GLOBAL LONG-TERM UNCONSTRAINED

MARTIN CURRIE

JULY 2022

For institutional, professional and wholesale investors only

CYBERSECURITY

Cybersecurity breaches have been steadily rising, and there is a risk, given increased geopolitical tensions, that incidences of state-sponsored cybersecurity breaches could also be on the rise.

Zehrid Osmani

Head of Global Long-Term Unconstrained

Senior Portfolio Manager

Yulia Hofstede

Portfolio Manager

Defragmenting the market

There is an old adage that there are two types of corporates – those that have been victims of cybersecurity breaches, and those that don't know yet that they have been victims of a breach. This highlights the challenges faced by corporates to put in place efficient cybersecurity defences.

In our report, we assess both the threat and the opportunity from cybersecurity, examining the market's structure, dynamics and growth potential. Cybersecurity is a threat to corporate sustainability. Its consideration is a necessary and an important part of what constitutes good governance and sustainability practice.Therefore, we expand on the various ESG aspects we consider in our proprietary risk frameworks.

Executive summary

Cybersecurity breaches can impact every area of a business, it can lead to the theft of Intellectual Property (IP), ultimately damaging customer trust and brand reputation. These can have major financial repercussions, and negatively impact shareholder value.

Geopolitical threats and increasing sophistication are growing risks

Corporates' exposure to geopolitical risks are increasing with the growing emergence of nation-state backed attacks, such as the SolarWinds attack. Cyberattacks are becoming more sophisticated and are increasingly likely to go undetected for long periods of time – highlighting a significant impact for corporates.

Cybersecurity spending is outpacing wider IT investment

Corporate IT spend on cybersecurity is likely to continue to grow at a sustained pace, we forecast annualised growth of c.+20% to 2030e. This is far outpacing overall annualized corporate IT spending growth of c.+10% over the same period.[1]

Achieving security coverage will be challenging given market fragmentation and staff shortages

The cybersecurity market is extremely fragmented, with many companies operating in small niches. It is therefore challenging for companies to achieve the right level of security coverage through an integrated approach – an issue exacerbated by bottlenecks from staff shortages of cybersecurity professionals.

Artificial Intelligence (AI) is emerging as a risk and an opportunity

AI is an opportunity for corporates – but is also posing new risks. Automated type of attacks, algorithmic model-based and machine learning are relatively new developments. Most companies believe that they will not be able to respond to cyberattacks without AI.[2]

Cybersecurity is both a key Governance and Sustainability concern

Cybersecurity is a core area of risk for companies across all sectors, covering both the Governance and Sustainability of their business models. It is a board level consideration, which is increasingly being understood by the companies we cover.

[1]Source: Martin Currie internal estimates.

[2]Source: Statista and Cap Gemini, July 2019. Reinventing Cybersecurity with Artificial Intelligence.

Cybersecurity: a growing cost to corporates both financially and reputationally

By 2021, Cybercrime is forecasted to cost businesses US$6 trillion globally, this is versus US$3 trillion in 20153, that translates into $11m lost every minute. If it were a country, cybercrime damages would be the third-largest economy after the US and China.[3]

Cybersecurity is an important strategic consideration for companies. It is vital to protect intellectual property (IP) – and therefore its competitive advantages and stakeholders' data.

Cybersecurity breaches can lead to sizeable loss of revenues and have broader major financial repercussions for corporates, not least legal ones. The negative impact on shareholder value can be more sizeable than the financial repercussions when considering the permanent damage to customer trust and brand reputation. It is therefore an important matter of both governance and sustainability for any business, and a strategic dimension for both the board and senior management to consider.

Today's cyberthreats range from malware to phishing and web application attacks

Malware – Software with a malicious intent, this includes ransomware, viruses, worms and spyware.

Phishing – A fraudulent message designed to trick a person into revealing sensitive information

Man-in-the-middle attack – Perpetrator positions themselves in the conversation between a user and the application (i.e. banking app) to steal personal information

Denial-of-service attack – Shuts down a network or machine making it inaccessible to its users

SQL injection – Insertion of malicious code to access information

Zero-day exploit – Software vulnerability discovered by the attacker before the vendor

DNS tunnelling – Encoding data to covertly control a remote server or application

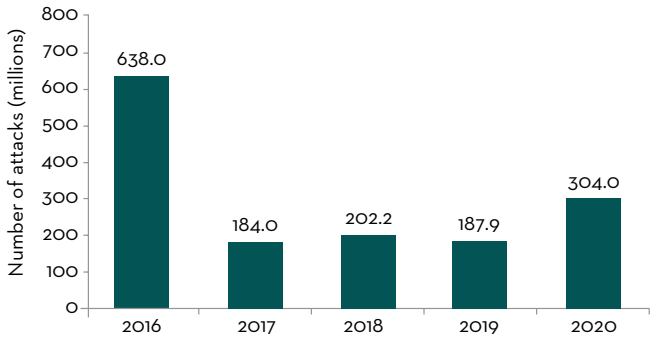
[3]Source: Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanachttps://cybersecurityventures.com/cybersecurity-almanac-2019/

Cybercrime forecast to cost US$6 trillion

Ransomware attacks remain abundant

Cybercrime was forecasted to cost businesses US$6 trillion globally in 2021. Specifically, global ransomware damage costs were forecasted to reach **US$20bn in 2021** versus US$5bn in 2017.[4] 2020 saw the second highest number of such attacks since 2016.

Annual number of ransomware attacks worldwide 2016 - 2020 (millions)



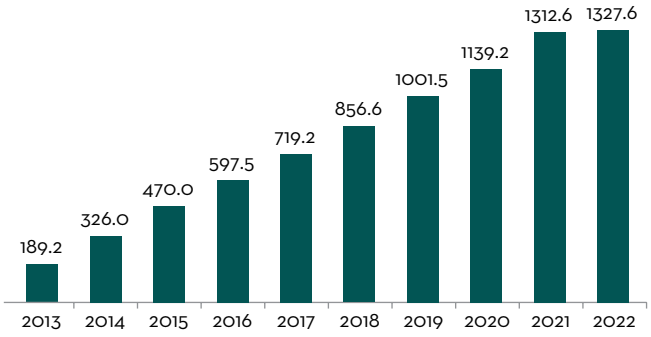
Source: Statista and SonicWall, March 2021. Annual number of ransomware attacks worldwide from 2016 to 2020 (in millions).

Malware programmes have doubled since 2015

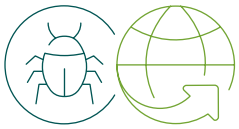
The malware industry is growing rapidly

Estimated to have surpassed **1 billion** known malware programmes in 2019 – more than doubling since 2015. According to the AV-Test Institute, the development rate is estimated at 4.8 samples per second.

Total malware programs (millions)



Source: AV-Test Institute's statistics (av-test.org), as of 14 February 2022. https://www.av-test.org

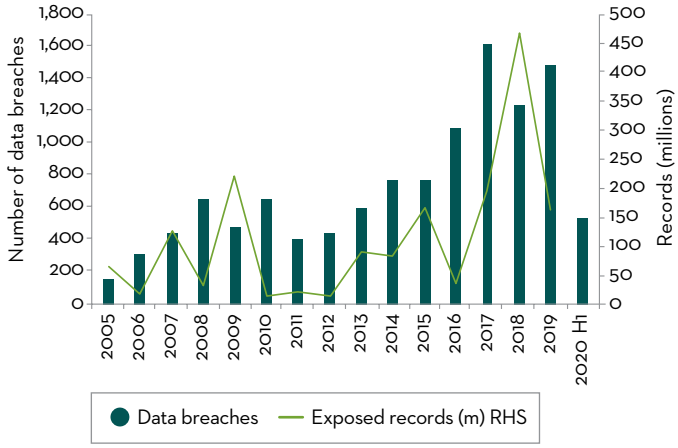


Increased digitalisation leading to a global phenomenon

Number of data breaches has been steadily increasing over the past two decades

This is due to **more abundant data and its digitalisation**. The chart opposite shows data breaches rising in the US, and is illustrative of the global phenomenon.

Number of data breaches and exposed records in USA 2005 - 2021



Source: Statista, Identity Theft Resource Center Survey published August 2020.

[4]Source: Cybersecurity Ventures. March 2021.

Understanding the risk: SolarWinds case study

A unique attack in terms of technical capability and breadth

"One of the most effective cyber-espionage campaigns of all time"

Alex Stamos, director of the Internet Observatory at Stanford University and the former head of security at Facebook

Supply chain attack

Executed through third party software that has access to the victims infrastructure.

Hackers gained access to SolarWinds production environment through an embedded backdoor in the Orion network monitoring product.

Customers were infected as they ran the firm's updates.

Government agencies impacted

Victims included US Treasury and the Pentagon

Full extent of the attack still unknown

Hackers may still have access to network despite patching

Revealed in December 2020
Over 100 companies compromised

Many lessons learned

Increased expenditure

Expected from US Government agencies

New approaches

Openness to explore novel approaches, new providers and tools

Call for greater collaboration

Microsoft CEO calls for greater collaboration between public and corporate sectors

What made this attack unique?

Technical capabilities

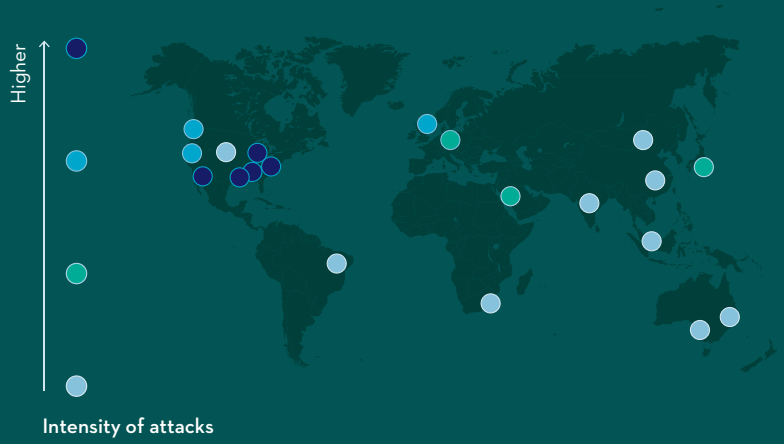
Knowledge of software development process

Breadth of attack

Global extent of supply chain vulnerability

Cautious approach

Hackers would wait two weeks before using backdoor

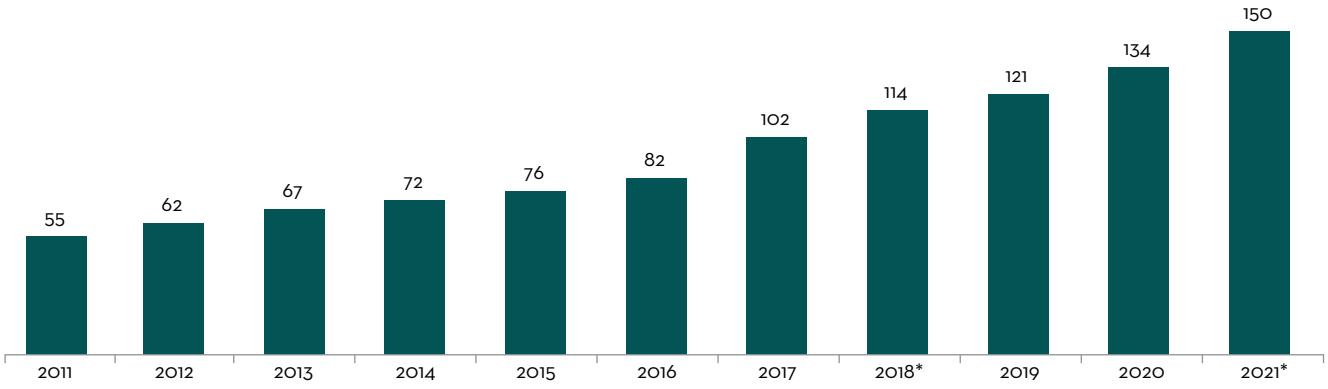


The cybersecurity market

Today's cybersecurity spend exceeds $120bn. According to Cybersecurity Ventures, this market was just $3.5bn in 2007. Over a 15-year period, it has therefore compounded at c.27%[5].

We expect compound annual growth of c.20% from the cybersecurity market to 2030, this is compared to c.10% from the wider IT sector over the same period[6]. Our definition of the cybersecurity market is broad, as we aim to capture the opportunity in the Internet of Things (IoT) and consumer categories. For example, increasingly cybersecurity spending is breaking out of the constraints of IT corporate budgets. Training, for example, might be an expense booked by an HR department.

Global information security products and services market revenue (US$ billion)



Evolving threat landscape

We see cybersecurity as an expansive market and the threat landscape has expanded beyond the enterprise domain – with the need to protect a company's data and resources from cyberthreats. IoT, the Industrial IoT and the consumer sector (e.g. smartphones) all fall outside this domain. Cloud computing and the broader definitions today of a mobile device have extended the edge of the cybersecurity market.

A particular challenge is the shortage of talent. A survey conducted in 2019, showed that 51% of cybersecurity professionals say their organisation is at moderate or extreme risk due to a cybersecurity staff shortage[7]. This could create bottlenecks for businesses getting the right level of cybersecurity coverage, as they deploy their IT budget in this area.

[5]Source: Gartner and Cybersecurity Ventures, June 2020. Gartner estimate for 2019, as of June 2020.

[6]Source: Martin Currie internal estimates, June 2022.

[7]Source: Darktrace ISC, April 2021. Darktrace IPO prospectus (ISC)2 (2019), "Strategies for Building and Growing Strong Cybersecurity Teams, Cybersecurity Workforce Study, 2019".

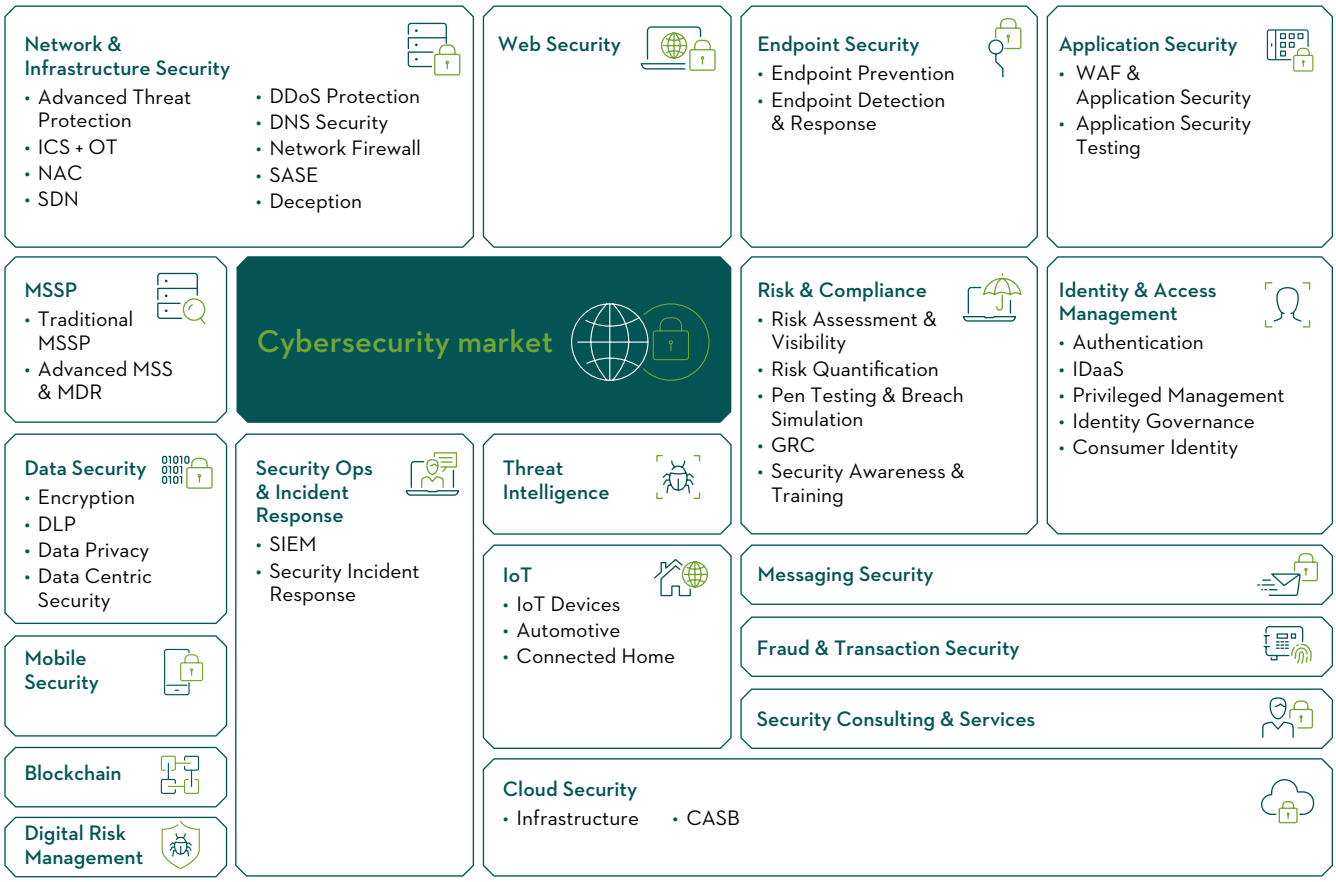
Landscape – a highly fragmented but consolidating market

Cybersecurity landscape – players, market shares, competitive positioning

The cybersecurity market is highly segmented, with areas such network and infrastructure security, access management, application security and cloud and data security to name but a few. It is evolving fast, IOT, blockchain and some areas within consumer security are categories that are yet to be defined.

The significant fragmentation within the market could lead to confusion within companies, with lack of standardisation potentially increasing the risk of weakness within the ecosystem. This is shown below:

A highly fragmented market



Tracking cybersecurity market share through time is particularly challenging. Although at times there are clear leaders in a segment, it is common for market positioning to change rapidly. This is through either market consolidation or new challengers advancing. According to Crunchbase Pro there are over 22,000 cybersecurity, privacy and security start-ups. In 2020, funding raising by start-ups exceeded US$10 billion versus US$2 billion 2010[8].

One market player we would highlight is the tech giant, Microsoft. It has been ramping up its bundling strategy, offering "end-to-end capabilities" across security, identity, compliance and risk management. It has been reported in the media[8], that Microsoft invests over US$1 billion p.a. to advance its security, data protection and risk management businesses.

We expect market consolidation to continue, in 2020 M&A activity remained robust amounting to US$20 billion[9].

The information provided should not be considered a recommendation to purchase or sell any particular strategy/ fund/security. It should not be assumed that any of the securities discussed here were or will prove to be profitable.

[8]Source: Forbes and Crunchbase Pro, 29 November 2020. The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase (forbes.com).

[9]Source: Momentum Cyber Security Almanac 2021, July 2021.

Opportunities and emerging trends

The security challenges of remote and hybrid working

With increased digitalisation and the accelerated migration to the Cloud from the normalisation of hybrid working, identities are expanding beyond people to include applications and machine identities. This creates an additional security risk.

Identity management ensures that only authorised entities have the access to technology resources they need to perform their job functions. Privileged identities give users the ability to control, manage, and monitor the access privileges that people have to crucial resources.

In such circumstances, endpoint detection and zero-trust deployment have become more important (described below), among other cybersecurity tools and techniques.

Endpoint detection is a behaviour-centric tool protecting remote devices. They continuously monitor workstations (and other endpoints) to identify threats when they happen.

Zero-trust deployment always assumes a breach and continuously validates every stage of a digital interaction.

Additionally, human error has been the biggest cybersecurity challenge during COVID-19 pandemic, according to the Cyberchrology paper "The Human Element" published by ESET in partnership with the Myers-Briggs Company[10].

Artificial Intelligence (AI)-powered attacks

Five years ago, application patching and basic network segmentation were the focus. Today, however, AI is posing new risks. New types of risk included automated attacks, algorithmic models and AI fuzzing, that uses machine learning.

Microsoft flagged a novel type of cyberthreat in a blog post in December 2020[11]. Here AI was used to spread targeted disinformation from stolen datasets about individuals using text messaging and encrypted messaging apps.

69% **69% of companies** believe they will not be able to respond to cyberattacks without AI, according to Capgemini's 2019 report[12].

88% **88% of companies** expect AI-powered attacks to become common[13].

The information provided should not be considered a recommendation to purchase or sell any particular strategy/ fund/security. It should not be assumed that any of the securities discussed here were or will prove to be profitable.

[10]Source: Cyberchrology and ESET, Myers Briggs as as date. The Human Element https://www.eset.com/uk/business/cyberchology/

[11]Source: Brad Smith and Microsoft, 17 December 2020. *A moment of reckoning: the need for a strong and global cybersecurity response – Microsoft On the Issues.*

[12]Source: Statista and Cap Gemini, July 2019. Reinventing Cybersecurity with Artificial Intelligence.

[13]Source: Darktrace and Forrester Consulting, March 2020. https://www.darktrace.com/en/press/2020/319/

Nation-state threats

Nation-state attacks have grown in sophistication. The SolarWinds attack (see previous case study on page 5), that counted several US government agencies amongst its victims, led to Microsoft's President Brad Smith in December 2020 to call for collaboration between the public and corporate sectors, to prevent and deal effectively with nation-state attacks[14].

Even prior to this attack, Microsoft flagged in its September 2020 Digital Defence Report, that nation-state actors are prepared to "play the long game" which makes detection harder.

The SolarWinds compromise was a supply chain attack executed through a 3rd party software provider. Since then, there have been renewed calls for a platform-type of approach to security, as opposed to using several standalone solutions. In our view there is positive brand equity for those companies who respond to the challenge and provide novel approaches.

Quantum cybersecurity

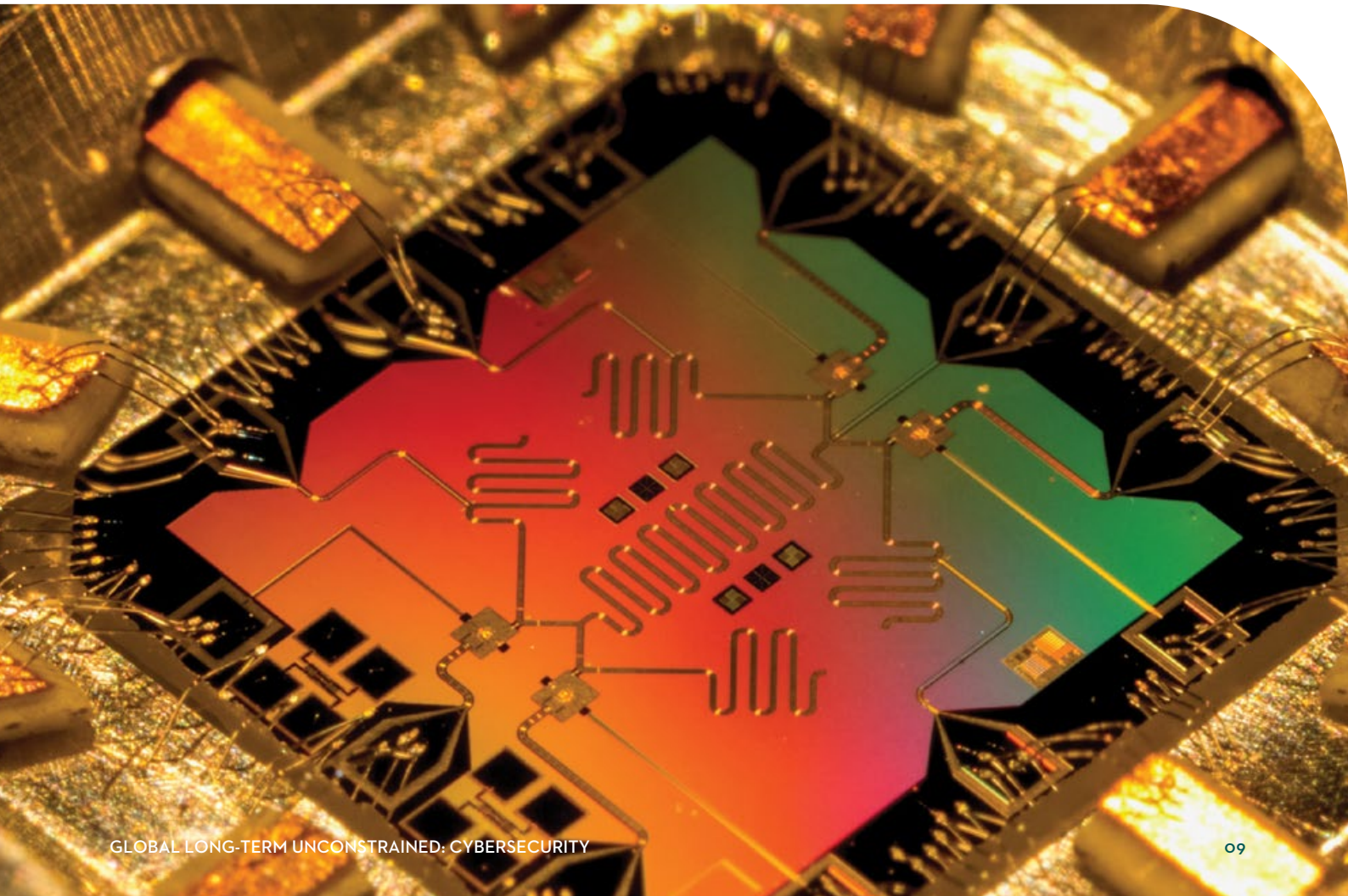
Quantum-secure communications, specifically quantum key distribution (QKD) is another emerging trend in the cybersecurity landscape. It is one which can provide both stronger cybersecurity barriers – but also more challenging cyberattacks if used for negative purposes.

We are of the view that China is furthest ahead on quantum communication. Media reports[15] have suggested that Chinese scientists set up an integrated network using fiber transmission and via satellite, have established a realised QKD over a combined distance of 4,600km. The fiber link of over 2,000km is significantly longer than any QKD transmission distance achieved previously. Meanwhile, the QKD satellite is the only known one in operation, as opposed to proofs of concept.

Moreover, China's QuantumCTek Group rolled out in June 2021 smartphones equipped with a super SIM card, allowing users to make quantum encrypted phone calls[15].

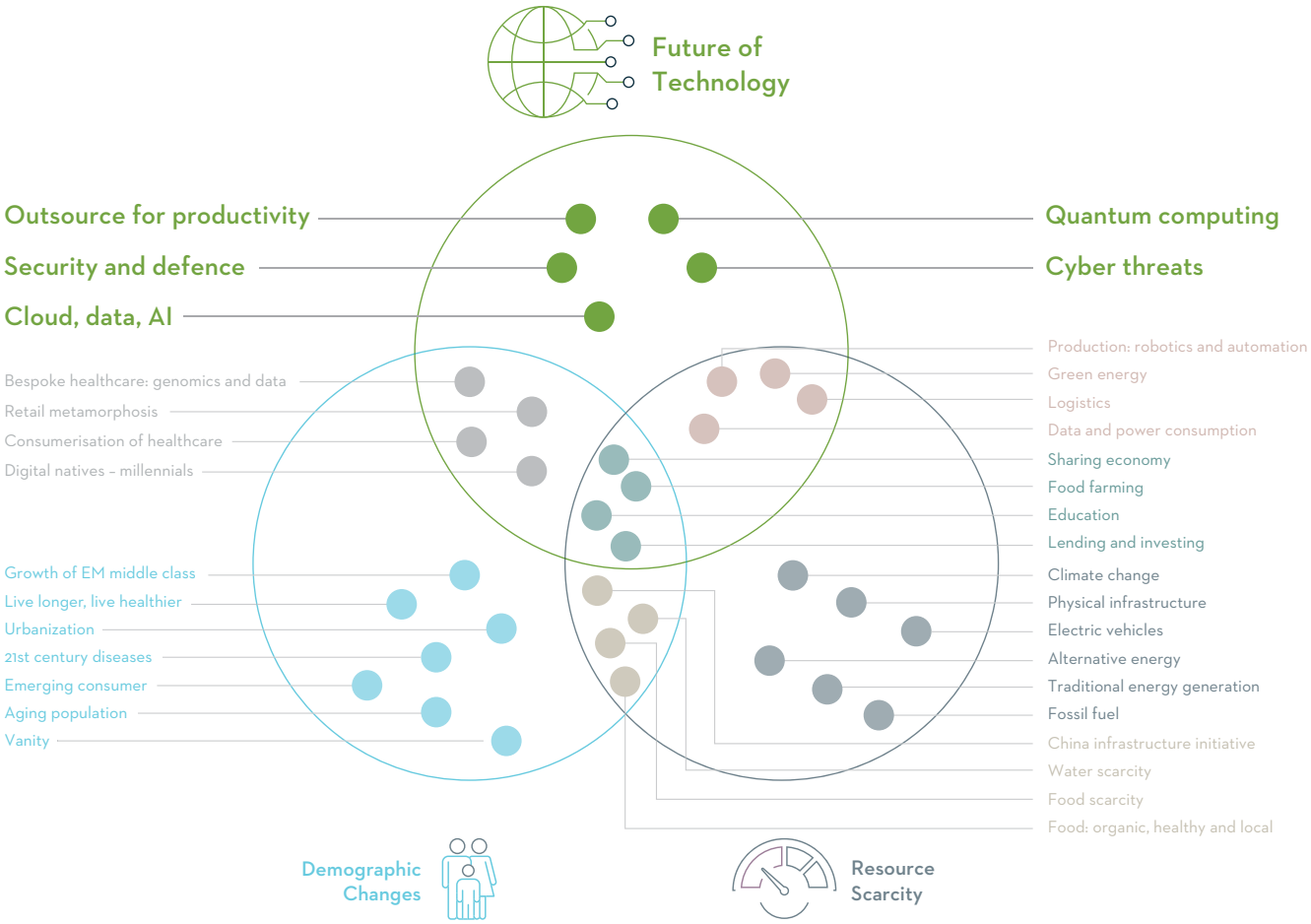
[14]Source: Brad Smith and Microsoft, 17 December 2020. *A moment of reckoning: the need for a strong and global cybersecurity response* https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

[15]Source: People Daily Online, 7 January 2021. *China realizes secure, stable quantum communications network spanning 4,600km.*



Thematic framework

Related sub-themes



Assessing cybersecurity risk

Our Governance and Sustainability framework

We analyse cybersecurity using our proprietary Governance and Sustainability risk assessment. Cybersecurity represents one of the five common factors that we use assess each business's Sustainability risks. It is also captured through our Governance analysis. This is through our assessment of the board and their understanding of cyberthreats and, whether these are included in the firm's corporate targets. The table below details our framework, highlighting the cybersecurity risk field specifically. We risk assess each category from 1 (lowest risk) to 5 (highest risk).

We have carried an intensive period of engagement with each corporate across our research coverage. This is to better understand their approach to the cybersecurity risks faced by their businesses. We will expand on this in a future report. Given the importance of cybersecurity as a threat to a business's reputation, impact on customer trust and ultimately shareholder value – this ensures we assess in detail how companies tackle this threat.

Given the importance of cybersecurity as a threat to a business's reputation, impact on customer trust and ultimately shareholder value – this ensures we assess in detail how companies tackle this threat.

Governance — 2.3

Board assessment			3		
Management score		2			
Remuneration			3		
Culture			3		
Stake vs Shareholders conflict	1				
Governance Momentum		2			

Board assessment — 2.5

Board quality			**3**		
Board independence			**3**		
Board diversity, age and tenure		**2**			
Board oversight			**3**		
Board competence			**3**		
Board accessibility		**2**			
Chairperson quality				**4**	
Audit Committee	**1**				
Significant votes against	**1**				
Shareholder rights alignment			**3**		

Management — 2.3

Management Quality			3		
Management breadth			3		
Management depth		2			
Management Competence		**2**			
Management accessibility	1				
Accounting practices / quality		2			
Crisis management			3		

Remuneration — 2.4

Remuneration alignment			3		
Remuneration transparency	1				
Remuneration appropriateness				4	
Remuneration disparity	1				
Remuneration benchmark			3		

Culture — 2.6

Corporate Culture			3		
Sustainability focus			3		
Diversity			3		
Integrity & ethics		2			
Relationship with stakeholders		2			

Sustainability — 2.0

Environmental risks	1				
Social risks	1				
Understanding and integration		2			
Common Factors risks			3		
Sustainability momentum			3		

Environmental risks — 1.4

Carbon footprint	1				
Pollution risk	1				
Resources risk	1				
Supply chain		2			
Environmental momentum		2			

Social risks — 2.2

Social Impact		2			
Social improvements		2			
Exploitation risk	1				
Political lobbying		2			
Overall involvement			3		
Social momentum			3		

Understanding and integration — 2.2

Understanding of material risks and opps		2			
Management of risks and opps		2			
Highest level of ownership		2			
Integration into strategy	1				
Integration into remuneration			3		
Integration into reporting			3		

Common Factors — 2.2

Climate Change	1				
Cyber Security			**3**		
Human Capital			3		
Customer Trust		**2**			
Taxation		2			

Data shown is for illustrative purposes only.

Important information

This information is issued and approved by Martin Currie Investment Management Limited ('MCIM'), authorized and regulated by the Financial Conduct Authority. It does not constitute investment advice. Market and currency movements may cause the capital value of shares, and the income from them, to fall as well as rise and you may get back less than you invested.

The information contained in this document has been compiled with considerable care to ensure its accuracy. However, no representation or warranty, express or implied, is made to its accuracy or completeness. Martin Currie has procured any research or analysis contained in this document for its own use. It is provided to you only incidentally and any opinions expressed are subject to change without notice. This document may not be distributed to third parties. It is confidential and intended only for the recipient. Therecipient may not photocopy, transmit or otherwise share this document, or any part of it, with any other person without the express written permission of Martin Currie Investment Management Limited.

This document is intended only for a wholesale, institutional or otherwise professional audience. Martin Currie Investment Management Limited does not intend for this document to be issued to any other audience and it should not be made available to any person who does not meet this criteria. Martin Currie accepts no responsibility for dissemination of this document to a person who does not fit this criteria. The document does not form the basis of, nor should it be relied upon in connection with, any subsequent contract or agreement. It does not constitute, and may not be used for the purpose of, an offer or invitation to subscribe for or otherwise acquire shares in any of the products mentioned.

Past performance is not a guide to future returns.

The distribution of specific products is restricted in certain jurisdictions, investors should be aware of these restrictions before requesting further specific information. The views expressed are opinions of the portfolio managers as of the date of this document and are subject to change based on market and other conditions and may differ from other portfolio managers or of the firm as a whole. These opinions are not intended to be a forecast of future events, research, a guarantee of future results or investment advice.

Some of the information provided in this document has been compiled using data from a representative account. This account has been chosen on the basis it is an existing account managed by Martin Currie, within the strategy referred to in this document. Representative accounts for each strategy have been chosen on the basis that they are the longest running account for the strategy. This data has been provided as an illustration only, the figures should not be relied upon as an indication of future performance. The data provided for this account may be different to other accounts following the same strategy.

The information should not be considered as comprehensive and additional information and disclosure should be sought.

The information provided should not be considered a recommendation to purchase or sell any particular strategy/fund/security. It should not be assumed that any of the security transactions discussed here were or will prove to be profitable.

The analysis of Environmental, Social and Governance (ESG) factors forms an important part of the investment process and helps inform investment decisions. The strategy/ies do not necessarily target particular sustainability outcomes.

Risk warnings – Investors should also be aware of the following risk factors which may be applicable to the strategy shown in this document.

- Investing in foreign markets introduces a risk where adverse movements in currency exchange rates could result in a decrease in the value of your investment.
- This strategy may hold a limited number of investments. If one of these investments falls in value this can have a greater impact on the strategy's value than if it held a larger number of investments.
- Smaller companies may be riskier and their shares may be less liquid than larger companies, meaning that their share price may be more volatile.
- Emerging markets or less developed countries may face more political, economic or structural challenges than developed countries. Accordingly, investment in emerging markets is generally characterised by higher levels of risk than investment in fully developed markets.
- Income strategy charges are deducted from capital. Because of this, the level of income may be higher but the growth potential of the capital value of the investment may be reduced.

For wholesale investors in Australia

Any distribution of this material in Australia is by Martin Currie Australia ('MCA'). Martin Currie Australia is a division of Franklin Templeton Australia Limited (FTAL), (ABN 76 004 835 849).

Franklin Templeton Australia Limited is a wholly owned subsidiary of Franklin Resources, Inc., and holds an Australian Financial Services Licence (AFSL No. 240827) issued pursuant to the Corporations Act 2001.

For institutional investors in the USA

The information contained within this presentation is for Institutional Investors only who meet the definition of Accredited Investor as defined in Rule 501 of the United States Securities Act of 1933, as amended ('The 1933 Act') and the definition of Qualified Purchasers as defined in section 2 (a) (51) (A) of the United States Investment Company Act of 1940, as amended ('the 1940 Act'). It is not for intended for use by members of the general public.

MARTIN CURRIE

Martin Currie Investment Management Limited, registered in Scotland (no SC066107)
Martin Currie Inc, incorporated in New York and having a UK branch registered in Scotland (no SF000300),
Saltire Court, 20 Castle Terrace, Edinburgh EH1 2ES

Tel: (44) 131 229 5252 Fax: (44) 131 222 2532 **www.martincurrie.com**

Both companies are authorised and regulated by the Financial Conduct Authority. Martin Currie Inc, 280 Park Avenue New York, NY 10017 is also registered with the Securities Exchange Commission. Please note that calls to the above number and any other communications may be recorded.