CIO Special
February 15, 2022

Authors:
Alberto Fadelli
Head Chief Investment Office Italy

Daniel Sacco
Investment Officer Italy

Matteo Giovanni Fava
Investment Officer Italy

Cyber security: protection for the digital environment

Key take aways

- Cyber security is of direct relevance for the trends that have emerged during the pandemic – specifically the growing use of technology, smart working, and the increase in online interactions.
- As the world continues becoming more closely connected via digital infrastructure, artificial intelligence and 5G there will be greater demand for investments and rules to protect data and increase the security of all online interactions.
- Cyber security is linked to different topics: ranging from technology and laws, new rules of collaboration, critical infrastructure protection, cyber privacy, "security of things", cyber war, IT systems resilience and cybercrime.

01 Introduction

The share of the world's population using the internet increased from 0.05% in 1990 to 49% in 2017[1] to over 3.4 bn.

Global internet coverage is generating more and more data and information, with the total volume for 2021 estimated at 79 Zettabytes (ZB or 10^{21})[2] and expected to more than double to 181 ZB in 2025.

With data volumes and online transactions on the rise questions are being asked about the protection of all our internet interactions because data threads, security breaches, costs related to breaches, and in general the associated lost business for companies[3] are growing concerns for citizens, governments, and companies around the globe.

These concerns are backed up by the costs generated by rising cybercrime rates,[4] estimated at USD1.5tn in 2018, growing numbers of data theft (+160% in 2020 vs. 2019), unauthorised server access (+233% in 2020 vs. 2019)[5] and the rising average cost of mega breaches (category between 50 and 65 mn sets of data) to USD401mn in 2019 (from USD388mn in 2018).

The Covid-19 pandemic had an impact on a variety of market trends and also necessitated mass usage of remote working, which drove up the average cost of data breaches to USD4.96mn (over 24% higher than normal).[6]

The U.S. remains the country with the highest average costs for data breaches (USD9.05m) followed by Middle East (USD6.93mn), Canada and Germany.[5]

Looking at the situation in Europe, which varies widely from country to country (with the highest costs in Germany and among the lowest in Scandinavia), we notice that the public and government sector was a major target in the period April 2020 – July 2021, while the healthcare sector was also targeted significantly with an increased number of attacks during the same period.[7]

The healthcare sector warrants particular attention because at the global level it had the most costly breaches (USD9.23mn) in 2021, having risen by some 30% in one year.

Please use the QR code to access a selection of other Deutsche Bank CIO reports (www.deutschewealth.com).

Another noteworthy statistic is the time taken to identify an issue, which grew 30 days since 2017 to 287 days in 2021.[6]

In order to gain a complete overview, it's important to look at the types of records compromised by breaches. Customers' personally identifiable information (PII) is the largest category, representing 44% of the overall records, while breaches of employee PII are a critical problem for companies and represent 26% of the data.[6]

02 Geopolitics and international trade

The study of the impact of Earth's geography on politics and international relations is known as geopolitics. However, the ongoing digitalisation of all areas of daily life, as well as the world's growing dependence on the internet, has transformed cyberspace into an extra domain in which sovereign nations may collaborate with and compete against one another. To put it another way, the digital environment has bridged or broke down geographical barriers as we know them. The speed of this digital transformation has accelerated even faster since the Covid-19 pandemic, culminating in a growing reliance on the digital sphere for how we live, work, and interact.

As a result, cyber security is no longer only a technological concern, but it has also entered the geopolitical domain. Critical technologies, from basic information and communication infrastructure to emerging ones like 5G, cloud computing, artificial intelligence, and quantum computing – and the related cyber risks they foreshadow – provide pathways for impacting a country's national security, economic growth, and societal values. Cyber capabilities and key technologies are emerging as tools of state power that may be used against enemies. At the same time, hostile actors have systematically targeted essential assets and critical infrastructure – such as healthcare – causing massive economic and reputational consequences for enterprises and governments. These developments underline the growing need for protection against cyber-attacks.

Cyber security is increasingly being mentioned as a cornerstone of "national security". National cyber security concerns can be viewed from four main perspectives: military, political, economic, and socio-cultural security threats. At the same time, however, most institutions, including both businesses and governments, are becoming increasingly reliant on global supply networks, which include both digital and physical supply chains. The cyber risks associated with digital and physical supply chains, such as the increased number of channels that can be targeted by cyber-attacks and data leaks, exacerbate cyber security problems. It is important to note that national cyber security and supply chain cybersecurity are intrinsically intertwined. Issues around cyber security in the supply chain for vital sectors/services will heighten national cyber security concerns. Fears regarding national cyber security, on the other hand, influence attitudes about supply chain risk, particularly supply chain cyber security.

For instance, as infrastructure in numerous sectors (from water to electricity to transportation) becomes digitally connected, the potential for large-scale breakdowns and other harm has grown. Examples of this are the NotPetya cyber-attack on Ukraine's power grid, which caused power outages,[8] the Colonial Pipeline ransomware attack in May 2021 affected the billing infrastructure of the operating company, the pipeline operation was shut down as a precautionary measure, which lead to fuel shortages, panic buying, reschedules flights and the declaration of the state of emergency in 17 states as well as Washington DC and a ransomware attack that denied access to data, forcing hospitals in the United Kingdom to cancel operations and redirect patients to other facilities.[9] In addition, the 5G network will become an integral part of this vital infrastructure since it is used to deliver critical services such as healthcare, energy, and transportation, implying that an interruption in the 5G network might result in a loss of access to critical services.

Countries can intervene in cyberspace with cyber security policies and laws that strengthen their offensive and defensive capabilities to safeguard institutions, corporations, and individuals from future cyber assaults. There is little question that these rules and regulations will have an influence on cyber space, not just for the nations involved, but also for the entire global internet community.

Since it is unrealistic to scrutinise the millions of lines of software or firmware in every single product, governments and organisations all over the world have sought to devise defensive strategies to protect themselves against cyber threats and to prevent trade from generating new attack vectors. It is been estimated that at least 50 countries have introduced cyber security laws and policies to enunciate their national online security strategy.[10] One common method that has been recommended informally is imposing an import ban on potentially harmful items from risky nations. However, this gives rise to numerous policy considerations, such as

1. how to define a risky country given the globalised value chain for almost every product,
2. which products are of critical importance, and
3. assuming that such restrictions rapidly become global policies which are met with retaliation, what could be the effect on international trade and the economy?

Many international trade restrictions have been implemented due to of security fears, such as LinkedIn's restriction in Russia[11] or the limitation of data flows to India from the European Union[12] and so on. Government agencies may establish rules that might result in cyber disputes without a clear grasp of the bigger implications, while corporations struggle to adapt to increasing cyber security concerns and constraints. In the international economic arena, for example, the "National Security Exception" principle allows governments to intervene when required in circumstances of "essential security interest".

As a result, we may anticipate data localisation rules that limit cross-border data transfer throughout the world becoming a major topic during trade agreement negotiations in the guise of "data protection" and national security. Incidents such as the 2017 Equifax Data Breach,[13] which compromised the personal information of 143 mn individuals, are still a vivid memory for many people. Cyber security measures are therefore likely to act as roadblocks to data transfers and digital trade. in the supply chain for digital services, however, data is seen as a crucial enabling asset.

Indeed, the digital sector and developing technologies rely on global data flows for innovation as well as access to hardware and software for manufacturing and distribution. Consider artificial intelligence (AI), a data-driven breakthrough that has the potential to add trillions of dollars to global output over the next ten years and hasten the move to a service-based global

economy. According to the McKinsey Global Institute, artificial intelligence (AI) might increase global productivity by 16% or USD13tn by 2030.[14] Data is also progressively being stored in the cloud, which is comprised of globally dispersed data centres that transfer data to users as well as to other data centres for backup and safety.

Global data flows also enable the online distribution of products and services, both direct-to-consumer and business-to-business across global supply chains. International e-commerce already accounts for around 12% of global merchandise trade.[15] According to a 2019 United Nations Conference on Trade and Development (UNCTAD) estimate, worldwide e-commerce was valued at USD29tn in 2017, with around 1.3bn consumers purchasing online – a 12% increase from the previous year.[16] E-commerce also has the potential to significantly enhance small company engagement in international trade. For example, having a website provides small firms with an instant international profile without the need to create a physical presence in another country.

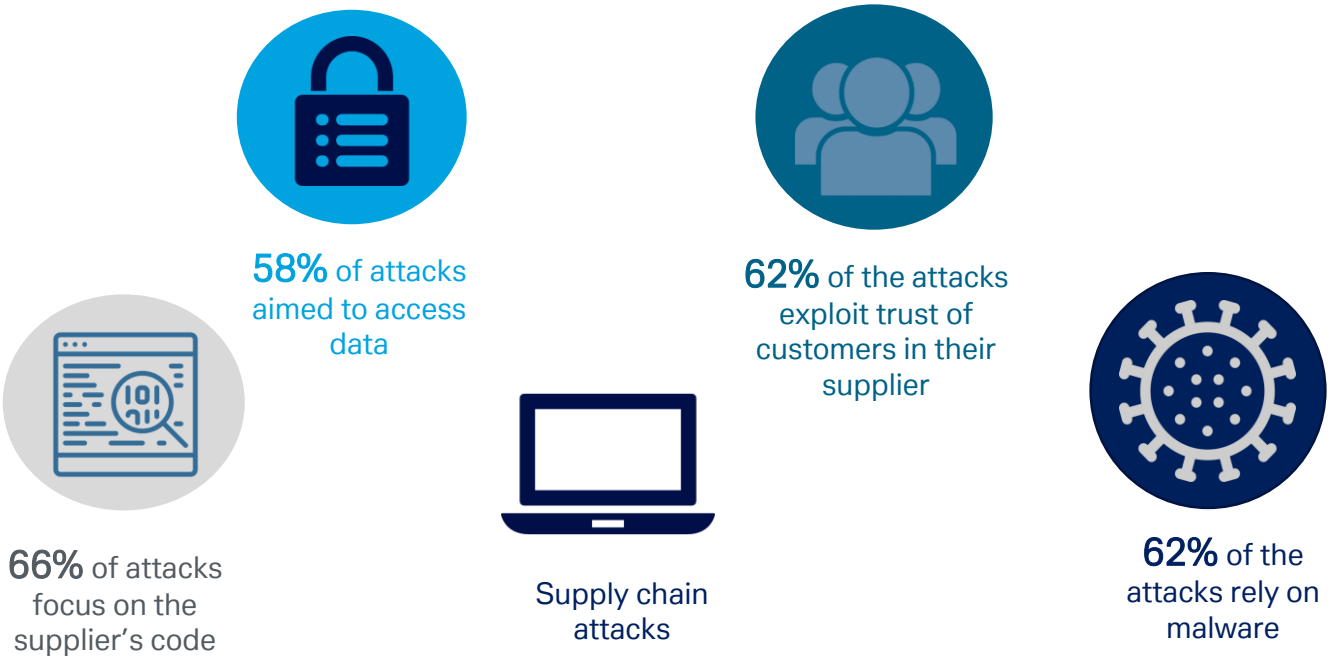
It should be clear by now how global data flows underly global supply networks, opening up new avenues for international economic engagement. Global supply chain involvement is being influenced by data and digital technology in a variety of ways, facilitated by interconnectivity and cross-border data transfers that ease communications and may be used to manage logistics. Global data flows are also enabling "supply chain 4.0", in which information flows are interconnected and omnidirectional rather than linear, opening up new options for boosting productivity and enhancing employment.

Going forward, the introduction of 5G networks and technologies will significantly accelerate the growth of the digital economy and digital trade. 5G will increase data speeds and capacity, facilitating the development of new technologies such as autonomous vehicles, virtual reality and biomedical applications. It will also enable significant growth in the IoT – the linking of billions of products to the network,[17] from homes to industries. Cisco predicts that by 2030, 500bn devices will be connected to the network . The Internet Protocol will be utilised in network design and by applications that operate on it. As everything becomes an IP app, 5G will essentially transform everything into data, meaning ever-increasing cyber security concerns and risks for enterprises.

Cyber security problems in international trade should be regarded a business strategy issue, not merely a regulatory compliance matter. Businesses in the global supply chain must respond to normative pressures from policies that impact their international trade activities. On the other hand, cyber security concerns in the international supply chain are forcing companies to reconsider their global supply chains – not just the physical supply chain, but also the digital supply chain – in order to safeguard organisational assets. The business architecture and organizational boundaries have shifted in this digital supply chain scenario. Threats can emerge from both inside and outside a company. In the digital supply chain, vendors, consumers, and partners are linked to one another. Aside from its economic and social potential, the global digital network gives rise to new hazards in the form of online fraud, abuse, crime and security concerns.

Some supply chain deficiencies that can be exploited to introduce these threats include "purchasing information technology products or parts from independent distributors, brokers, or the gray market", "lack of adequate testing for software updates and patches", "incomplete information on IT suppliers" and "use of insecure supply chain delivery and storage mechanism[s]".[18]

Chart 1: Supply chain attacks on the rise



Source: ENISA Threat Landscape for Supply Chain Attacks as of July 2019.

These trends have intensified the need for joint regional and global actions to construct a safe, trustworthy, and adaptable cyberspace over the last three to four years. Because cyber threats are global and not constrained by borders, nations must collaborate – both internationally and regionally – to protect the cyber security of our essential infrastructure, companies, and people. A rules-based order is crucial because it ensures the trust, predictability, and stability required by all states, large and small, for economic advancement, job creation, and technological adoption. As things currently stand, we need more international collaboration, not less, to establish the ground rules for our digital commons. The future of cyber security in international trade will define not only cyberspace for individual nations, but also for the larger globalized society.

03 Conclusion

Market trends, internet and technological developments linked to the internet of things and the growth in online interactions highlight the importance of data protection, connection security and more broadly the protection of internet infrastructures and the security of all online transactions.

On one hand, governments, institutions and companies around the world are now more concerned about data protection and the reliability of internet infrastructures because their own growth is heavily dependent on the development of technological / communication systems. On the other hand, privacy and security are of such paramount importance to so many individuals that some customers say they will not do business with a company that has data security issues.[19]

The overarching message is that cyber security is such an important topic because it's a priority for consumers, companies and governments given that data sharing and information storage are central to everyday life.

Bibliography

1. World Telecommunication / ICT Indicators Database – International Telecommunication Union. Retrieved from: http://data.worldbank.org/data-catalog/world-development-indicators
2. Statista (on IDC's Forecast from late 2018). Retrieved from: https://www.statista.com/statistics/871513/worldwide-data-created/
3. Cost of a Data Breach Report 2021 – IBM.
4. "33 Alarming Cybercrime Statistics You Should Know in 2019," by Casey Cane, Security Boulevard, November 15, 2019 cited in Cyber Security Report by Check Point.
5. IMB Security X-Force Threat Intelligence Index 2021.
6. IBM Cost of a Data Breach Report 2021.
7. ENISA THREAT LANDSCAPE 2021 / April 2020 to mid-July 2021, ENISA, October 2021.
8. Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
9. Retrieved from: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack
10. ITU Global Cybersecurity Index 2017.
11. Retrieved from: https://www.bbc.com/news/technology-38014501
12. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6321
13. Retrieved from: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
14. Retrieved from: https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy
15. Retrieved from: https://crsreports.congress.gov/product/pdf/IF/IF11194#:~:text=The%20McKinsey%20Global%20Institute%20estimates,(B2C%20or%20retail)%20sales
16. Retrieved from: https://unctad.org/press-material/global-e-commerce-sales-surged-29-trillion
17. Retrieved from: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf
18. Retrieved from: https://www.gao.gov/products/gao-12-342sp
19. Retrieved from: https://www.pwc.com.au/digitalpulse/report-protect-me-consumers-cyber-security.html

Glossary

Personally identifiable information (PII) is information used by any organization to confirm an individual's identity.

The Internet of Things (IoT) is comprised of computers and other devices with embedded electronics that allow them to collect and share data.

The United Nations Conference on Trade and Development (UNCTAD) was established in 1964 as an intergovernmental organisation to promote the interests of developing states in world trade.

USD is the currency code for the U.S. Dollar.

Important information

General
This document may not be distributed in Canada or Japan. This document is intended for retail or professional clients only. This document is being circulated in good faith by Deutsche Bank AG, its branches (as permitted in any relevant jurisdiction), affiliated companies and its officers and employees (collectively, "Deutsche Bank").
This material is for your information only and is not intended as an offer, or recommendation or solicitation of an offer to buy or sell any investment, security, financial instrument or other specific product, to conclude a transaction, or to provide any investment service or investment advice, or to provide any research, investment research or investment recommendation, in any jurisdiction. All materials in this communication are meant to be reviewed in their entirety.
If a court of competent jurisdiction deems any provision of this disclaimer unenforceable, the remaining provisions will remain in full force and effect.
This document has been prepared as a general market commentary without consideration of the investment needs, objectives or financial circumstances of any investor. Investments are subject to generic market risks which derive from the instrument or are specific to the instrument or attached to the particular issuer. Should such risks materialise, investors may incur losses, including (without limitation) a total loss of the invested capital. The value of investments can fall as well as rise and you may not recover the amount originally invested at any point in time. This document does not identify all the risks (direct or indirect) or other considerations which may be material to an investor when making an investment decision.
This document and all information included herein are provided "as is", "as available" and no representation or warranty of any kind, express, implied or statutory, is made by Deutsche Bank regarding any statement or information contained herein or in conjunction with this document. All opinions, market prices, estimates, forward looking statements, hypothetical statements, forecast returns or other opinions leading to financial conclusions contained herein reflect Deutsche Bank's subjective judgment on the date of this report. Without limitation, Deutsche Bank does not warrant the accuracy, adequacy, completeness, reliability, timeliness or availability of this communication or any information in this document and expressly disclaims liability for errors or omissions herein. Forward looking statements involve significant elements of subjective judgments and analyses and changes thereto and/or consideration of different or additional factors could have a material impact on the results indicated. Therefore, actual results may vary, perhaps materially, from the results contained herein.
Deutsche Bank does not assume any obligation to either update the information contained in this document or inform investors about available updated information. The information contained in this document is subject to change without notice and based on a number of assumptions which may not prove valid, and may be different from conclusions expressed by other departments within Deutsche Bank. Although the information contained in this document has been diligently compiled by Deutsche Bank and derived from sources that Deutsche Bank considers trustworthy and reliable, Deutsche Bank does not guarantee or cannot make any guarantee about the completeness, fairness, or accuracy of the information and it should not be relied upon as such. This document may provide, for your convenience, references to websites and other external sources. Deutsche Bank takes no responsibility for their content and their content does not form any part of this document. Accessing such external sources is at your own risk. Before making an investment decision, investors need to consider, with or without the assistance of an investment adviser, whether any investments and strategies described or provided by Deutsche Bank, are appropriate, in light of their particular investment needs, objectives, financial circumstances and instrument specifics. When making an investment decision, potential investors should not rely on this document but only on what is contained in the final offering documents relating to the investment. As a global financial services provider, Deutsche Bank from time to time faces actual and potential conflicts of interest. Deutsche Bank's policy is to take all appropriate steps to maintain and operate effective organisational and administrative arrangements to identify and manage such conflicts. Senior management within Deutsche Bank are responsible for ensuring that Deutsche Bank's systems, controls and procedures are adequate to identify and manage conflicts of interest. Deutsche Bank does not give tax or legal advice, including in this document and nothing in this document should be interpreted as Deutsche Bank providing any person with any investment advice. Investors should seek advice from their own tax experts, lawyers and investment advisers in considering investments and strategies described by Deutsche Bank. Unless notified to the contrary in a particular case, investment instruments are not insured by any governmental entity, not subject to deposit protection schemes and not guaranteed, including by Deutsche Bank. This document may not be reproduced or circulated without Deutsche Bank's express written authorisation. Deutsche Bank expressly prohibits the distribution and transfer of this material to third parties. Deutsche Bank accepts no liability whatsoever arising from the use or distribution of this material or for any action taken or decision made in respect of investments mentioned in this document the investor may have entered into or may enter in future.
The manner of circulation and distribution of this document may be restricted by law or regulation in certain countries, including, without limitation, the United States. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction, where such distribution, publication, availability or use would be contrary to law or regulation or which would subject Deutsche Bank to any registration or licensing requirement within such jurisdiction not currently met. Persons into whose possession this document may come are required to inform themselves of, and to observe, such restrictions. Past performance is no guarantee of future results; nothing contained herein shall constitute any representation, warranty or prediction as to future performance. Further information is available upon investor's request.

Kingdom of Bahrain
For Residents of the Kingdom of Bahrain: This document does not constitute an offer for sale of, or participation in, securities, derivatives or funds marketed in Bahrain within the meaning of Bahrain Monetary Agency Regulations. All applications for investment should be received and any allotments should be made, in each case from outside of Bahrain. This document has been prepared for private information purposes of intended investors only who will be institutions. No invitation shall be made to the public in the Kingdom of Bahrain and this document will not be issued, passed to, or made available to the public generally. The Central Bank (CBB) has not reviewed, nor has it approved, this document or the marketing of such securities, derivatives or funds in the Kingdom of Bahrain. Accordingly, the securities, derivatives or funds may not be offered or sold in Bahrain or to residents thereof except as permitted by Bahrain law. The CBB is not responsible for performance of the securities, derivatives or funds.

State of Kuwait
This document has been sent to you at your own request. This presentation is not for general circulation to the public in Kuwait. The Interests have not been licensed for offering in Kuwait by the Kuwait Capital Markets Authority or any other relevant Kuwaiti government agency. The offering of

Important information

the Interests in Kuwait on the basis a private placement or public offering is, therefore, restricted in accordance with Decree Law No. 31 of 1990 and the implementing regulations thereto (as amended) and Law No. 7 of 2010 and the bylaws thereto (as amended). No private or public offering of the Interests is being made in Kuwait, and no agreement relating to the sale of the Interests will be concluded in Kuwait. No marketing or solicitation or inducement activities are being used to offer or market the Interests in Kuwait.

United Arab Emirates
Deutsche Bank AG in the Dubai International Financial Centre (registered no. 00045) is regulated by the Dubai Financial Services Authority. Deutsche Bank AG -DIFC Branch may only undertake the financial services activities that fall within the scope of its existing DFSA license. Principal place of business in the DIFC: Dubai International Financial Centre, The Gate Village, Building 5, PO Box 504902, Dubai, U.A.E. This information has been distributed by Deutsche Bank AG. Related financial products or services are only available to Professional Clients, as defined by the Dubai Financial Services Authority.

State of Qatar
Deutsche Bank AG in the Qatar Financial Centre (registered no. 00032) is regulated by the Qatar Financial Centre Regulatory Authority. Deutsche Bank AG -QFC Branch may only undertake the financial services activities that fall within the scope of its existing QFCRA license. Principal place of business in the QFC: Qatar Financial Centre, Tower, West Bay, Level 5, PO Box 14928, Doha, Qatar. This information has been distributed by Deutsche Bank AG. Related financial products or services are only available to Business Customers, as defined by the Qatar Financial Centre Regulatory Authority.

Kingdom of Belgium
This document has been distributed in Belgium by Deutsche Bank AG acting though its Brussels Branch. Deutsche Bank AG is a stock corporation ("Aktiengesellschaft") incorporated under the laws of the Federal Republic of Germany and licensed to carry on banking business and to provide financial services subject to the supervision and control of the European Central Bank ("ECB") and the German Federal Financial Supervisory Authority ("Bundesanstalt für Finanzdienstleistungsaufsicht" or "BaFin").Deutsche Bank AG, Brussels Branch has its registered address at Marnixlaan 13-15, B-1000 Brussels, registered at the RPM Brussels, under the number VAT BE 0418.371.094. Further details are available on request or can be found at www.deutschebank.be.

Kingdom of Saudi Arabia
Deutsche Securities Saudi Arabia Company (registered no. 07073-37) is regulated by the Capital Market Authority. Deutsche Securities Saudi Arabia may only undertake the financial services activities that fall within the scope of its existing CMA license. Principal place of business in Saudi Arabia: King Fahad Road, Al Olaya District, P.O. Box 301809, Faisaliah Tower, 17th Floor, 11372 Riyadh, Saudi Arabia.

United Kingdom
In the United Kingdom ("UK"), this publication is considered a financial promotion and is approved by DB UK Bank Limited on behalf of all entities trading as Deutsche Bank Wealth Management in the UK. Deutsche Bank Wealth Management is a trading name of DB UK Bank Limited. Registered in England & Wales (No. 00315841). Registered Office: 23 Great Winchester Street, London EC2P 2AX. DB UK Bank Limited is authorised and regulated by the Financial Conduct Authority and its Financial Services Registration Number is 140848. Deutsche Bank reserves the right to distribute this publication through any of its UK subsidiaries, and in any such case, this publication is considered a financial promotion and is approved by such subsidiary where it is authorised by the appropriate UK regulator (if such subsidiary is not so authorised, then this publication is approved by another UK member of the Deutsche Bank Wealth Management group that has the requisite authorisation to provide such approval).

Hong Kong
This document and its contents are provided for information only. Nothing in this document is intended to be an offer of any investment or a solicitation or recommendation to buy or to sell an investment and should not be interpreted or construed as an offer, solicitation or recommendation. To the extent that this document makes reference to any specific investment opportunity, its contents have not been reviewed. The contents of this document have not been reviewed by any regulatory authority in Hong Kong. You are advised to exercise caution in relation to the investments contained herein. If you are in any doubt about any of the contents of this document, you should obtain independent professional advice. This document has not been approved by the Securities and Futures Commission in Hong Kong nor has a copy of this document been registered by the Registrar of Companies in Hong Kong and, accordingly, (a) the investments (except for investments which are a "structured product", as defined in the Securities and Futures Ordinance (Cap. 571 of the Laws of Hong Kong) (the "SFO")) may not be offered or sold in Hong Kong by means of this document or any other document other than to "professional investors" within the meaning of the SFO and any rules made thereunder, or in other circumstances which do not result in the document being a "prospectus" as defined in the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32 of the Laws of Hong Kong) ("CO") or which do not constitute an offer to the public within the meaning of the CO and (b) no person shall issue or possess for the purposes of issue, whether in Hong Kong or elsewhere, any advertisement, invitation or document relating to the investments which is directed at, or the contents of which are likely to be accessed or read by, the public in Hong Kong (except if permitted to do so under the securities laws of Hong Kong) other than with respect to the investments which are or are intended to be disposed of only to persons outside Hong Kong or only to "professional investors" within the meaning of the SFO and any rules made thereunder.

Singapore
The contents of this document have not been reviewed by the Monetary Authority of Singapore ("MAS"). The investments mentioned herein are not allowed to be made to the public or any members of the public in Singapore other than (i) to an institutional investor under Section 274 or 304 of the Securities and Futures Act (Cap 289) ("SFA"), as the case may be (as any such Section of the SFA may be amended, supplemented and/or replaced from time to time), (ii) to a relevant person (which includes an Accredited Investor) pursuant to Section 275 or 305 and in accordance with other

Important information

conditions specified in Section 275 or 305 respectively of the SFA, as the case may be (as any such Section of the SFA may be amended, supplemented and/or replaced from time to time), (iii) to an institutional investor, an accredited investor, expert investor or overseas investor (each as defined under the Financial Advisers Regulations) ("FAR") (as any such definition may be amended, supplemented and/or replaced from time to time) or (iv) otherwise pursuant to, and in accordance with the conditions of, any other applicable provision of the SFA or the FAR (as the same may be amended, supplemented and/or replaced from time to time).

United States
In the United States, brokerage services are offered through Deutsche Bank Securities Inc., a broker-dealer and registered investment adviser, which conducts securities activities in the United States. Deutsche Bank Securities Inc. is a member of FINRA, NYSE and SIPC. Banking and lending services are offered through Deutsche Bank Trust Company Americas, member FDIC, and other members of the Deutsche Bank Group. In respect of the United States, see earlier statements made in this document. Deutsche Bank makes no representations or warranties that the information contained herein is appropriate or available for use in countries outside of the United States, or that services discussed in this document are available or appropriate for sale or use in all jurisdictions, or by all counterparties. Unless registered, licensed as otherwise may be permissible in accordance with applicable law, none of Deutsche Bank or its affiliates is offering any services in the United States or that are designed to attract US persons (as such term is defined under Regulation S of the United States Securities Act of 1933, as amended).This United States-specific disclaimer will be governed by and construed in accordance with the laws of the State of Delaware, without regard to any conflicts of law provisions that would mandate the application of the law of another jurisdiction.

Germany
This document has been created by Deutsche Bank Wealth Management, acting through Deutsche Bank AG and has neither been presented to nor approved by the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht). For certain of the investments referred to in this document, prospectuses have been approved by competent authorities and published. Investors are required to base their investment decision on such approved prospectuses including possible supplements. Further, this document does not constitute financial analysis within the meaning of the German Securities Trading Act (Wertpapierhandelsgesetz) and, thus, does not have to comply with the statutory requirements for financial analysis. Deutsche Bank AG is a stock corporation ("Aktiengesellschaft") incorporated under the laws of the Federal Republic of Germany with principal office in Frankfurt am Main. It is registered with the district court ("Amtsgericht") in Frankfurt am Main under No HRB 30 000 and licensed to carry on banking business and to provide financial services. Supervisory authorities: The European Central Bank ("ECB"), Sonnemannstrasse 22, 60314 Frankfurt am Main, Germany and the German Federal Financial Supervisory Authority ("Bundesanstalt für Finanzdienstleistungsaufsicht" or "BaFin"), Graurheindorfer Strasse 108, 53117 Bonn and Marie-Curie-Strasse 24-28, 60439 Frankfurt am Main, Germany.

India
The investments mentioned in this document are not being offered to the Indian public for sale or subscription. This document is not registered and/or approved by the Securities and Exchange Board of India, the Reserve Bank of India or any other governmental/ regulatory authority in India. This document is not and should not be deemed to be a "prospectus" as defined under the provisions of the Companies Act, 2013 (18 of 2013) and the same shall not be filed with any regulatory authority in India. Pursuant to the Foreign Exchange Management Act, 1999 and the regulations issued there under, any investor resident in India may be required to obtain prior special permission of the Reserve Bank of India before making investments outside of India including any investments mentioned in this document.

Italy
This report is distributed in Italy by Deutsche Bank S.p.A., a bank incorporated and registered under Italian law subject to the supervision and control of Banca d'Italia and CONSOB.

Luxembourg
This report is distributed in Luxembourg by Deutsche Bank Luxembourg S.A., a bank incorporated and registered under Luxembourg law subject to the supervision and control of the Commission de Surveillance du Secteur Financier.

Spain
Deutsche Bank, Sociedad Anónima Española is a credit institution regulated by the Bank of Spain and the CNMV, and registered in their respective Official Registries under the Code 019. Deutsche Bank, Sociedad Anónima Española may only undertake the financial services and banking activities that fall within the scope of its existing license. The principal place of business in Spain is located in Paseo de la Castellana number 18, 28046 - Madrid. This information has been distributed by Deutsche Bank, Sociedad Anónima Española.

Portugal
Deutsche Bank AG, Portugal Branch is a credit institution regulated by the Bank of Portugal and the Portuguese Securities Commission ("CMVM"), registered with numbers 43 and 349, respectively and with commercial registry number 980459079. Deutsche Bank AG, Portugal Branch may only undertake the financial services and banking activities that fall within the scope of its existing license. The registered address is Rua Castilho, 20, 1250-069 Lisbon, Portugal. This information has been distributed by Deutsche Bank AG, Portugal Branch.

Important information

Austria
This document is distributed by Deutsche Bank AG Vienna Branch, registered in the commercial register of the Vienna Commercial Court under number FN 140266z. Deutsche Bank AG is a public company incorporated under German law and authorized to conduct banking business and provide financial services. It is supervised by the European Central Bank (ECB), Sonnemannstraße 22, 60314 Frankfurt am Main, Germany and by the Federal Financial Supervisory Authority (BaFin), Graurheindorfer Straße 108, 53117 Bonn, Germany and Marie-Curie-Strasse 24-28, 60439 Frankfurt am Main, Germany. The Vienna branch is also supervised by the Austrian Financial Market Authority (FMA), Otto-Wagner Platz 5, 1090 Vienna. This document has neither been submitted to nor approved by the aforementioned supervisory authorities. Prospectuses may have been published for certain of the investments mentioned in this document. In such a case, investment decisions should be made solely on the basis of the published prospectuses, including any annexes. Only these documents are binding. This document constitutes marketing material for informational and promotional purposes only and is not the result of any financial analysis or research.

The Netherlands
This document is distributed by Deutsche Bank AG, Amsterdam Branch, with registered address at De entree 195 (1101 HE) in Amsterdam, the Netherlands, and registered in the Netherlands trade register under number 33304583 and in the register within the meaning of Section 1:107 of the Netherlands Financial Supervision Act (Wet op het financieel toezicht). This register can be consulted through www.dnb.nl.

051039 021522