UBS

US equities

Update: Beneficiaries of transformational technologies | 21 September 2017

Chief Investment Office Americas, Wealth Management
Kevin Dennean, CFA, Technology Equity Sector Strategist Americas, kevin.dennean@ubs.com; Laura Kane, CFA, CPA, Head of Investment Themes Americas, laura.kane@ubs.com

- We reiterate our view that the growth in two broad transformational technologies – digital data and smart automation and robotics – should allow companies involved in these activities to post above average earnings growth over the next decade and outperform the broader market. We also see longer-term potential for 5G wireless to enable new services and applications including smart cities, autonomous driving, and massive Internet of Things. Lastly, we view cyber-security as the key enabling technology for both digital data and smart automation and robotics. We continue to expect security spending to outpace overall IT spending.

A version of this report is available with specific security recommendations for the US onshore investors. For a copy, please consult your UBS Financial Advisor

Related research

- *Update: Beneficiaries of transformational technologies, 22 March 2017*

Identifying beneficiaries of transformational technologies

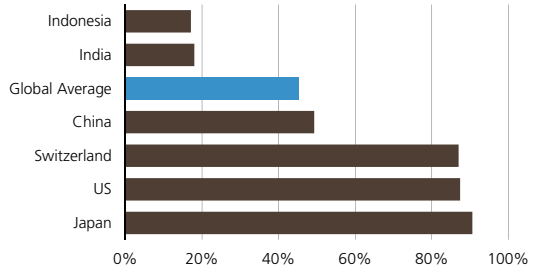
Our Transformational Technologies theme aims to identify beneficiaries of technological disruption over the next decade. The theme launched in January 2015 with a focus on digital data and industrial automation, two broad categories that we believe will be key sources of technological innovation over the next several years. Both areas have the potential to profoundly transform the structure of our economy, disrupt existing business models, and create substantial growth opportunities for those well-positioned to participate. We subsequently increased our exposure to cyber-security, which we see as a key enabler of digital data and industrial automation. More recently, we added exposure to wireless infrastructure as carrier spending likely improves in 2H17 and 5G wireless sees increasing traction in 2018. Given recent headlines, we take a deeper dive into cyber security and 5G wireless, and offer a brief review of our thoughts on digital data and industrial automation.

This report has been prepared by UBS Financial Services Inc. (UBS FS). **Please see important disclaimers and disclosures that begin on page 7.**

Opportunities in digital marketing

Digital Marketing may not be a new development, but we believe the saturation of smartphones and the increased usage of technology to analyze large untapped pools of data provide a strong tailwind for further growth. Digital Marketing has the potential to significantly increase customer interaction and engagement and improve the return on investment for marketers. A key aspect of digital marketing is its ability to analyze the effectiveness of a digital campaign in near real-time and to course correct as necessary. While digital marketing has largely been focused on internet search (Search Engine Optimization and Search Engine Marketing) and direct digital marketing, we believe non-linear video consumption (e.g., YouTube or other on demand video) will provide a significant opportunity for further use of Digital Marketing.

Fig. 1: Global internet penetration as of 2015
Internet penetration of some key geographies



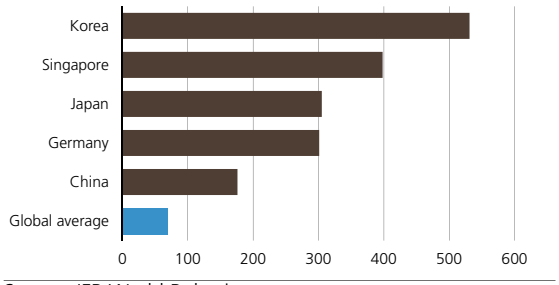
Source: World Bank and UBS

Additionally, we believe that companies increasingly understand that they have tremendous amounts of customer data and other information that can be monetized through more effective digital marketing and customer interaction. Lastly, there is an opportunity for Digital Marketing to subsume other traditional media advertising formats such as print and radio as Digital Marketing increasingly may be viewed as the primary marketing function rather than an adjacency to more traditional methods.

Industrial automation – the next wave of the Industrial Revolution

Meanwhile, we reiterate our preference for automation and robotics. Smart automation is still in its early stages of growth, and we expect the industry to grow at a mid-to-high single-digit pace over the next decade driven by the rise of industrial software. Manufacturers will need to invest in advanced automation technology to maintain profitability in the face of labor shortages and fast-rising wages in emerging markets. Further, the automation segment should continue to be supported by the rise of connected devices, collectively referred to as the "Internet of Things," which drives upgrade and replacement cycles.

Fig. 2: Robot density by country as of 2015 Robots per 10,000 employees



Source: IFR World Robotics

Cyber-security – the key enabling technology

Security underpins both digital data and industrial automation and in our view is the key enabling technology for the next wave of innovation across both information technology and the industrial sector. As more devices are connected, the so-called "attack surface" for cyber-attacks increases exponentially. We expect continued strong spending on security along with significant consolidation in terms of companies, technologies, and products.

Hacking becomes more dangerous...

At the same time, the perpetrators of cyber crime are changing. Hacking was originally the sport of "script kiddies", who were amateur hackers that were primarily interested in relatively harmless cyber-pranks to show off for their peers. As the internet proliferated, hacking became more malicious and the threat actors grew to include professional cyber-criminals, organized cyber-crime rings, state spon-

sored cyber terrorists, "hacktivists" (politically motivated, non-state hackers such as the Anonymous group), and corporations engaged in corporate espionage.

Hacking also became more dangerous and costly to victims. Rather than an annoying, but innocuous screen message, hackers began to focus on exfiltrating valuable corporate data. Customer data became a prime target and the more personal the data, the more valuable it became. While prices for stolen data vary widely, multiple press sources report that health care data can sell for hundreds of dollars, or 50x the cost of relatively simple data (e.g., name, address, date of birth, credit card numbers). Perhaps most troubling, industrial infrastructure including nuclear labs, power grids, and water systems are increasingly targeted by politically motivated cyber-attacks.

...and cheaper

Lastly, the cost of hacking has declined significantly, Continued internet adoption in regions with highly educated but severely underemployed citizens has created a large pool of willing and able hackers. Virtual exchanges allow cyber criminals to implement quickly cyber-attacks using "best of breed" malware assembled for only a nominal fee (measured in the hundreds of dollars).

Making matters worse, an increasing dearth of experienced IT security professionals exacerbates an already difficult situation. Although university programs have increased in response, it will take at least a few years before the labor supply for cyber security is adequate.

2014 was a watershed year for cyber security...

These factors finally came to a critical head in 2014. Although corporations had been well aware of the risks of cyber attacks for many years, a series of attacks that were shockingly large in scope and perpetrated by new and underappreciated sources elevated cyber security from an operational issue handled by IT department to a board level issue that was front of mind with every CEO. Furthermore, governments began to appreciate the risks as well as the opportunities of cyber warfare.

Budgets increased dramatically, with numerous anecdotal stories of "blank check" spending on cyber security becoming common. IT departments continued to be challenged by the proliferation of discrete, un-integrated "point solutions" that often created so much data that valid breach identifications were lost among the noise of false positives.

...but lead to some overspending

The "blank check", panic-induced spending of 2014 unsurprisingly slowed in 2015. However, there were other factors that weighed on security spending.

First, the continued success of cyber attacks even as spending ramped aggressively caused a re-evaluation of security philosophy, architecture, and processes. Security professionals, CIOs, and even boards are increasingly accepted that a 100% success rate in preventing attacks

is impossible. The evaluation of the effectiveness of Chief Security Officers (CSOs) and security operations in many cases shifted to response and remediation time rather than just prevention.

Second, we believe that many security operations simply paused spending to reassess their security architectures and processes.

Third, as the views on security philosophy and goals evolved, so did purchasing patterns and preferences. IT departments began to shift away from traditional defense in depth security architecture that relies on multiple, discrete security solutions that typically lack integration and require separate personnel and training to manage.

These factors combined for a slowdown in the rate of growth in cyber-security in 2015.

Growth poised to reaccelerate

However, we see the recent slowdown in cyber-security spending as largely temporary. Survey data continues to show cyber-security as a top Chief Information Office (CIO) priority. The future of cyber-security may not mirror the past, but we nonetheless fully expect cyber-security spending to be among the fastest growing segments of all of IT.

Expect significant consolidation

At the same time, the dearth of experience cyber security professionals and the operational risks presented by "vendor sprawl" is driving the industry towards consolidation. This consolidation is happening at both the product level and the company level.

At the product level, the industry is focused on so-called "platformization", which is the consolidation of previously discrete cyber-security functions onto a single hardware or software product. This has operational and cost benefits. Operationally, a so-called "single pane of glass", or the ability to manage multiple security functions and systems from one console, can help drive improved security outcomes by reducing false-positives and highlighting truly critical alerts. The ability to manage multiple security functions through a single system can help reduce the overall cost of cyber-security. Interestingly, we believe at least a portion of these cost savings are often reinvested in other parts of security.

We expect this consolidation of cyber-security technology solutions will occur both organically and through industry consolidation. Leading vendors with modern, flexible architectures that allow them to absorb adjacent security functions will gain market share on a secular basis. At the same time, we believe there will be significant M&A activity. We expect many networking and communications equipment companies will continue to see cyber-security as a natural fit to their own markets, with the added benefit of the higher-margin, higher recurring revenue nature of many security products. Legacy security companies, such as many anti-virus companies, will also likely be acquisitive in an attempt to reinvigorate their growth rates. Private equity has been fairly active in cyber-security and will likely continue to be buyers of security assets.

The changing security landscape
To be sure, prevention is still viewed as the first defense in cyber-security. However, it is no longer the only defense. The industry is responding with an increased focus on event and behavioral analysis, threat intelligence sharing, and a higher level of security automation and orchestration.

Event and behavorial analysis relies heavily on Big Data to collect and correlate information across various IT systems (storage, log-on, networking, files). This provides a more complete picture of the attack and allows security professionals to better understand not just the attack, but the means, motive, and source of the attack, and allow security organizations to better understand the attack and increase preparedness. Lastly, this information is often shared to the benefit of the overall user base.

5G - Sooner than you thought, different than you imagined
5G is the next phase in the evolution of wireless technology. As with prior generations, 5G will enable faster wireless broadband speeds at lower costs. Importantly, when fully implemented, 5G is expected to enable new applications and services such as autonomous driving, massive IoT, and telemedicine, among others. In the more intermediate-term, 5G will be deployed first as an alternative broadband access technology, with this "third pipe" of fixed wireless access potentially enabling new competition.

The underlying network will evolve significantly and will require development of new technologies across each key piece of the wireless network including radio access, transport, and the core network. Lastly, widespread deployment of 5G will require significant availability of new spectrum.

5G is currently defined more as a set of requirements than technologies, and this has left the 5G proponents open to criticism that this next generation of wireless is simply an industry marketing tool. We certainly acknowledge that there may be some degree of truth to this, but the reality is that marketing hype always arrives before the technology, and 5G is no different. In our opinion, the current open-ended nature of 5G reflects the view that this next generation of wireless is viewed by proponents as a platform rather than just another "G". Our view on 5G's reality is grounded in carriers' stated commitments to field trials in 2017.

While 5G looks to be the future, 4G wireless will continue to progress and offer consumers better mobile data rates and improved coverage. As an example, Verizon recently upgraded its network to LTE Advanced, which the carrier claims can boost peak download speeds by 50% through carrier aggregation, a technique that bonds multiple wireless channels together.

Additionally, much of the global mobile subscriber base is still on 3G and even 2G networks. While 4G spending may have indeed peaked, we nonetheless expect that there will be continued investment in 4G infrastructure, providing a long runway of revenue for the major equipment vendors.

Against this backdrop, we expect carrier spending will likely trough globally in mid-2017 and grow modestly thereafter. With 5G fixed wireless access trials imminent and a clear path to mobile 5G deployments in the next five years, we believe there are investment implications for the near- to intermediate term, and longer-term risks and opportunities that will be realized over time.

In the near- to intermediate-term, communications equipment providers should benefit as 4G network build-outs continue. A critical point is that 5G will be backwards-compatible with 4G across many parts of the network, so we expect carriers will continue to expand and densify (I.e., increase the density of coverage) of their existing networks. Industry analyst IHS estimates that worldwide mobile infrastructure spending fell 10% to USD 43bn in 2016, with the sharpest decline in China. Spending on software improved modestly (+2%), and accounted for approximately 1/3rd of total infrastructure; we believe carriers will continue to increase software investment in existing networks to add in additional capacity and functionality.

The bottom line

We reiterate our view that growth in two broad categories of transformational technologies – digital data and automation and robotics – should allow companies involved in these activities to produce above average profit growth and outperform the broader market as a result over the longer term. We also view security as the key enabling technology that underpins both digital data and industrial automation and we expect that security spending will remain one of the fastest growth areas within the IT sector. Lastly, although it is still early, we do believe 5G wireless will progress faster than expected and that this next generation of wireless technology will be critical in enabling new applications and services.

Appendix

Terms and Abbreviations

Term / Abbreviation	Description / Definition	Term / Abbreviation	Description / Definition
1H, 2H, etc. or 1H11, 2H11, etc.	First half, second half, etc. or first half 2011, second half 2011, etc.	A	actual i.e. 2010A
E	expected i.e. 2011E	Shares o/s	Shares outstanding
CIO	UBS Chief Investment Office		

Disclaimer

Research publications from Chief Investment Office Americas, Wealth Management, formerly known as CIO Wealth Management Research, are published by UBS Wealth Management and UBS Wealth Management Americas, Business Divisions of UBS AG or an affiliate thereof (collectively, UBS). In certain countries UBS AG is referred to as UBS SA. This publication is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product. The analysis contained herein does not constitute a personal recommendation or take into account the particular investment objectives, investment strategies, financial situation and needs of any specific recipient. It is based on numerous assumptions. Different assumptions could result in materially different results. We recommend that you obtain financial and/or tax advice as to the implications (including tax) of investing in the manner described or in any of the products mentioned herein. Certain services and products are subject to legal restrictions and cannot be offered worldwide on an unrestricted basis and/or may not be eligible for sale to all investors. All information and opinions expressed in this document were obtained from sources believed to be reliable and in good faith, but no representation or warranty, express or implied, is made as to its accuracy or completeness (other than disclosures relating to UBS). All information and opinions as well as any prices indicated are current only as of the dateof this report, and are subject to change without notice. Opinions expressed herein may differ or be contrary to thoseexpressed by other business areas or divisions of UBS as a result of using different assumptions and/or criteria. At any time, investment decisions (including whether to buy, sell or hold securities) made by UBS and its employees may differ from or be contrary to the opinions expressed in UBS research publications. Some investments may not be readily realizable since the market in the securities is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. UBS relies on information barriers to control the flow of information contained in one or more areas within UBS, into other areas, units, divisions or affiliates of UBS. Futures and options trading is considered risky. Past performance of an investment is no guarantee for its future performance. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in FX rates may have an adverse effect on the price, value or income of an investment. This report is for distribution only under such circumstances as may be permitted by applicable law.

Distributed to US persons by UBS Financial Services Inc. or UBS Securities LLC, subsidiaries of UBS AG. UBS Switzerland AG, UBS Deutschland AG, UBS Bank, S.A., UBS Brasil Administradora de Valores Mobiliarios Ltda, UBS Asesores Mexico, S.A. de C.V., UBS Securities Japan Co., Ltd, UBS Wealth Management Israel Ltd and UBS Menkul Degerler AS are affiliates of UBS AG. UBS Financial Services Incorporated of Puerto Rico is a subsidiary of UBS Financial Services Inc. UBS Financial Services Inc. accepts responsibility for the content of a report prepared by a non-US affiliate when it distributes reports to US persons. All transactions by a US person in the securities mentioned in this report should be effected through a US-registered broker dealer affiliated with UBS, and not through a non-US affiliate. The contents of this report have not been and will not be approved by any securities or investment authority in the United States or elsewhere. UBS Financial Services Inc. is not acting as a municipal advisor to any municipal entity or obligated person within the meaning of Section 15B of the Securities Exchange Act (the "Municipal Advisor Rule") and the opinions or views contained herein are not intended to be, and do not constitute, advice within the meaning of the Municipal Advisor Rule.

UBS specifically prohibits the redistribution or reproduction of this material in whole or in part without the prior written permission of UBS. UBS accepts no liability whatsoever for any redistribution of this document or its contents by third parties.

Version as per September 2017.

© UBS 2017. The key symbol and UBS are among the registered and unregistered trademarks of UBS. All rights reserved.