Security and safety touch lives everywhere. Governments need to keep infrastructure safe and functioning, enterprises must protect data and consumers have to trust products like baby food.

Growing trends toward urbanization, stricter regulation and greater consumer awareness about product quality, data security, environmental protection and social responsibility are just a few factors that support the theme. It ranges from high-tech cyber-security solutions to traditional security equipment for homeowners or infrastructure security like airports.

We think the addressable market is a defensive one that offers attractive growth rates in the mid-to-high single digits over the next 5–10 years. We estimate its overall size at around USD 600bn last year, and think it will reach USD 700bn by 2021 (around mid-single digit annual growth). We recommend investing in it in a well-diversified way to gain exposure to the entire security and safety value chain worldwide.

Our view
While cyber-security incidents continued to rise in 2018, the magnitude of breaches was unprecedented. There were 15 cyber-security breaches that affected at least five million users, with the top incident at Marriot affecting more than 500 million users. Big firms were not spared as evidenced by the widely followed Cambridge Analytica scandal at Facebook or Google+, which eventually forced Cambridge Analytica’s shutdown. With the implementation of the new General Data Protection Regulation (GDPR) in the EU in May 2018 and increasing cyber-security regulations globally, security should remain in the spotlight in 2019.

The global security and safety market is a thematic investment idea that benefits not only from structural trends such as rising cyber-attacks but also 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 market participants do appear to understand this and the security and safety industry is succeeding in helping us to limit or 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 more than 5% annually during 2018–2021, 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, the most promising parts of its value chain: 1) cyber-security; 2) testing, inspection and certification; 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 areas than in rural areas (based on 2014 numbers), according to the US National Center for Victims of Crime. 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. 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. According to Ponemon and Bloomberg Intelligence, the average cost of security breach remains elevated. As seen in Fig. 3, the global average cost of security breach is USD 3.6m, with the impact as high as USD 7.4m in the US. While in developing countries, one may argue the dollar cost may be lower but the impact these breaches create is unimaginable. We believe cyber-crime has serious implications for employment as repeated cyber-threats can jeopardize new investment

<table>
<thead>
<tr>
<th>Country</th>
<th>Cost (USD m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>3.1</td>
</tr>
<tr>
<td>Japan</td>
<td>3.5</td>
</tr>
<tr>
<td>France</td>
<td>3.5</td>
</tr>
<tr>
<td>US</td>
<td>7.4</td>
</tr>
<tr>
<td>Global average</td>
<td>3.6</td>
</tr>
</tbody>
</table>

Source: Ponemon, Bloomberg Intelligence, UBS, as of 2017
and, in turn, job creation. In summary, cyber breaches cost the global economy billions of dollars, with the total cost rising 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. Before, aggressors mainly targeted personal information, but the latest malicious attacks, such as the incidents at Facebook or Marriott have brought entire corporate IT infrastructures to a standstill. Cyber-attackers’ intentions have also shifted from gaining notoriety to benefiting financially or politically.

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 Cybersecurity Act 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 (see 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 close to USD 125bn in 2018, growing by 8% annually during the past few years. We believe steadily rising enterprise IT spending, coupled with the need to beef up security systems, should help the end-market continue to grow by 8% annually on average over the next two years, with the addressable market potentially reaching USD 145bn 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.

As is the case with any IT industry, cyber-security is broadly divided into three major components: security hardware, software and services. However, with increasing contribution from cloud, we believe it’s time to segment it as an independent unit and carve out of software. Despite that, as seen in Fig. 4, software is the largest segment, followed by services, hardware and then cloud. However, as seen in Fig. 5, cloud security is the fastest growing segment, in our view. According to IDC and Bloomberg Intelligence, cloud security, with 14% average annual growth, is the fastest growing market within the cyber-security market at the expense of traditional appliance-based and on-premise security solutions.

**Fig. 4: Cyber-security spending breakdown**

Source: IDC, Bloomberg Intelligence, UBS, as of December 2018

**Fig. 5: Cloud is the fastest growing segment within cyber-security over the next three years**

Source: IDC, Bloomberg Intelligence, UBS estimates, as of December 2018

**Fig. 6: Fastest growing cyber-security segments**

Average annual growth rates

Source: IDC, Bloomberg Intelligence, UBS, as of December 2018

Note: DDOS = distributed denial-of-service
Beyond the traditional growth areas, the cyber-security market is also witnessing rapid changes driven by rapid innovation. New business models are needed to defend against the ever-growing cyber complexities. As a result, during the past few years, new solutions have emerged. Fig. 6 highlights some of the fastest growing new segments within cyber-security that are growing by more than 10% annually like specialized threat solutions or Internet of Things security solutions. Looking ahead, we expect artificial intelligence (AI) to play a bigger role in cyber-security. For instance, AI can be used to automate the detection and response of security vulnerabilities or even help deal with the problem of having too many false alerts.

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.

The addressable TIC market size estimates vary anywhere from EUR 100bn to EUR 300bn, of which about 40% represents the outsourced market. This implies a current market opportunity of around EUR 80bn at the mid-point. We estimate that the market leaders SGS, Intertek, Bureau Veritas, Applus, Eurofins together represent about 25% of the addressable “non-in-house” market (see Fig. 7). Overall, the TIC industry is fragmented. The top companies are very big compared to the many other niche players with revenues of less than USD 10m annually. The sector has been one of the most active in M&As.

Also, the regional and end-market split shows a lack of concentration, which makes it an attractive business model as there is no dependence on a single region or market.

Between 2001 and 2013, the average annual market growth rate for the top five TIC companies was almost 8% p.a., which beat the nominal GDP growth. Since then, the sector has had some tough years, but has recovered from a trough of only 1.2% growth in 2016 due to the oil & gas recession and a wider industrial downturn. We expect the top five testing companies to grow 4–5% annually during 2019–2021 (see Fig. 8).

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, but we expect them to seek more ISO certificates in the coming years. Companies aren’t the only entities that want to adapt to these standards; government regulation also 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.

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. Based on this broader definition of the LST market industry, experts estimate the market size at USD 110bn last year (see Fig. 9). Historically, LST firms have organically increased revenue slightly more than the 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 at around 5% annually now that it is at a more mature stage. Margins should still exceed the broader market given the ongoing consolidation, operating leverage and pricing power above inflation. Though LST companies are expanding more slowly than other security companies, 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, food and pharma-testing markets (testing, inspection and certification companies are typical customers). Over the last decade, the sector became less cyclical than in the past due to higher sales exposure to less cyclical industries like pharma. Therefore, the health of the pharma industry is important. But the funding of government testing agencies (in the US, China) also has a big influence. In China, for instance, the focus on food, the environment, and healthcare in the government’s 5-year plan is good for LST companies.

The sector is characterized by high barriers to entry and a stable business model; as 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. We estimate the global home security market at around EUR 244bn in 2018. This includes doors and windows (EUR 123bn), locks and access (EUR 46bn), alarms (EUR 43bn), smart IT (EUR 22bn), and intrusion (EUR 12bn) (see Fig. 10). We exclude guards (EUR 77bn in 2018E) in our definition.

In this section, we want to focus on the global lock market, which will be a very attractive part of the smart home security market in the future.

Today’s world is still characterized by mainly mechanical locks, dominating the market with more than 90% of the installed base (see Fig. 11). However, as Fig. 12 indicates, the growth rates over the last few years have shown that electro-mechanical locks are increasingly used, clearly outpacing the growth rates of traditional locks by 5x. A typical niche where electro-mechanical locks are used already are hotel chains or managed apartment blocks. There you don’t have a key anymore, only a chip card. This is a much safer way of controlling access, and we expect it to migrate to residential applications.

Most locks globally are still mechanical, a technology that has existed for 8,000 years, but electro-mechanical locks look set for take-off to create a mass market. The Internet of Things (IoT) technology, in our view, will be the driving force behind it and will create broad-based demand also in flats and single homes in the next decade.

In the past, the total lock market grew only 2-3% p.a., but the potential for new and retrofitted locks could accelerate market growth to over 5% (see Fig. 13). Over the decade to 2025, we expect around 60% p.a. growth in demand for the global smart lock market, growing from around three million smart locks in 2016 to over 180 million units (see Fig. 14). With a total market size expected to reach around EUR 30bn by 2025 (from EUR 0.5bn in 2016), traditional locks will lose market share while smart locks will gain market share. In addition to this underlying demand growth, consolidation (e.g. Assa Abloy has acquired an average of 5–10 companies annually in recent years) will increase revenue and earnings, in our view. The desire for greater residential security has historically sold security products.

Better protection is also reflected in lower crime rates, which have sunk over the last decade (see Fig. 15). This is even more impressive given the rising population. 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
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. In the other sub-sectors, a main risk is regulation. Less strict regulation might lessen demand for TIC companies 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.

Other promising trends in the commercial and residential construction area include access control, 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 driver’s 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.

**Fig. 14: UBS estimate for global lock market in units and smart lock penetration**

<table>
<thead>
<tr>
<th>Year</th>
<th>Traditional Locks (mn)</th>
<th>Smart Locks (mn)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>100</td>
<td>20</td>
</tr>
<tr>
<td>2015</td>
<td>500</td>
<td>100</td>
</tr>
<tr>
<td>2020</td>
<td>700</td>
<td>200</td>
</tr>
</tbody>
</table>

Source: UBS estimates, as of August 2018

**Fig. 15: Plunging total crime rates in the US**

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Number of Crimes (lhs)</th>
<th>US Population (rhs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>12.5</td>
<td>260</td>
</tr>
<tr>
<td>2017</td>
<td>9.0</td>
<td>330</td>
</tr>
</tbody>
</table>

Source: US Disaster Center, as of January 2019 Note: rhs = right hand side; lhs = left hand side
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 generally benefits 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. 16, our bottom-up estimates project that the addressable market should increase by an average of slightly more than 5% over the next few years. Though it is already a large industry (estimated size around USD 598bn in 2018), we believe its growth rate will remain healthy. More importantly, its earnings growth should reach high-single or low double-digit rates, in our view, 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. 16: Security and safety addressable market
In USD billions

Source: Industry and company reports, UBS estimates (based on EUR/USD exchange rate of 1.15) Note: Cyber = Cyber-security; Comm & Resi Con = Commercial & Residential Construction; as of 11 January 2019

ESG/Sustainable Investing Considerations: Sustainable investing strategies aim to consider and in some instances integrate the analysis of environmental, social and governance (ESG) factors into the investment process and portfolio. Strategies across geographies and styles approach ESG analysis and incorporate the findings in a variety of ways. Incorporating ESG factors or Sustainable Investing considerations may inhibit the portfolio manager’s ability to participate in certain investment opportunities that otherwise would be consistent with its investment objective and other principal investment strategies. The returns on a portfolio consisting primarily of ESG or sustainable investments may be lower or higher than a portfolio where such factors are not considered by the portfolio manager. Because sustainability criteria can exclude some investments, investors may not be able to take advantage of the same opportunities or market trends as investors that do not use such criteria. Companies may not necessarily meet high performance standards on all aspects of ESG or sustainable investing issues; there is also no guarantee that any company will meet expectations in connection with corporate responsibility, sustainability, and/or impact performance.
## 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>bn</td>
<td>Billion</td>
<td>COM</td>
<td>Common shares</td>
</tr>
<tr>
<td>E</td>
<td>expected i.e. 2011E</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 Global Wealth Management, formerly known as CIO Americas, Wealth Management, are published by UBS Global Wealth Management, a Business Division 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 PuertoRico 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 April 2018.

© UBS 2019. The key symbol and UBS are among the registered and unregistered trademarks of UBS. All rights reserved.