HSBC Global Research

Free to View
Disruptive Technology – ESG
Global | Thematic research

April 2021
www.research.hsbc.com

By: Davey Jose, Antonin Baudry, Faizan Lakhani and Amy Tyler

SPOTLIGHT

Age of Cybersecurity

Spend to defend

As cyber attacks on states, companies and individuals grow, spending on security is set to rise rapidly

But there is a potential underspend in cybersecurity despite the heightened risks to industry and governments

We explore the cybersecurity ecosystem and examine ESG, financial, and reputational issues at stake

Play video with Davey Jose

This is an abridged version of a report by the same title published on 29-Apr-21. Please contact your HSBC representative or email AskResearch@hsbc.com for more information.

Contents

Cybersecurity and investor insights	**3**
Age of Cybersecurity	**5**
What is cybersecurity today?	**In the full piece**
Financial, stock market and insurance implications	**In the full piece**
Enterprise cybersecurity	**In the full piece**
State level cybersecurity	**In the full piece**
Cyber breach case studies	**In the full piece**
Disclosure appendix	**12**
Disclaimer	**14**

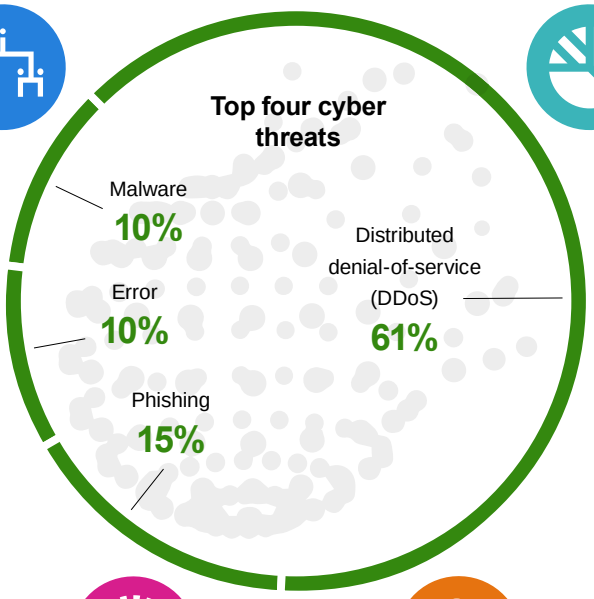
Cybersecurity and investor insights

Digitisation implies investment opportunities in the value chain

Cloud – as industries become further digitised, cyber security products follow suit

Governance – firms are experiencing more severe cyber attacks, resulting in significant financial and reputational damage

Financial – cyber attacks and data breaches can have significant impacts on a company, both from a financial/ operational perspective and via stock market moves



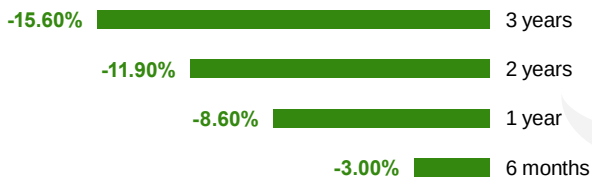
Social – substantial disruption and stress for individuals involved because of stolen data or loss of confidence in digitisation and technology

Enterprise – the security market space is fragmented and competitive. Global and regional players supply network security and services to multiple sectors

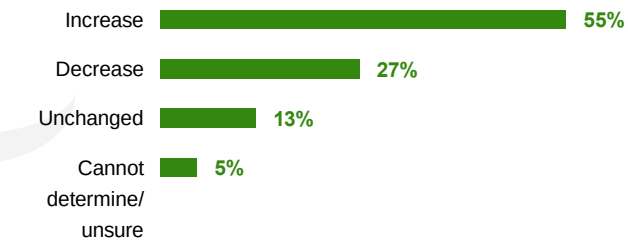
Environment – threats pose a significant challenge for utilities with pressure on efficiency rather than data breaches

Governments – become more efficient and offer enhanced digital services to continue to strengthen security

Average underperformance of a NASDAQ-listed company following a data breach announcement



Cybersecurity budgets are set to increase in 2021



Facts and figures

USD10.5trn

Annual costs of global cyber crime by 2025, up from USD3trn in 2015

14.5% CAGR

Global cybersecurity spend set to grow between 2020 and 2026

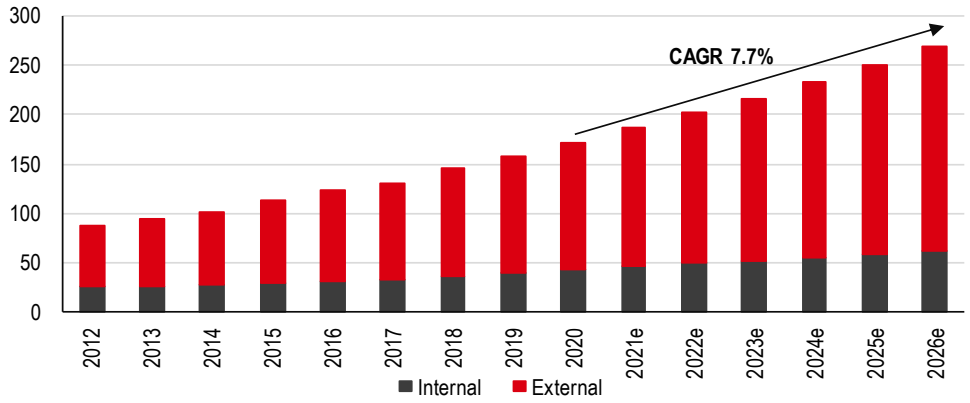
USD20bn

Global cyber insurance market set to grow by 2025 (from USD7bn)

Source: HSBC, Comparitech, Cybersecurity Ventures, Verizon, Munich Re

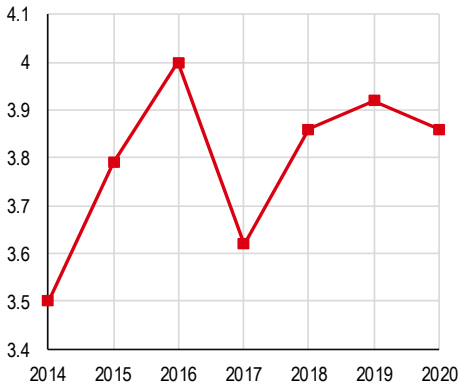
Age of Cybersecurity in charts

Chart 1. Global cybersecurity spend: projected CAGR 7.7% 202026 (USDbn annually)



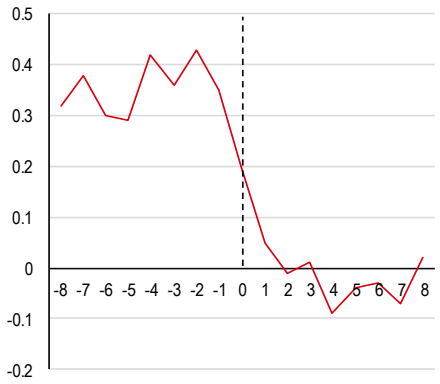
Source: HSBC, Cybersecurity Intelligence

Chart 2. Average cost of a data breach has increased by over 10% since 2014 (USDm)



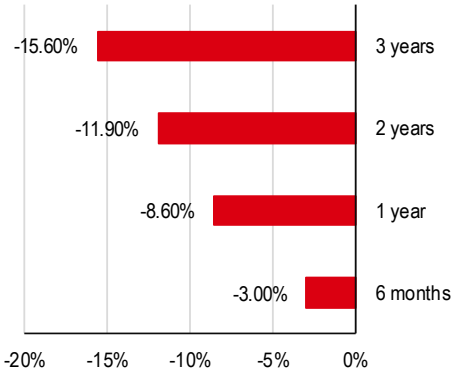
Source: Ponemon Institute.
NB. research across 524 organisations in 17 different industries.

Chart 3. Cyber breaches impact reputation of firms in quarters post data breach (2005-16) (y-axis: reputation rating*)



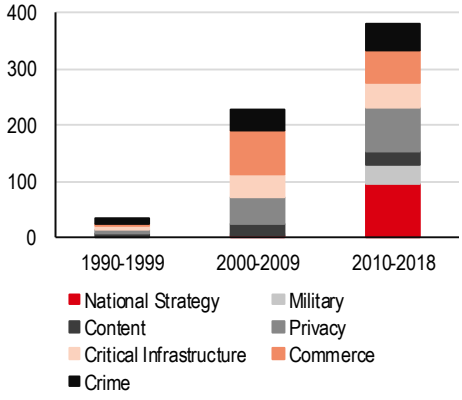
Source: Rotman School of Management, Note: * = reputation rating based on a number of reputation risk issues

Chart 4. Longer term, share prices underperform NASDAQ post data breach (2007-2020)



Source: HSBC, Comparitech

Chart 5. Cybersecurity regulations globally have increased tenfold since the 1990s



Source: HSBC, CSIS

This is an abridged version of a report by the same title published on 29-Apr-21. Please contact your HSBC representative or email AskResearch@hsbc.com for more information

Age of Cybersecurity

- As digitisation of everything (DoE) grows, it will bring digital vulnerabilities, allowing global inflicted damages from cyber crime to grow from USD6trn to USD10trn by mid-2020s
- There is potential underspend in cybersecurity, but as country level regulations catch up, cybersecurity technology providers could benefit, with 14.5% cyber spend CAGR into the middle of the decade
- Cybersecurity will have ESG implications, via potential disruption to connected national infrastructure and emerging markets

Why do we need cybersecurity?

> **Shall we play a game?**
>
> **Joshua/WOPR in War Games (1983)**

From movies to reality

The 1980s motion picture War Games dramatised a worst-case scenario from hacking, leading to potential global thermonuclear war. Since the early days of largely unconnected computer systems in the 1980s, today almost everything is becoming increasingly connected to the internet, from your work computer and home smart fridge, to large industrial critical infrastructure. The importance of cybersecurity in a digital inter-connected world is clear: to protect these interconnected systems from a variety of digital attacks, thus safeguarding the day to day functioning of the global economy.

Growth of digitisation implies cybersecurity investment opportunity

Physical to digital security

Security technologies have played an important role in preventing harm to various aspects of the operation and functioning of civilisation for eons. One could suggest that security technology has evolved from being purely physical in the past to more digital in the data-centric world in which we now reside. Society and industry have gone from being protected by physical walls around cities to having invisible digital firewalls on our computers in the 21st century.

Plenty of digital growth upside in 2020s…

As our global economy becomes more digital, inter-connected and networked, the threats posed to nation states and industry by various entities will only increase. Even though it feels like technology is everywhere today, the world isn't fully digitised yet. Only 30% of software currently resides in the cloud, only 5% of warehouses are deemed fully automated, only 5% of factories are "smart" and only 20% of payments are through digital wallets so far. These digitisations are only set to grow over the coming decade.

A positive for those providing cybersecurity products, solutions and services

Even with this current level of digitisation, in 2021, cyber crime is still estimated to cost a total of USD6 trillion in inflicted damages – equivalent in size to the third largest economy after the US and China. Cyber crime inflicted damages are expected to grow to over USD10 trillion by 2025[1]. The threat of

1 Cyber crime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. Cybersecurity Ventures, 2020

cyber crime can come from a multitude of sources including hackers, insiders, competitors, industrial spies, organised crime groups, nation states and terrorists. Moreover, cybersecurity spend is expected to grow up to 14.5% CAGR from 2020 to 2026. If digitisation numbers for various industries grow faster than expected, then we believe cyber crime opportunities could balloon further.

Key highlights

Below are some of the key takeaways from the full report. Please contact your HSBC representative or email AskResearch@hsbc.com for more information

- ***What is cybersecurity today?***

Types of cyber threats…

  - This section includes the fundamental types of cyber attack, real-world examples and the costs they inflict on an organisation. From malware to DNS tunnelling attacks, global cyber crime is expected to cost USD10.5 trillion globally in inflicted damages by 2025. With this, the rise in cybersecurity spending is expected to reach up to USD270 billion per annum by 2026. The impact of the COVID-19 pandemic has accelerated spending on cybersecurity, with over 50% of budgets increasing due to remote working environments and the increased challenges this brings for businesses.

Types of cybersecurity…

  - Types of cybersecurity are outlined, with companies that provide such services included. Over 50% of cybersecurity spending is on security services, including monitoring and managing security functions. Cybersecurity solutions for enterprises are examined in the section with the rise of Security Operations Centres, or SOC-as-a-Service (SOCaaS) companies and managed security services introducing automation and artificial intelligence. Additionally, the analysis of cybersecurity hardware, firmware and the evolution of payments is explored, with 63% of firms experiencing at least one breach due to vulnerabilities in hardware security and the impact of card-not-present transactions representing over 70% of card frauds across regions in 2019.

- ***Financial, stock market and insurance implications***

Financial costs from cyber attacks

  - It's probably not a surprise that cyber attacks and data breaches experienced by organisations can have significant impacts on a company, both from a financial and operational perspective and stock market moves. Therefore, it's important to understand fully the extent of such impacts. This section outlines the increasing costs of a data breach on organisations: with a 10% rise in costs since 2014, the average cost is currently USD3.86 million per breach. Real-world examples observe the number of records breached and the costs or fines faced by the companies. For example, Capital One were fined USD80 million for a data breach in 2019 that exposed 106 million customer accounts.

Reputational harm from cyber breaches

  - Not only is financial loss a significant impact of data breaches, but reputational damage can have long-term impacts on an organisation. On average, business reputation doesn't begin to recover until eight quarters following a data breach announcement.

Stock market and insurance implications from cyber incidents

  - Additionally, this section explores the stock market impact of data breaches, observing underperformance against stock market indices, such as the NASDAQ, on average down 15.60% in the three years following a data breach announcement. Observable is the variance of market reactions towards data breaches, with some companies experiencing significant falls in their stock prices, and others observing very little or no impact. Comparing sectors, on average finance experienced the greatest decline in stock prices, following an announcement, of -16.7% against the NASDAQ, in comparison to the technology sector, which averaged -2.9%. This begs the question as to whether companies should invest in cybersecurity solutions. This section explores this, with the expectation of increased fines and data breach notification laws, increasing the cost of cyber attacks on businesses and the impact on the stock market,

making investments worthwhile. With the development of cybersecurity solutions comes insurance for cyber attacks, with the market expected to grow 20-30% annually in the face of increasing digital threats, becoming a USD25bn market by 2025.

- ***Enterprise cybersecurity***

Types of enterprise cybersecurity companies

- Enterprise cybersecurity comprises firms that provide cybersecurity products and services, and those who consume them. We outline the competitive nature of the market for cybersecurity and the range of firms providing these services, with some very specialised in one sector, such as Fortified Health Security for the healthcare industry, or those broader providers such as Cisco, which service multiple industries. Financial Services is the sector most covered by the cybersecurity firms included in this report, with cloud security the most popular product provided by these firms.

Cybersecurity impacts by sector

- This section also drills down into specific sectors that consume cybersecurity products and services, with examples of those that provide these services. Healthcare has been particularly hit by cyber attacks in the last year, with a 60% increase in attacks globally since the start of the pandemic. The transport and logistics industries are facing increasing threats via the increased uptake of IoT devices, and the automotive sector is observing increased use of connected devices, with 67% of new cars in the UK connected to the internet, and expectations of 100% connection by 2026. The financial sector faces the most costs of a data breach on average. It has experienced a 54% increase in reported cyber incidents since the beginning of the pandemic; with the increase in remote working, physical security becomes a challenge also. We also analyse the cyber threats faced by the manufacturing, agriculture and government sectors in this section.

- ***State level cybersecurity***

The rise of cybersecurity spend in national defence budgets

- This chapter looks at the role of the state at a national level of cybersecurity. Globally, digitalisation has increased rapidly, which grows the threat of cyber attacks on infrastructure of national security importance. Therefore, defence budgets are increasingly including cybersecurity as a main feature and focus of resources. This section summarises cybersecurity spend where available for the regions included, as well as examples of key cybersecurity contracts awarded by national governments.

Who gains from national cyber spend?

- Governments' cybersecurity budgets are expected to increase. An example is the UK, where GBP1.5 billion extra will be injected into cybersecurity over the next four years. Some companies, such as Google, are beginning to reject government contracts owing to the misalignment of company principles for the use of such technologies.

National cybersecurity regulations

- Regulations of cyber and data breaches are moving forward around the world, which could put more pressure on companies to increase investment in cyber defence, as well as being important factors for investors

- ***Cyber breach case studies***

We highlight interesting cyber breach case studies

- This chapter outlines ten key examples of cyber breaches and their impact on the affected company's share price, with comparison to local stock market indices. We chose case studies via notable falls in share prices, such as the Equifax breach in 2017, which resulted in a 32% decline over the week following the cyber breach announcement, with the stock underperforming the S&P500 for the following nine months. Additionally, we look at case studies where a significant number of individuals were impacted, that included sensitive information, and which resulted in fines or substantial costs.

- One example is the Capital One breach in 2019, which impacted 106 million consumers, and included information such as credit card numbers. The company was fined USD80 million. The share price fell 6% and underperformed the S&P for four months; however, there was little change following the announcement of the fine.
- Case studies include charts illustrating the share price changes versus stock market indices including the CAC, S&P500 and FTSE100. Prices are based to 100 on the cyber breach announcement date, with two to three months prior and six to nine months post-breach to illustrate performance comparison.

ESG implications from cybersecurity

Naturally cybersecurity ticks all three components of ESG. These are the key ideas embedded within the report:

Connected national infrastructure could pose environmental issues if not protected

- **Environment** – In 2019, sPower, a Utah-based solar power energy generation provider, experienced a DDoS (distributed denial-of-service) attack, which disconnected the generation source with the power grid. Often hackers' aims are power shortages rather than stealing data, which highlights concerns over future attacks on renewables as regions become more reliant on them. By 2030, 54% of the electricity mix in Europe is expected to be renewable to meet targets[2].

  With the increased use of remote monitoring, intelligent connected devices and increased automation, cyber threats pose a significant challenge for utilities, especially with the pressure of efficiency of operations being a primary concern for companies. For example the renewable energy sector, which is expected to expand by 10% in 2021[3] could increasingly become a target for cyber attacks as it grows in importance to being a part of the infrastructure of nation states. Environmental concerns lie with attacks that can cause environmental damage or prevent organisations fulfilling operations.

  Sectors where we believe cybersecurity has environmental implications include agriculture, manufacturing and renewables. See the chapter *Enterprise cybersecurity*.

The elderly, enterprises and emerging markets link cybersecurity and other social risks

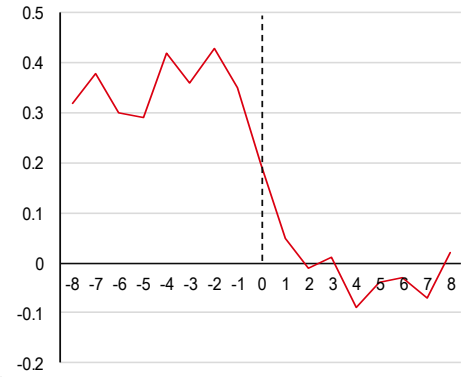
- **Social** – Impacts of cyber attacks can go beyond financial damage, with substantial disruption for individuals involved, whether it's the stress caused by stolen data or the loss of confidence in technology. As consumers, those impacted by a cyber attack experience disruption to daily life, especially when financial loss or interruption of essential resources such as energy is involved. The older population become particularly targeted, with those aged 55 and over losing around GBP3.7m between 2018 and 2019 due to cyber crime[4].

  From an enterprise point of view, there's the risk of employee demoralisation and reputational damage as a result of a cyber breach, Chart A1 illustrates the impact on firms' reputations, which on average, doesn't begin to recover until eight quarters post-breach.

  Less economically developed regions such as Africa are particularly vulnerable due to lack of cybersecurity infrastructure and knowledge. Cyber crime cost the continent USD3.5 billion in 2017, with a worrying 96% of cyber incidents unreported or unsolved[5]. Chart A2 includes countries within the region with particularly high cyber crime costs.

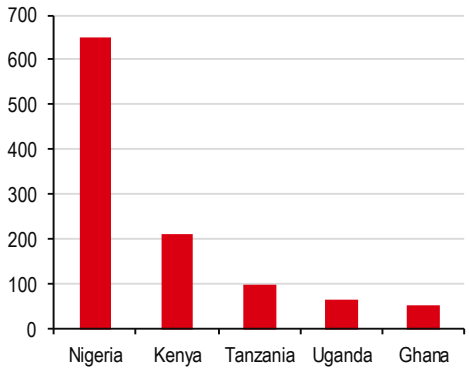
2 'Renewable technologies in the EU electricity sector: trends and projections', European Commission, 2017
3 'Renewables 2020', IEA, Nov 2020
4 'Uncovering the extent of cybercrime across the UK', Age UK, 2020
5 'Africa Cyber Security Report 2017', Serianu, 2017

Chart A1. Cyber breaches impact reputation of firms in quarters post data breach (2005-16) (y-axis: reputation rating*)



Source: Rotman School of Management, Note: * = reputation rating based on a number of reputation risk issues

Chart A2. Countries with significant cyber crime costs across Africa (USDm) (2017)



Source: HSBC, Africa Cyber Security Report

Cyber breaches are governance issues for enterprise, bringing long-term stock market impacts

- **Governance** – Increasingly, firms are experiencing cyber attacks at greater volumes and severity, resulting in significant financial and reputational damage. With fines and cyber breach notification regulations on the rise – such as the UK's DPA 2018 amendment increasing the maximum fine of GBP0.5m to GBP17.5m or 4% of turnover – cyber risk is progressively becoming a principal risk for corporations and their boards.

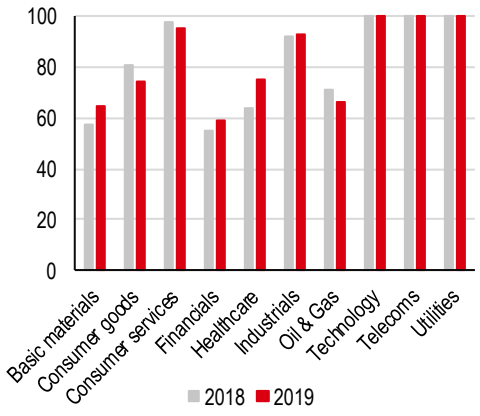
  In 2018, 89% of FTSE 100 companies disclosed an element of cyber risk as a principal risk to the delivery of their strategy in their annual reports. However, only 8% of boards had a Chief Information Security Officer (CISO) as part of their executive team[6].

  In addition, cyber risk has for a long time not been reflected in the typical composition of boards. More than one-third of the FTSE 350, who report technology and cyber security as a key risk to their business, do not have directors with relevant expertise on their boards. This rises to half or more when it comes to the oil and gas, consumer goods and financial sectors.[7] In an attempt to tackle this situation and improve risk oversight and mitigation, many sectors saw a rise in board appointments of directors with cyber or wider information technology expertise. However, this approach may not be effective for all companies as any appointment has to be considered against the other strategic demands of the business. We think the focus should be on strengthening bespoke training for the board and executive team and using other available resources, for example establishing advisory panels to enable effective strategic board conversations on cyber security issues.

  The impact of COVID-19 has intensified the need for focus on cyber security, with 70% of organisations stating that remote working increases the cost of a data breach and 76% stating that it would take longer to identify and contain such breach[8].

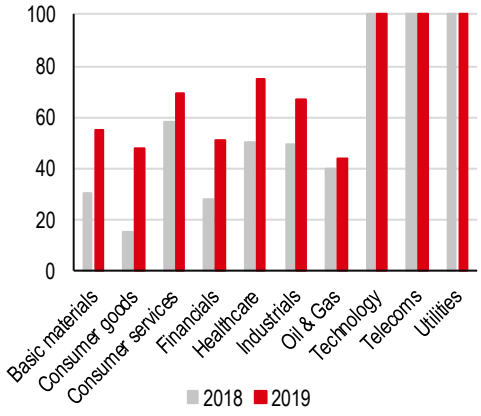
6 'Only 1 in 5 FTSE 100 firms have cyber risk testing programmes', Teiss, 28 March 2018
7 Grant Thornton Corporate Governance Review 2019
8 'Cost of a Data Breach Report', Ponemon Institute, 2020

Chart A3. % of companies disclosing technology as a key risk…



Source: HSBC, Grant Thornton Corporate Governance Review

Chart A4. …and % of those that have technology expertise on the board



Source: HSBC, Grant Thornton Corporate Governance Review

With cyber attacks potentially having significant impacts on share prices, investors are especially focused on cyber security as a critical aspect of company valuation. According to PwC and its Seven Principles for Governance of Cyber Security Risk, 73% of investors identified cyber security as an area of concern. With a growing number of data breach disclosure regulations being introduced, such as in Australia in 2018, the resulting public knowledge of cyber attacks could impact the stock market to greater effect than before.

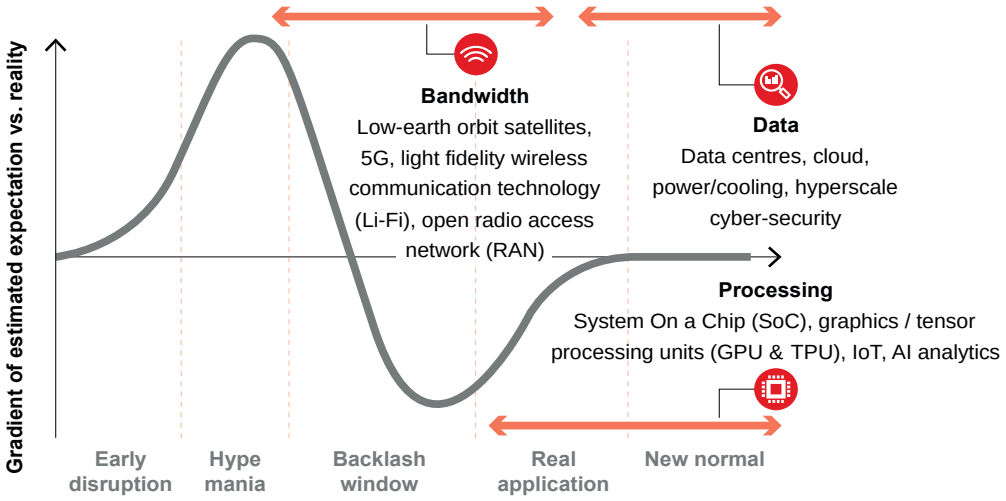
See chapters *Financial, stock market and insurance implications* and *State level cybersecurity* for more detail relating to cyber attacks and governance issues, for companies and countries.

HSBC Disruptive Framework and cybersecurity

Cybersecurity is in the "new normal" part of our disruption framework…

In our report *The Edge of Disruption* (22 November 2020), we outlined our four key disruptive technological themes (connectivity, automation, experiential and digital health) and explained why the pandemic has accelerated their adoption with industry and society. We also created the HSBC Disruption Framework for each of these themes, placing the different technologies in this framework to help investors understand how mature the innovation is and if it's ready to become the new normal, disrupt business models and have economic implications.

Chart A5. HSBC Disruption Framework: Connectivity infrastructure



Source: HSBC

This means cybersecurity is an essential part of enterprises and can generate significant revenues for technology providers

With the rise of data-centric businesses and the digital state, all connected, the value of data increases. It's estimated that there will be three internet of things (IoT) devices in existence for every person by next year.[9] At the same time, social commerce continues to rise, with more brands focusing on direct-to-consumer selling and relationships.

However, this also means there is the risk of bad actors trying to breach security and obtain data or take systems off-line. Bad actors can use these digital entry points to offer an expansive attack surface in the form of connected devices, digital storefronts and engagement tools.

Products, services and solutions for technology stack is in the "new normal" part of our framework, as cyber security is an essential part of businesses with connectivity. For consumer-focused organisations, this means a higher risk of data breaches and loss if the right protocols and technologies are not in place. As a result, we expect to see product and platform security come to the forefront next year, particularly as organisations realize the value that consumers place in trust, privacy, and security.

The next evolution of cybersecurity will be to deploy AI to automate security further – we suggest this is in the "real applications" stage of the framework, so not necessarily the main part of revenue generation for cyber yet.

This is an abridged version of a report by the same title published on 29-Apr-21. Please contact your HSBC representative or email AskResearch@hsbc.com for more information

9 Cap Gemini

Disclosure appendix

Analyst Certification

The following analyst(s), economist(s), or strategist(s) who is(are) primarily responsible for this report, including any analyst(s) whose name(s) appear(s) as author of an individual section or sections of the report and any analyst(s) named as the covering analyst(s) of a subsidiary company in a sum-of-the-parts valuation certifies(y) that the opinion(s) on the subject security(ies) or issuer(s), any views or forecasts expressed in the section(s) of which such individual(s) is(are) named as author(s), and any other views or forecasts expressed herein, including any views expressed on the back page of the research report, accurately reflect their personal view(s) and that no part of their compensation was, is or will be directly or indirectly related to the specific recommendation(s) or views contained in this research report: Davey Jose, Antonin Baudry, Faizan Lakhani, Amy Tyler, Herald van der Linde, CFA, Wai-Shin Chan, CFA, Jonathan Day, Yaryna Kobel, Thomas Fossard and Steven Haywood

Important disclosures

Equities: Stock ratings and basis for financial analysis

HSBC and its affiliates, including the issuer of this report ("HSBC") believes an investor's decision to buy or sell a stock should depend on individual circumstances such as the investor's existing holdings, risk tolerance and other considerations and that investors utilise various disciplines and investment horizons when making investment decisions. Ratings should not be used or relied on in isolation as investment advice. Different securities firms use a variety of ratings terms as well as different rating systems to describe their recommendations and therefore investors should carefully read the definitions of the ratings used in each research report. Further, investors should carefully read the entire research report and not infer its contents from the rating because research reports contain more complete information concerning the analysts' views and the basis for the rating.

From 23rd March 2015 HSBC has assigned ratings on the following basis:

The target price is based on the analyst's assessment of the stock's actual current value, although we expect it to take six to 12 months for the market price to reflect this. When the target price is more than 20% above the current share price, the stock will be classified as a Buy; when it is between 5% and 20% above the current share price, the stock may be classified as a Buy or a Hold; when it is between 5% below and 5% above the current share price, the stock will be classified as a Hold; when it is between 5% and 20% below the current share price, the stock may be classified as a Hold or a Reduce; and when it is more than 20% below the current share price, the stock will be classified as a Reduce.

Our ratings are re-calibrated against these bands at the time of any 'material change' (initiation or resumption of coverage, change in target price or estimates).

Upside/Downside is the percentage difference between the target price and the share price.

Prior to this date, HSBC's rating structure was applied on the following basis:

For each stock we set a required rate of return calculated from the cost of equity for that stock's domestic or, as appropriate, regional market established by our strategy team. The target price for a stock represented the value the analyst expected the stock to reach over our performance horizon. The performance horizon was 12 months. For a stock to be classified as Overweight, the potential return, which equals the percentage difference between the current share price and the target price, including the forecast dividend yield when indicated, had to exceed the required return by at least 5 percentage points over the succeeding 12 months (or 10 percentage points for a stock classified as Volatile*). For a stock to be classified as Underweight, the stock was expected to underperform its required return by at least 5 percentage points over the succeeding 12 months (or 10 percentage points for a stock classified as Volatile*). Stocks between these bands were classified as Neutral.

*A stock was classified as volatile if its historical volatility had exceeded 40%, if the stock had been listed for less than 12 months (unless it was in an industry or sector where volatility is low) or if the analyst expected significant volatility. However, stocks which we did not consider volatile may in fact also have behaved in such a way. Historical volatility was defined as the past month's average of the daily 365-day moving average volatilities. In order to avoid misleadingly frequent changes in rating, however, volatility had to move 2.5 percentage points past the 40% benchmark in either direction for a stock's status to change.

Rating distribution for long-term investment opportunities

As of 29 April 2021, the distribution of all independent ratings published by HSBC is as follows:

Buy	58%	(29% of these provided with Investment Banking Services)
Hold	34%	(28% of these provided with Investment Banking Services)
Sell	8%	(25% of these provided with Investment Banking Services)

For the purposes of the distribution above the following mapping structure is used during the transition from the previous to current rating models: under our previous model, Overweight = Buy, Neutral = Hold and Underweight = Sell; under our current model Buy = Buy, Hold = Hold and Reduce = Sell. For rating definitions under both models, please see "Stock ratings and basis for financial analysis" above.

For the distribution of non-independent ratings published by HSBC, please see the disclosure page available at http://www.hsbcnet.com/gbm/financial-regulation/investment-recommendations-disclosures.

To view a list of all the independent fundamental ratings disseminated by HSBC during the preceding 12-month period, please use the following links to access the disclosure page:

Clients of Global Research and Global Banking and Markets: www.research.hsbc.com/A/Disclosures

Clients of HSBC Private Banking: www.research.privatebank.hsbc.com/Disclosures

HSBC and its affiliates will from time to time sell to and buy from customers the securities/instruments, both equity and debt (including derivatives) of companies covered in HSBC Research on a principal or agency basis or act as a market maker or liquidity provider in the securities/instruments mentioned in this report.

Analysts, economists, and strategists are paid in part by reference to the profitability of HSBC which includes investment banking, sales & trading, and principal trading revenues.

Whether, or in what time frame, an update of this analysis will be published is not determined in advance.

Non-U.S. analysts may not be associated persons of HSBC Securities (USA) Inc, and therefore may not be subject to FINRA Rule 2241 or FINRA Rule 2242 restrictions on communications with the subject company, public appearances and trading securities held by the analysts.

Economic sanctions imposed by the EU, the UK, the USA, and certain other jurisdictions generally prohibit transacting or dealing in any debt or equity issued by Russian SSI entities on or after 16 July 2014 (Restricted SSI Securities). Economic sanctions imposed by the USA also generally prohibit US persons from purchasing or selling publicly traded securities issued by companies designated by the US Government as "Communist Chinese military companies" (CMCs) or any securities that are derivative of, or designed to provide investment exposure, to the targeted CMC securities (collectively, Restricted CMC Securities). This report does not constitute advice in relation to any Restricted SSI Securities or Restricted CMC Securities, and as such, this report should not be construed as an inducement to transact in any Restricted SSI Securities or Restricted CMC Securities.

For disclosures in respect of any company mentioned in this report, please see the most recently published report on that company available at www.hsbcnet.com/research. HSBC Private Banking clients should contact their Relationship Manager for queries regarding other research reports. In order to find out more about the proprietary models used to produce this report, please contact the authoring analyst.

Additional disclosures

1 This report is dated as at 29 April 2021.

2 All market data included in this report are dated as at close 23 April 2021, unless a different date and/or a specific time of day is indicated in the report.

3 HSBC has procedures in place to identify and manage any potential conflicts of interest that arise in connection with its Research business. HSBC's analysts and its other staff who are involved in the preparation and dissemination of Research operate and have a management reporting line independent of HSBC's Investment Banking business. Information Barrier procedures are in place between the Investment Banking, Principal Trading, and Research businesses to ensure that any confidential and/or price sensitive information is handled in an appropriate manner.

4 You are not permitted to use, for reference, any data in this document for the purpose of (i) determining the interest payable, or other sums due, under loan agreements or under other financial contracts or instruments, (ii) determining the price at which a financial instrument may be bought or sold or traded or redeemed, or the value of a financial instrument, and/or (iii) measuring the performance of a financial instrument or of an investment fund.

Disclaimer

Legal entities as at 1 December 2020

'UAE' HSBC Bank Middle East Limited, DIFC; HSBC Bank Middle East Limited, Dubai; 'HK' The Hongkong and Shanghai Banking Corporation Limited, Hong Kong; 'TW' HSBC Securities (Taiwan) Corporation Limited; 'CA' HSBC Securities (Canada) Inc.; 'France' HSBC Continental Europe; 'Spain' HSBC Continental Europe, Sucursal en España; 'Italy' HSBC Continental Europe, Italy; 'Sweden' HSBC Continental Europe Bank, Sweden Filial; 'DE' HSBC Trinkaus & Burkhardt AG, Düsseldorf; 000 HSBC Bank (RR), Moscow; 'IN' HSBC Securities and Capital Markets (India) Private Limited, Mumbai; 'JP' HSBC Securities (Japan) Limited, Tokyo; 'EG' HSBC Securities Egypt SAE, Cairo; 'CN' HSBC Investment Bank Asia Limited, Beijing Representative Office; The Hongkong and Shanghai Banking Corporation Limited, Singapore Branch; The Hongkong and Shanghai Banking Corporation Limited, Seoul Securities Branch; The Hongkong and Shanghai Banking Corporation Limited, Seoul Branch; HSBC Securities (South Africa) (Pty) Ltd, Johannesburg; HSBC Bank plc, London, Tel Aviv; 'US' HSBC Securities (USA) Inc, New York; HSBC Yatirim Menkul Degerler AS, Istanbul; HSBC México, SA, Institución de Banca Múltiple, Grupo Financiero HSBC; HSBC Bank Australia Limited; HSBC Bank Argentina SA; HSBC Saudi Arabia Limited; The Hongkong and Shanghai Banking Corporation Limited, New Zealand Branch incorporated in Hong Kong SAR; The Hongkong and Shanghai Banking Corporation Limited, Bangkok Branch; PT Bank HSBC Indonesia; HSBC Qianhai Securities Limited; Banco HSBC S.A.

Issuer of report
HSBC Bank plc
8 Canada Square
London, E14 5HQ, United Kingdom
Telephone: +44 20 7991 8888
Fax: +44 20 7992 4880
Website: www.research.hsbc.com

In the UK, this publication is distributed by HSBC Bank plc for the information of its Clients (as defined in the Rules of FCA) and those of its affiliates only. Nothing herein excludes or restricts any duty or liability to a customer which HSBC Bank plc has under the Financial Services and Markets Act 2000 or under the Rules of FCA and PRA. A recipient who chooses to deal with any person who is not a representative of HSBC Bank plc in the UK will not enjoy the protections afforded by the UK regulatory regime. HSBC Bank plc is regulated by the Financial Conduct Authority and the Prudential Regulation Authority. If this research is received by a customer of an affiliate of HSBC, its provision to the recipient is subject to the terms of business in place between the recipient and such affiliate.

HSBC Securities (USA) Inc. accepts responsibility for the content of this research report prepared by its non-US foreign affiliate. The information contained herein is under no circumstances to be construed as investment advice and is not tailored to the needs of the recipient. All U.S. persons receiving and/or accessing this report and wishing to effect transactions in any security discussed herein should do so with HSBC Securities (USA) Inc. in the United States and not with its non-US foreign affiliate, the issuer of this report.

In the European Economic Area, this publication has been distributed by HSBC Continental Europe or by such other HSBC affiliate from which the recipient receives relevant services

In Singapore, this publication is distributed by The Hongkong and Shanghai Banking Corporation Limited, Singapore Branch for the general information of institutional investors or other persons specified in Sections 274 and 304 of the Securities and Futures Act (Chapter 289) ("SFA") and accredited investors and other persons in accordance with the conditions specified in Sections 275 and 305 of the SFA. Only Economics or Currencies reports are intended for distribution to a person who is not an Accredited Investor, Expert Investor or Institutional Investor as defined in SFA. The Hongkong and Shanghai Banking Corporation Limited, Singapore Branch accepts legal responsibility for the contents of reports pursuant to Regulation 32C(1)(d) of the Financial Advisers Regulations. This publication is not a prospectus as defined in the SFA. This publication is not a prospectus as defined in the SFA. It may not be further distributed in whole or in part for any purpose. The Hongkong and Shanghai Banking Corporation Limited Singapore Branch is regulated by the Monetary Authority of Singapore. Recipients in Singapore should contact a "Hongkong and Shanghai Banking Corporation Limited, Singapore Branch" representative in respect of any matters arising from, or in connection with this report. Please refer to The Hongkong and Shanghai Banking Corporation Limited Singapore Branch's website at www.business.hsbc.com.sg for contact details.

In Australia, this publication has been distributed by The Hongkong and Shanghai Banking Corporation Limited (ABN 65 117 925 970, AFSL 301737) for the general information of its "wholesale" customers (as defined in the Corporations Act 2001). Where distributed to retail customers, this research is distributed by HSBC Bank Australia Limited (ABN 48 006 434 162, AFSL No. 232595). These respective entities make no representations that the products or services mentioned in this document are available to persons in Australia or are necessarily suitable for any particular person or appropriate in accordance with local law. No consideration has been given to the particular investment objectives, financial situation or particular needs of any recipient.

This publication has been distributed in Japan by HSBC Securities (Japan) Limited. It may not be further distributed, in whole or in part, for any purpose. In Hong Kong, this document has been distributed by The Hongkong and Shanghai Banking Corporation Limited in the conduct of its Hong Kong regulated business for the information of its institutional and professional customers; it is not intended for and should not be distributed to retail customers in Hong Kong. The Hongkong and Shanghai Banking Corporation Limited makes no representations that the products or services mentioned in this document are available to persons in Hong Kong or are necessarily suitable for any particular person or appropriate in accordance with local law. All inquiries by such recipients must be directed to The Hongkong and Shanghai Banking Corporation Limited. In Korea, this publication is distributed by The Hongkong and Shanghai Banking Corporation Limited, Seoul Securities Branch ("HBAP SLS") for the general information of professional investors specified in Article 9 of the Financial Investment Services and Capital Markets Act ("FSCMA"). This publication is not a prospectus as defined in the FSCMA. It may not be further distributed in whole or in part for any purpose. HBAP SLS is regulated by the Financial Services Commission and the Financial Supervisory Service of Korea. This publication is distributed in New Zealand by The Hongkong and Shanghai Banking Corporation Limited, New Zealand Branch incorporated in Hong Kong SAR.

In Canada, this document has been distributed by HSBC Securities (Canada) Inc. (member IIROC), and/or its affiliates. The information contained herein is under no circumstances to be construed as investment advice in any province or territory of Canada and is not tailored to the needs of the recipient. No securities commission or similar regulatory authority in Canada has reviewed or in any way passed judgment upon these materials, the information contained herein or the merits of the securities described herein, and any representation to the contrary is an offense. In Brazil, this document has been distributed by Banco HSBC S.A. ("HSBC Brazil"), and/or its affiliates. As required by Instruction No. 598/18 of the Securities and Exchange Commission of Brazil (Comissão de Valores Mobiliários), potential conflicts of interest concerning (i) HSBC Brazil and/or its affiliates; and (ii) the analyst(s) responsible for authoring this report are stated on the chart above labelled "HSBC & Analyst Disclosures".

This document is not and should not be construed as an offer to sell or the solicitation of an offer to purchase or subscribe for any investment. HSBC has based this document on information obtained from sources it believes to be reliable but which it has not independently verified; HSBC makes no guarantee, representation or warranty and accepts no responsibility or liability as to its accuracy or completeness. The opinions contained within the report are based upon publicly available information at the time of publication and are subject to change without notice. From time to time research analysts conduct site visits of covered issuers. HSBC policies prohibit research analysts from accepting payment or reimbursement for travel expenses from the issuer for such visits.

Past performance is not necessarily a guide to future performance. The value of any investment or income may go down as well as up and you may not get back the full amount invested. Where an investment is denominated in a currency other than the local currency of the recipient of the research report, changes in the exchange rates may have an adverse effect on the value, price or income of that investment. In case of investments for which there is no recognised market it may be difficult for investors to sell their investments or to obtain reliable information about its value or the extent of the risk to which it is exposed.

HSBC Bank plc is registered in England No 14259, is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority and is a member of the London Stock Exchange. (070905)

If you are an HSBC Private Banking ("PB") customer with approval for receipt of relevant research publications by an applicable HSBC legal entity, you are eligible to receive this publication. To be eligible to receive such publications, you must have agreed to the applicable HSBC entity's terms and conditions for accessing research and the terms and conditions of any other internet banking service offered by that HSBC entity through which you will access research publications ("the Terms"). Distribution of this publication is the sole responsibility of the HSBC entity with whom you have agreed the Terms. If you do not meet the aforementioned eligibility requirements please disregard this publication and, if you are a customer of PB, please notify your Relationship Manager. Receipt of research publications is strictly subject to the Terms and any other conditions or disclaimers applicable to the provision of the publications that may be advised by PB.

[1168969]