.

### ***New tools for fighting cyber-crime***

With the right tools in place, financial institutions can improve their ability to manage cyber-risk. For example, financial institutions can deploy state-of-the-art data mining tools and other technologies to detect anomalies in security and fraud applications, using data from both structured and unstructured sources. We also note that while the trend toward cloud-based services can introduce new risks, it can also support a financial institution's defensive strategy. Cloud-based cyber-security can improve intelligence gathering and threat modeling,

block attacks more effectively, help different teams (or organisations) collaborate and learn more effectively, reduce the lag time between detection and mediation and create secure communication channels. When you factor in potential cost reductions, cloud-enabled cyber-security becomes all the more compelling.

Cyber-security is a large problem and it is not going away. Despite prevention and authentication efforts, we can virtually guarantee that anomalous and unauthorised activity will continue to occur. But with the right tools in place, you can see it when it happens and remediate it quickly. With a structured approach to cyber-security, financial institutions will also be more prepared as threats evolve. This will help them to avoid financial damage, negative publicity, and loss of customers' trust, any of which could have catastrophic effects.

---

<sup>34</sup> For additional information, see PwC's "Significant others: How financial firms can manage third party risk," <https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-third-party-vendor-risk-management.pdf>. May 2015.

## Make sure you have access to the necessary talent and skills to execute and win

*As financial institutions look to the future, one of the biggest hurdles will have nothing at all to do with technology. For years, traditional financial institutions have designed their offerings from the inside out: ‘this is what we will offer,’ rather than ‘what do our customers want?’ But this model no longer works. And the skills and interests of today’s IT team members and third-party talent may not be up to the challenges of tomorrow’s technical environment, where partnering with customers will be essential.*

### Looking backward, looking forward

Financial institutions in general simply do not have the internal knowledge and expertise they will need to implement a ‘what do our customers want?’ approach. For example, a COBOL programmer who maintains a core banking platform may not have the skills or interests to learn to code artificial intelligence applications. From our discussions with senior IT executives across the industry, it is clear that many executives, non-IT staff-members, and even technical personnel do not have the skills needed to build and operate an effective digital channel offering.

Financial institutions are starting to realise they will need talent with very different skills by 2020. On the surface, this might mean finding more industrial engineers for robotics work, or retraining underwriters to do higher value work once AI is used to automate certain existing functions. But the issue runs deeper than developing a different competency model.

First, you need to understand what is already working and what needs to be done differently. This might involve changes

across the human capital strategy through revitalised recruitment, learning and development, partnering and cultural initiatives. Typically, this could include efforts such as:

- Recruiting expert talent from other technology organisations and think-tanks, rather than staying focused on recruiting from within the financial services industry
- Developing robust learning modules to enhance the skills of executives, IT – and non-IT staff
- Taking more active steps to create and foster a culture of innovative thinking and talent development
- Engaging more extensively and creatively with third-party sources of talent, including the use of “talent exchanges”

### Learning from Asia

One way that financial institutions can address this priority: turning to the East, taking advantage of Asia’s emergence as a key centre of technology-driven innovation. In some cases, financial institutions and FinTech companies in Asia are already addressing issues described in this paper,

and they may serve as a good resources for others. We also expect that some firms will establish Innovation Hubs in Asia, either looking for opportunities to learn from others’ breakout strategies or looking for talent with specialised software and engineering skills that may not be readily available at home.

### Different generation, different values

Just as changing demographics are reshaping customer attitudes, we see them changing employee attitudes as well. This has important implications for financial institutions as they look to attract and retain a new generation of talent. Incentives that once appealed to top performers may become less important or not relevant at all. For example, to succeed with the emerging cohort of millennials, financial institutions will need to reexamine what they offer employees in terms of compensation, benefits, flexibility (of both time and location), development opportunities and more. Will a bank be able to lure away a robotics engineer from a FinTech upstart using the current incentives? If not, what would it take? The answers may not be intuitively obvious.



### Current state

Identify skills gaps so you can transform your organisation from a current state where learning, recruiting and culture are not enablers of innovation and collaboration...



### Future state

...to a future state in which learning, recruiting and culture help to drive innovative thinking and collaboration in a digital financial services industry



Organisation focuses recruiting efforts primarily within the industry, from other competitor banks and financial institutions

Recruiting



Firm delivers typical, bank-focused learning and development training modules on existing and archaic systems, platforms and processes

Learning



Culture based primarily on past objectives and instead of forward-thinking drivers

Culture



Rethink the talent sourcing process by:

- Seeking creative candidates outside the industry at think-tanks, technology firms, and other non-traditional sources
- Re-branding hiring strategies to emphasise opportunities to work with innovative technology as well as competitive compensation
- Considering flexible workforce alternatives, like talent exchanges and project-based hiring
- Partner with third parties to get needed talent on a short- or long-term basis

Recruiting



Facilitate focused on-the-job training, mentoring, and peer coaching by:

- Implementing communities of interest and voice of customer initiatives to drive digital banking information sharing
- Partnering with skilled professionals, technological leaders, educational institutions, and pertinent professional association to develop/deliver relevant training materials

Learning



Promote a culture of collaboration and innovation by:

- Encouraging employees to contribute ideas to enhance and advance the organisations as part of innovation campaigns and social media driven initiatives
- Using guided sessions to find and share best practices, and benchmarking against a hyper-competitor to invigorate thinking
- Developing an Innovation Centre of Excellence to focus on driving imagination, creative thinking, and inventiveness more deeply into the organisation's culture

Learning



Another trend that financial institutions will need to address is the growing preference for flexibility and entrepreneurship among many in the labour force. In the United States, for example, the US Chamber of Commerce has found that 27% of the labour force is currently self-employed<sup>35</sup>, and some believe that this ‘contingent workforce’ could rise to 40% or more within several years. Practically, for this reason alone, financial institutions will need to adopt a ‘talent exchange’ mindset, leveraging part-time and/or self-employed individuals in a creative manner. This may range from bidding out specific tasks or work to expanding the use of seasonal or temporary workers. Of course, this will introduce challenges around culture and quality, and this will introduce new opportunities as well. For example, we might see employers using online platforms to manage confidentiality and legal risks in new and creative ways.

### **Getting better results from performance management**

Ideally, performance management should engage and motivate employees. This process – setting expectations, observing and providing feedback, and appraising results – should encourage risk-responsible behaviours and a focus on the “right” things. Human capital strategy is also key to

achieving broader business goals: making the customer the top priority; building a healthy risk culture; improving the business; promoting innovation; and engaging in corporate responsibility.

Financial institutions should look to improve the traditional performance management model so they are inspiring their teams to do great work:

- **Goal setting:** translate purpose and values to link them with common enterprise goals
- **Real-time feedback and periodic check-ins:** provide on-the-job feedback and coaching; enhance transparency through informal peer and colleague feedback
- **Annual reviews:** manage year-end expectations with more focus on future state performance
- **Integrated performance and rewards:** create clearly defined and evidenced links between performance ratings and rewards outcomes
- **Include all team members:** expand feedback and performance management processes to third-party labour and partners

As new forces impact the industry and attitudes toward work continue to change, some of the attributes that have benefitted financial institutions in the past (such as ‘we are a large, stable employer’) may lose their appeal. Refreshing your firm’s approach to recruiting, learning and development, and culture may offer an effective (if low-tech) way to address issues that FinTech has brought into the open.

<sup>35</sup> <https://www.uschamberfoundation.org/reports/millennial-generation-research-review>

# Conclusion

*Financial institutions have a lot on their plate: emerging competitors, shifting demographics, rising customer expectations and changing regulations. Technology offers solutions, allowing financial institutions to cut costs and become more efficient at what they do. But this is tricky, because it is a classic ‘limited time offer’. Most technology is not proprietary, so it is a bit of a race: if you blink, you might find that your competition has already built up advantages that are now harder for you to match.*

As we see it, most financial institutions are currently focusing much of their IT attention on the short-term. We understand this: on any given day, there are fires to fight, with regulatory fixes, fraud attempts, budget discussions and so on. But with the trends we have described here, you will not want to look up after a few more years of short-term thinking to notice that the calendar says “2020.”

In fact, we think that many financial institutions are looking at all of these issues, to some extent. But they are often looking at them reactively, in silos, without

coordination. In other cases, we see CIOs who are hesitant to ‘bite the bullet’ on big projects, figuring that they can limp along with older systems for another year or two until technology stabilises and funding may be available. Unfortunately, we think that strategy will become more dangerous as time passes. After all, a core simplification project really can take three-to-five years. Devising a talent plan for 2020, and getting the right staff in the right places? Creating an innovation hub – possibly in Asia, or redesigning your architecture? These can take several years too. To be competitive in the game in 2020, there are steps to start taking now.

Here is what success looks like: when the next change comes, you are ready. You have the models and architecture in place to quickly understand, leverage, and operationalise emerging technologies without creating chaos in the organisation. And you are able to do this while you ‘keep the lights on’ at a fraction of today’s expense.

This is achievable. In fact, it is what the leaders of 2020 are preparing for right now, on their own and with outside help.

Each financial institution will respond to these trends and priorities in their own way, largely dependent on their unique position in the market, desired path forward, brand positioning, regulatory circumstances, and organisation capabilities.

For our part, we encourage institutions to take a realistic view of their situation – holistically, across the entire IT organisation – to understand the current state, the desired state, and how to get from here to there. With 2020 rapidly approaching, this is no time for a piecemeal approach.

At PwC, we work with clients to build IT 2020 Readiness Programs. These start with a strategic review that lets CIOs and other executives understand where they stand, and what they will need to support business strategy by the end of the decade. We examine an institution’s operating model,



human capital approach, ability to innovate, and ability to execute, among other things. We also take into account what we know about the IT environment of 2020: the integration themes, advanced analytics, core and digital systems, cloud adoption, talent flexibility, and innovation culture that will drive our world.

With the results of such an 'IT Healthcheck' in hand, you can work to determine the gaps you will need to close. With these guiding principles, you can establish the consensus you will need to support change.

Finally, you will want to make a pragmatic roadmap for how you will close the gaps identified. We work with clients to reconcile these against current initiatives, re-prioritise as necessary, and define the funding model. This helps everyone understand how they will execute together, with alignment and accountability to achieve the 2020 vision.

We hope our perspective is helpful as you think about refreshing your own strategy for 2020 and beyond.

### ***Here are some potential questions to get started:***

- How quickly can you innovate when technologies, competitors, and markets change? Do you have a methodology in place to help you evaluate how and where you might use emerging technology like blockchain? Can you do this consistently, without creating chaos in the organisation? What is your strategy for learning from, partnering with, or acquiring FinTech disruptors?
- Does your IT team understand how they will deploy AI and robotics? Do you use systems to store, process and integrate unstructured data? When users become even more mobile, how will this change your offerings?
- Do you have a robust cybersecurity program in place? How will your program adapt to handle security related to IoT? How often do you update your approach to data privacy? What limits do you put on sharing information through APIs? How resilient is your organisation to a sustained, aggressive cyber-attack?
- Do you have a migration plan to take your on-premises technology stack and migrate it to the private (or public) cloud? What's the optimal role for SaaS, and what changes will you need to make to expand its use?
- Can you customise product offerings on an individual basis? How synchronised is your approach to omnichannel delivery? Do you have the right physical/virtual mix?
- How will you find the skilled resources you need as you shift from a physical to a more virtual infrastructure? What can you learn from competitors in other markets? How would talent exchanges and other contingent workforce projects affect your existing operations?

---

# Contacts



**Andy Symons**

Financial Services Leader and Innovation Partner

T: +64 9 355 8535

E: [andy.d.symons@nz.pwc.com](mailto:andy.d.symons@nz.pwc.com)



**Andrew Wilshire**

Director

T: +64 9 355 8024

E: [andrew.p.wilshire@nz.pwc.com](mailto:andrew.p.wilshire@nz.pwc.com)

[pwc.co.nz/fstech2020](http://pwc.co.nz/fstech2020)

© 2016 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.