Introduction to the Longer Term Investments (LTI) series

- The Longer Term Investments (LTI) series contains thematic investment ideas based on long term structural developments.
- Secular trends such as population growth, ageing, and increased urbanization create a variety of longer term investment opportunities.
- These investment opportunities are influenced by the interplay of technological advancement, resource scarcity, and the societal changes.
- Investors willing to invest over multiple business cycles can benefit from potential mispricings created by the typically shorter term focus of stock markets.

Our view

Cyber security, along with other security and safety risks, remains a major challenge as the world becomes more and more connected and, hence, vulnerable. The WannaCry ransomware attack last year again highlighted the need for secure systems as it affected users in more than 150 countries. The stage is set for increased scrutiny. In May the EU implements its new "General Data Protection Regulation (GDPR)" that brings a material risk of fines (up to 4% of global revenues for noncompliance), driving further investment in cyber-security.

The global security and safety market is a thematic investment idea that benefits not only from structural trends such as rising cyber-attacks but from threats to the global food chain and to air, water and soil quality. Our investment theme also covers security solutions for such traditional end-users as airports, mass transit systems, ports, power plants (and other energy providers) and homeowners. We discovered that making the world a safer place offers interesting business opportunities.

The good news in a rising risk environment is that the security and safety industry is succeeding in helping us avoid danger. With greater innovation and investment, the addressable market should continue to grow at rates in the mid-to-high single digits, depending on the sub-sector. Also, the industry is not especially cyclical and appeals to growth and quality-focused investors alike.
While we expect sales in the market to rise 6% annually during 2017-2020, we expect profits to increase more rapidly due to margin expansion arising from an improving product mix (more software sales) in the cyber-security sub-sector.

**Introduction**

Long-term trends such as urbanization, stricter regulation and growing consumer awareness about product quality, data security, environmental protection and social responsibility support our security and safety theme. We examine the most important and, in our view, most promising parts of its value chain: 1) cyber-security; 2) testing, inspection and certification companies; 3) life science tools; and 4) the commercial and residential construction security sector. We excluded the basic guarding segment of the market as we think it will experience long-term structural pressure from technological solutions. A short concluding section touches on where this theme overlaps with the topic of sustainable investing.

Aside from the individual drivers of each sub-sector, we have identified one long-term trend that links them all: **urbanization**. It leads to higher population density and more social differences. Both imply greater tensions and insecurity. For example, the rate of property crime in the US is much higher in urban than in rural areas (based on 2011 numbers), according to the US National Crime Victimization Survey. In emerging markets (EMs), an expanding urban middle class can afford more security products and services, which should boost sector growth. In 1950, only 29% of the world’s population lived in cities. By 2008, urban dwellers had exceeded rural ones. The UN expects this trend to continue, with 70% of the global population residing in cities by 2050 (see Fig. 1).

While most developed country inhabitants were already concentrated in urban areas by the mid-20th century, EM residents are still catching up. The urbanization trend will create major challenges and compelling investment opportunities, in our view. A case in point is the rising number of connected devices – PCs, smartphones and wearable devices – worldwide (see Fig. 2), which is leading to increased complexity and exposing users to security risks.

**Cyber-security**

Cyber-security poses a serious threat to individuals, corporations and governments alike. While the 2013 leak of classified information to a newspaper by Edward Snowden, a former US government contractor, served as an inflection point for the cyber-security debate, the ongoing security attacks on major companies highlight that nothing is fully secure. According to Bloomberg Intelligence and IBM, global cyber security incidents continue to rise 20-30% every year.

While cyber-security has been largely associated with computers and IT infrastructure, greater consumer use of smart devices like smartphones and tablet PCs has raised overall vulnerability to cyber-threats. At the enterprise level, shifting to cloud computing has cut company costs significantly while raising the risk of an online attack. Perpetrators have become more sophisticated.
Early aggressors mainly targeted personal information, but the latest malicious attacks, such as the incidents at Yahoo!, Target and eBay, have brought entire corporate IT infrastructures to a standstill. Cyber-attackers’ intentions have also shifted from gaining notoriety to benefiting financially or politically.

Cyber-crime has broader consequences than merely exposing the vulnerabilities of the affected party. It also damages trade, competitiveness and innovation at the macro level.

A study done by IBM and Ponemon highlights that the per capital cost of data breaches in 2016 was as high as USD 221 in the US or USD 213 in Germany (see Fig. 3). It cost the global economy billions of dollars. Furthermore, we believe cyber-crime has serious implications for employment as repeated cyber-threats can jeopardize new investment and, in turn, job creation.

Despite the broad-based implications of cyber-security risks, businesses are ill-prepared for them, in our view, as the rising number of threats clearly indicates. What do these developments mean for the cyber-security industry? For one, that security is no longer merely a concern of IT managers, but a key boardroom topic as enterprises have to recognize its strategic importance. Companies need to beef up their security infrastructure to prevent breaches. Various regulations like the US’s NIST framework and the EU Cyber Security framework mandate minimum cyber-security standards. Financial institutions, for instance, face hefty fines if they do not comply with them. Interestingly, regulators themselves are not isolated from the wave of cyber-security spending. The rising risks around data also mean that major internet platforms globally continue to boost R&D spending on security (Fig. 4). With regulations on internet platforms, including the upcoming implementation of GDPR (General Data Regulation Protection) in Europe, spending on security should remain in focus.

The size of the global market was USD 100bn in 2015, and has grown by around 8% annually the past two years. Improving global profitability and a pickup in enterprise IT spending should expand the end-market by 8-10% annually on average over the next two years, with the addressable market potentially reaching USD 150-160bn by the end of 2020. These estimates look reasonable to us. Cyber-security is also one of the most defensive segments within IT; spending on it has limited downside due to its importance, and has increased at a high-single-digit rate in recent years, at a time when broader enterprise IT spending limped along at low single digit rates.

The security market is broadly divided into six segments: network security, end-point security, identity and access management, security and vulnerability management, messaging security, and web security. As is the case with any IT industry, cyber-security is broadly divided into three major components: security hardware, software and services. We see security software as a clear stand-out within the cyber-security market given its above-average growth prospects, solid margins and high recurring revenue base. The size of the industry stood at USD 34bn in 2015 (see Fig. 5), according to IDC and Bloomberg Intelligence data, and we expect it to reach USD 50bn by 2020.
Testing, inspection & certification (TIC)

Companies in the TIC sector ensure that products and processes meet standards and regulatory requirements in terms of safety and performance. They serve different end-markets, including the automotive, consumer, environmental, food, medical, life sciences, and oil & gas sectors, and inspect, verify, test, and certify services against pre-specified standards.

We estimate the addressable TIC market to be worth more than EUR 200bn. This figure is based on an analysis done by Bureau Veritas, a global market leader, and includes in-house and outsourced services. The market opportunity for public and private companies is more than EUR 80bn; the rest is for government and insured services. The regional and end-market split shows a lack of concentration (see Figs. 6 and 7), which makes it an attractive business model as there is no dependence on a single region or market.

For the 20 years ending in 2014, the average annual market growth rate for TIC was almost 9%, which beat nominal GDP growth by 2 percentage points p.a. In recent years, oil & gas headwinds have hindered it, but we think that the TIC rate will continue to outpace GDP growth thanks to attractive end-markets and further market consolidation longer term (TIC market growth rates by UBS estimates: -0.8% in 2016 due to the drop in oil & gas investments, +2.5% in 2017, +3.5% in 2018 and +4.9% in 2019).

The growing EM middle class wants more consumer goods (e.g. appliances, clothes) that will require more TIC services. Asia-Pacific’s robust demand for cars and the growing construction market in important developed markets should boost growth as both the automotive and construction sectors are heavy users of TIC company products and services. A major end-market is the environmental sector, which benefits from trends, such as water scarcity, clean air, and EM waste management and recycling, as discussed in three of our previous Longer Term Investment Themes.

The individual market drivers include increasing consumer awareness about the quality and safety of products (as evidenced by the baby food scandal in China) and tighter regulations and standards in the environmental, food and healthcare sectors. Many companies use supplier and client certifications to maintain or improve their reputation. EM companies in particular often still lack global certification, a situation that we expect will change (we anticipate them seeking more ISO certificates). Companies aren’t the only entities that want to adapt to these standards; government regulation often requires products to be certified by independent third parties (toy testing, for instance, has been compulsory in the US since 2008).

Another trend is to reduce costs by outsourcing testing services in favor of external expertise that uses state-of-the-art equipment. A growing industrial base in China and India should also spur demand for TIC services. Energy-efficiency and other requirements are getting tougher and require certifications.

The TIC industry is fragmented. The market share of the top 15 companies is only 40%, with the rest of it split among niche players with...
revenues of less than USD 10m annually. The top three players are SGS, Bureau Veritas and Intertek, whose sales range between USD 3bn and >6bn (see Fig. 8). SGS operates more than 2,400 offices and laboratories globally. The top 10 companies are all European, with five non-listed companies (Dekra, TUV Sud, DNV, TUV Rheinland, and Lloyd’s Register) among them. The sector has been one of the most active in M&A.

Life science tools

Security and safety also encompasses the safe development of new drugs and the testing of water, soil and air quality. Life science tools (LST) companies that offer products satisfying these challenges can benefit from greater safety requirements. LST companies sell equipment used in laboratories and research centers to test and monitor products prior to their sale and provide information about things like water quality. This equipment includes incubators and freezers, consumables like glassware, microscopes and pipettes, and laboratory reagents and software. UBS estimates the size of the LST market at more than USD 100bn annually (see Fig. 9). Historically, LST firms have organically increased revenue slightly more than global GDP, and their margins have grown at a faster clip than the average S&P 500 company. We expect the sub-sector to expand in line with global GDP rates now that it is at a more mature stage. Margins should still exceed the broader market’s given ongoing consolidation, operating leverage and pricing power above inflation.

Though LST companies are expanding more slowly than other security ones, their stock belongs in a well-diversified security portfolio, as the breadth of the sector’s customers (200,000 laboratories and 100,000 customers) lends it defensive qualities. LST companies commonly supply the biopharma and food and pharma-testing markets (testing, inspection and certification companies are typical customers). The sector is characterized by high barriers to entry and a stable business model; since customers don’t buy products from unproven vendors, it offers earnings stability and visibility. The long-term growth drivers, such as protecting the global food chain and the environment (e.g. water control), combating hospital infections, assisting forensic labs involved with criminal cases and testing children’s toys, etc., are similar to those in the TIC sector.

Commercial & residential construction

Alongside cyber-security, commercial and residential construction security is one of the largest theme sub-sectors, with an array of products and services on offer. Assa Abloy, the market leader for locks and security systems, estimated a few years ago that the total security market is worth over EUR 250bn. It focuses on electromechanical and mechanical locks as well as security doors. We exclude some services (guards) in our definition of the sector and so assign it a smaller overall market size (EUR 200bn / USD 250bn, see Fig. 15). From a regional perspective, the highest growth rates are in EM. Africa and the Middle East remain particularly underdeveloped, though big markets like China and India should also grow at brisk rates. The build-out of new infrastructure and buildings in big cities (urbanization) fuels demand.
In addition to this underlying demand growth, consolidation (e.g. Assa Abloy has acquired an average of 5-10 companies annually) will increase revenue and earnings, in our view. The desire for greater residential security has historically sold security products.

Data from 2010 shows that an American household was burglarized every 13 seconds (based on crime statistics). One in three houses without an alarm system suffered a break-in or break-in attempt, while only one in 250 houses with an alarm system did. Another study analyzed the average loss from burglary, finding that in homes with an alarm system it is only USD 3,266 versus USD 5,343 in those without one (based on data gathered from Greenwich, CT), because an alarm system gives burglars less time to spend in each house.

Better protection is also reflected in lower crime rates, which have sunk over the last decade (see Fig. 10). This is even more impressive given the rising population. These dynamics are expressed in the fact that the market for electromechanical security products expanded 3-4x faster than the traditional mechanical lock market in the last 10 years. A nice side effect of better home security is a lower insurance premium, which creates additional incentives for investment. We expect major business opportunities in EMs as their middle class continues to grow. Typical home security products are electric locks, sensors and cameras. The rising awareness of the need for energy-efficient applications (smart homes) enhances growth potential as well.

Ongoing urbanization and a larger EM middle class also support the commercial and residential construction safety market. As the number of people who can afford security services grows, and as they tend to live in higher-density neighborhoods, demand for them should rise. Also, emerging and developed markets alike exhibit a greater need for security investment in infrastructure like airports (e.g. for biometrics). Another trend prevalent in developed countries stems from renovation: many older houses have no fire safety equipment. Last but not least, better technology and, with it, more outsourcing (e.g. remote monitoring, video surveillance) benefit companies active in this market.

Other promising trends in the commercial and residential construction area include access control, home security solutions, video surveillance and fire protection. With regard to access control, biometrics represents one of the highest-growth segments, given the increasing importance of identity security (for travel documents, identification cards, healthcare cards and drivers licenses). Similar strong demand is expected in the video surveillance market, which is fueled by the need to support public safety in light of terrorist threats and everyday crime, which is translating into higher spending by governments and the private sector alike. Finally, the fire security market is worthy of mention. At present, North America and Europe are still its largest markets, but Asia is catching up quickly.

Tighter regulation, construction activity and asset protection are the most important factors with regard to fire security. Many countries have laws in place that ensure the use of alert systems in old and new buildings (e.g. US National Fire Protection Act or the European Norm). According to the National Fire Protection Association, reported home
fires were 50% lower in 2014 than in 1980, and fire deaths were down 47% (see also Fig. 11). US fire deaths have been relatively stable despite a growing population because of, among other factors, more fire alarms. But almost two-thirds of fire deaths still occur in buildings without fire alarms or with non-functioning alarms, sad statistics that clearly support our investment theme.

Risks
Risks in the cyber-security area include the inability of security vendors to prepare for a major threat or to adjust to a major technological change, which would result in lower spending. A weaker macro outlook could also weigh on enterprise and government IT outlays, though we believe cyber-security should be relatively less affected, as evidenced by the US’s FY 2017 budget. In the other sub-sectors, a main risk comes from the regulatory side. Less strict regulation might lessen demand for TICs and construction-exposed names, reducing expected sales and earnings growth. Decreased government spending on critical infrastructure (airports, public places, etc.) would also reduce investment in security products. TIC companies have a broad range of end-markets, and weak demand in areas not discussed in this report (e.g. the oil & gas end-market) also jeopardizes sales and earnings. In the life science and tools sub-sector, the biggest risks are again regulatory changes and reimbursement uncertainties.

Link to sustainable investing
We view "Security and safety" as a sustainability-themed investment that fits in our sustainable investing (SI) framework. The products and services offered by security and safety companies apply primarily to the social aspects of environmental, social and governance (ESG) issues. In particular, cyber security issues have gained importance in recent years as sector products address the need to prevent data loss. Breaches of cyber security may damage society because they can disrupt the financial system, food and water provisioning, and communications. Traditional risks that security and safety companies address are found in the area of testing: assessing the quality of the global food supply chain, monitoring water, soil and air quality, and testing children’s toys for toxic heavy metals. The security and safety companies either operate the laboratories that conduct this testing or provide equipment to them. Other examples include building security, such as fire detection.
Conclusion

The importance of the security and safety industry should keep its products and services in high demand. While it should generally benefit from a pickup in the global economy, spending on it tends to exhibit less cyclicality, which makes the theme more defensive. As seen in Fig. 15, our bottom-up estimates project that the addressable market should increase by an average of 6% over the next few years. Though it is already a large industry (estimated size around USD 600bn in 2017), we believe its growth rates will remain impressive. More importantly, its earnings growth should reach high-single digits and low double-digit rates, given the margin expansion resulting from an improving mix as the share of higher-margin businesses increases. To fully benefit from this theme, investors need to take a long-term view. Companies that make up the theme, particularly those in the cyber-security sub-sector, feature solid balance sheets and strong cash flow generation. The other sub-sectors are also characterized by solid structural growth trends, such as the rising demand for testing in EMs and the greater need for commercial and residential construction security applications.

Fig. 12: Security and safety addressable market

In USD billions

Source: Industry and company reports, UBS estimates (based on EUR/USD exchange rate of 1.1)

Note: Cyber = Cyber-security, Comm & Resi Con = Commercial & Residential Construction
Appendix

**Terms and Abbreviations**

<table>
<thead>
<tr>
<th>Term / Abbreviation</th>
<th>Description / Definition</th>
<th>Term / Abbreviation</th>
<th>Description / Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011E, 2012E, etc.</td>
<td>2011 estimate, 2012 estimate, etc.</td>
<td>A</td>
<td>actual i.e. 2010A</td>
</tr>
<tr>
<td>COM</td>
<td>Common shares</td>
<td>E</td>
<td>expected i.e. 2011E</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal year / financial year</td>
<td>GDP</td>
<td>Gross domestic product</td>
</tr>
<tr>
<td>p.a.</td>
<td>Per annum (per year)</td>
<td>Shares o/s</td>
<td>Shares outstanding</td>
</tr>
<tr>
<td>UP</td>
<td>Underperform: The stock is expected to underperform the sector benchmark</td>
<td>CIO</td>
<td>UBS WM Chief Investment Office</td>
</tr>
</tbody>
</table>

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 date of this report, and are subject to change without notice. Opinions expressed herein may differ or be contrary to those expressed 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 2018. The key symbol and UBS are among the registered and unregistered trademarks of UBS. All rights reserved.