HSBC Global Research

Disruptive Technology

20 December 2022

Disruption Bytes

Cyber, metaverse and powering the data revolution

Free to View
Disruptive Technology - Global

- **Cybersecurity:** Have ransomware cyber incidence rates peaked and which country is proposing a ban on ransomware payments?
- **Powering the data revolution:** Are US droughts a threat to big tech data centres and what is being done to mitigate this?
- **Metaverse:** How are updated chipsets allowing AR glasses to bridge the gap with VR headsets?

Henry Ward*
Thematic Analyst, Disruptive Technologies
HSBC Bank plc

Davey Jose*
Thematic Analyst, Disruptive Technologies
HSBC Bank plc

Faizan Lakhani*
Analyst, Insurance
HSBC Bank plc

Nicolas Cote-Colisson*
Global Head of Communications Equity Research
HSBC Bank plc

Frank Lee*
Head of Technology Research, Asia
The Hongkong and Shanghai Banking Corporation Limited

** Employed by a non-US affiliate of HSBC Securities (USA) Inc, and is not registered/ qualified pursuant to FINRA regulations*

In this free to view note, we summarize some recent developments within HSBC's Disruptive Technology Theme you may have missed, highlighting potential implications investors should note.

Cybersecurity… In our report, *Cyberdemic*, we provided a number of case studies on cybersecurity breaches. And our report, *Future cybersecurity*, warned investors that ransomware was on the rise and the preferred tactic for digital crime. We take a look at the latest response from a government to two very significant cyber breaches and what's happening with ransomware incidence rates.

Powering the data revolution… In our report, *The Water Crisis*, our ESG analysts warned about the risks we face from water scarcity. Over half of the US is facing drought conditions and data centres on average have the daily water consumption of 100,000 households – which is leading to tensions in local communities. We explore what Amazon, Google, and Microsoft are doing to reduce their water consumption.

The augmented metaverse… In our report, *The Metaverse Age*, we highlighted that AR glasses and headsets exist but are less advanced than VR headsets, particularly due to the complexity of the optics technology required for AR. However, a new, smaller and more powerful chipsets are helping AR glasses bridge the gap and become a reality.

This is a redacted version of a report with the same title published on 20-Dec-22. Please contact your HSBC representative or email AskResearch@hsbc.com for more information or to request reports mentioned above.

Issuer of report: HSBC Bank plc

View HSBC Global Research at:
https://www.research.hsbc.com

Disruption Bytes

- **Cybersecurity:** Have ransomware cyber incidence rates peaked and which country is proposing a ban on ransomware payments?
- **Powering the data revolution:** Are US droughts a threat to big tech data centres and what is being done to mitigate this?
- **The augmented metaverse:** Which company has taken a potential leap forward to making AR glasses a reality and who's using it?

To ban or not to ban ransomware payments?

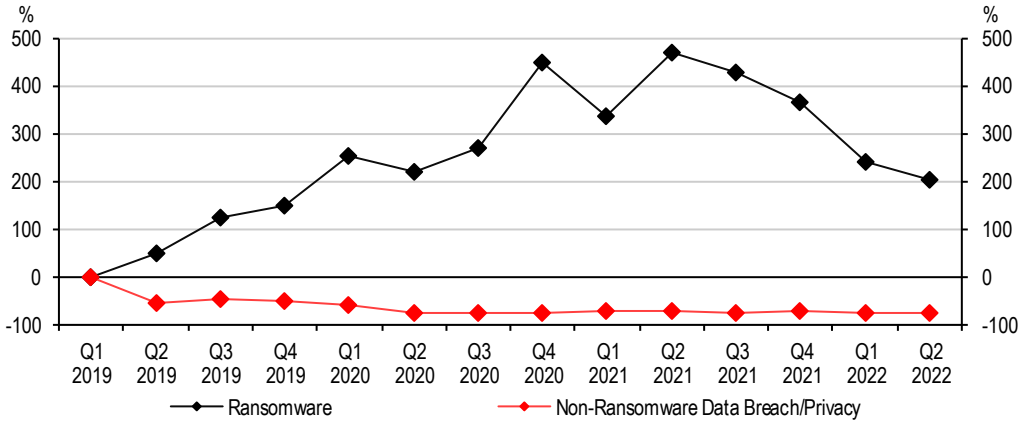
Ransomware growth outstrips non-ransomware data and privacy breaches

Have ransomware attacks peaked?

In some of our recent reports, we explored the nature of global cyber-attacks, how they were changed by the pandemic (through work from home trends) and how the threat of ransomware was growing. Furthermore, a panel of experts we hosted back on 18 May 2022 outlined that ransomware and phishing were still the preferred cyber threat methods.

However, ransomware attack growth appears to have peaked in Q2 2021 (up +469% to Q1 2019 levels). As of Q2 2022, they have fallen to +204% of those Q1 2019 levels[1].

Cyber incident rates (percentage change relative to Q1 2019)



Source: Aon

[1] E&O and Cyber Market Review – Midyear 2022, Aon, September 2022

A number of national bodies are considering banning ransomware payments as a way to counteract the wave of ransomware attacks seen in 2020:

North Carolina & Florida are first states to ban payments from public agencies

- In April 2022 North Carolina became the first US state to prohibit state agencies and local government from paying ransoms resulting from ransomware attacks. Public entities are even banned from communicating with the attacker[2]. Florida became the second state to enact similar legislation which prohibits state and local government entities from making ransomware payments[3]. In recent years New York, Pennsylvania, and Texas have also considered legislation that would ban government agencies from paying ransomware. However, the legislation in Texas fell flat in committee and was not considered by legislators[4].

Already restrictions on ransom payments e.g. sanctions, terrorism

- In 2021 the Dutch government considered banning ransom payments by insurers[5]. Whilst it is not expressly illegal to pay ransoms in the UK, US, and EU there are a number of restrictions when paying ransom. For instance, many cyber-criminal groups have financial sanctions against them and thus a ransom payment could not be made to these groups. It is also illegal pay ransom to a group suspected of terrorism[6] .

Australia is considering a ban on ransom payments after two significant breaches

- Australia's Home Affairs Minister Clare O'Neil has announced that the government is considering banning the payment of ransoms to cyber criminals. This follows a significant cyber-attack on Australia's largest health insurer Medibank Private (which compromise data of 10 million current and former customers), as well as on Australia's second largest telecommunications company Optus[7].

Will ransomware payment bans work?

The proposal looks like it is supported by the public and experts but has its critics

The proposal has had mixed reactions from experts, with some believing it would remove the profit incentive from these cyber threats and thus lower the rate of attacks. Whilst others have said it would only result in more personal data leaks across the dark web[8]. According to Venafi, a private cybersecurity company, 18% of those who paid ransoms had their data leaked anyway and 35% were unable to recover their data despite having paid[9] - advancing the belief that the ban could be effective. According to cybersecurity firm Talion, 78% of the UK public would support such a ban and 79% of cybersecurity professionals support such a ban[10].

Some say it could lead to a lack of transparency and the United States FBI agrees

However, others have suggested that organisations will likely still pay despite any legislative action, which would lead to an underreporting of attacks and a lack of transparency with regulators and law enforcement[11]. This specific concern was cited by the US Federal Bureau of Investigation in its recommendation to the Senate Judiciary Committee to not ban all ransom payments in July 2021[12].

Related key reports

- Please contact your HSBC representative for details on related reports.

[2] Not in My Backyard: NC Becomes First State to Prohibit Public Entities from Paying Ransoms, The National Law Review, 5 April 2022
[3] Florida's New Ransomware and Cybersecurity Requirements/Restrictions, JDSUPRA, 11 July 2022
[4] States Consider Legislation to Ban Ransomware Payments, Government Technology, 26 July 2021
[5] Dutch government considering ban on ransom payments by insurers, Pinsent Masons, 28 September 2021
[6] Is it legal to pay ransomware demands?, Cyance
[7] Australia to consider banning paying of ransoms to cyber criminals, Reuters, 14 November 2022
[8] Australia wants to ban ransomware payments, The Washington Examiner, 17 November 2022
[9] Australia wants to ban ransomware payments, The Washington Examiner, 17 November 2022
[10] Australia is considering a ban on cyber ransom payments, but it could backfire. Here's another idea, The Conversation, 14 November 2022
[11] Australia Considers Ban on Ransomware Payments to Decrease Profitability of Data Breaches, Tech News, 17 November 2022
[12] FBI tells Congress ransomware payments shouldn't be banned, CNN, 27 July 2021

Are US droughts a threat to big tech data centres?

Growth of data centres, strain on water and citizen concerns…

Data centres water consumption has caused concerns for years

According to the Synergy Research Group the number of "hyperscale" data centres globally had doubled between 2015-2020 and 40% of those are in the US – with Amazon, Google, and Microsoft accounting for more than half of that total[13]. Moreover, the Water Resources Centre at Texas Tech University has said that a typical data centre uses 3-5 million gallons of water per day – the equivalent amount of water as a city of 30,000-50,000 people[14].

Lack of company disclosure for water risks at data centres

20% of data centres draw water from moderate to high stress drought areas

Concerns were raised by local residents over summer 2022 about water scarcity and data centres, for instance, about 20% of data centres in the US rely on watersheds that were under moderate to high stress from drought[15]. Despite this according to Sustainalytics, of 122 companies it looked at that operated data centres only 16% of them disclosed their plans for water related risks[16]. And this is not just a US problem, in August 2022 The Times reported concerns over data centres water usage in the UK during a drought[17].

US droughts creating risks to data centres

Big tech companies are facing a drought risk to their data centres

In November 2022, amid worsening drought conditions in the US, CNBC reported that big tech companies were facing a drought risk to their data centres[18]. Companies have made commitments to lower their water usage, for instance, Meta ran a pilot programme (which has now been implemented in all of its data centres) to lower its relative humidity from 20% to 13% to lower its water usage in Los Lunas, New Mexico and Microsoft has claimed it wants to replenish more water than it consumes by 2030[19].

To varying degrees' companies are now doing something about it

According to the US drought monitor over half of the US is in a drought condition, covering 60% of the mainland 48 US states, this is up 9% in just one month[20]. So what are companies doing?[21]

- Microsoft publishes an annual sustainability report, including its water consumption. Which has grown from 67.5m cubic feet in 2017 to 158m cubic feet in 2021. As well as their pledge to be "water positive" by 2030 they have committed to reducing data centre waste water by 95% by 2024.
- Google has also committed to replenish 120% of its water consumption by 2030[22]. However, it does not publish its water consumption numbers but it does have internal measures.
- Amazon does not publish its water consumption numbers (though it does monitor usage internally) and has not set out a clear timeline of its planned water reduction. However, it has announced plans to reduce its consumption[23], particularly of potable water[24] i.e. drinkable water.

Related key reports

- Please contact your HSBC representative for details on related reports.

[13] Microsoft, Amazon and Google Account for Over Half of Today's 600 Hyperscale Data Centers, Synergy Research Group, 26 January 2021
[14] Drought-stricken communities push back against data centers, NBC News, 18 June 2021
[15] Data centers, backbone of the digital economy, face water scarcity and climate risk, NPR, 30 August 2022
[16] ESG Risks Affecting Data Centers: Why Water Resource Use Matters to Investors, Sustainalytics, 19 August 2022
[17] Fears over data centres soaking up water during UK drought, The Times, 23 August 2022
[18] Microsoft, Meta and others face rising drought risk to their data centers, CNBC, 15 November 2022
[19] Microsoft will replenish more water than it consumes by 2030, Microsoft, 21 September 2020
[20] Microsoft, Meta and others face rising drought risk to their data centers, CNBC, 15 November 2022
[21] The West's drought could bring about a data center reckoning, protocol, 2 July 2022
[22] Google Water Stewardship Accelerating positive change at Google, and beyond, Google, September 2021
[23] Water Stewardship in Data Centers, Amazon Sustainability
[24] Reducing water usage in AWS data centers, Amazon, 11 August 2020

Is technology to accelerate AR glasses nearly ready?

AR headsets currently lag behind VR headsets in maturity

Another technical hurdle overcome in the race to AR glasses

In our report, *The Metaverse Age*, we highlighted that AR glasses and headsets exist but are less advanced than VR headsets, particularly due to the complexity of the optics technology and smaller form factor required for AR.

But steps to reduce the gap are being taken

In November 2022, a major chipmaker launched its first dedicated AR chipset. The chip's processor is designed specifically for AR glasses so that it is thin and lightweight. The chip is made up of three parts and the company's reference design shows each as follows[25]:

- AR processor in right earpiece for perception and display output
- AR co-processor in the nose bridge for sensor aggregation, AI, and computer vision
- Connectivity chip (which can interact with smartphones chips to boost power) in left earpiece for low latency, low power, and Wi-Fi 7

Compared with the previous generation processor, this new chipset has a 40% smaller printed circuit board, 45% less wiring, reduced processor power and Wi-Fi power consumption by 50% and 40%, respectively[26]. And the overall platform delivers 2.5x AI performance[27].

Offloading processing requirements to compatible host devices

Processing away from headset?

The AR processor and co-processor work with smartphones, PCs, and networks to provide a distributed computing architecture. Which mixes locally produced data on smart glasses with the clouds (or other devices) computing power to expand its computing power and lower the heat generated in the glasses. The connectivity chip enables Wi-Fi 7 to provide high speed broadband connectivity between the glasses and the host device[28], which will enable AR glasses to be latency free[29].

Related key reports

- Please contact your HSBC representative for details on related reports.

[25] AR glasses will have a dedicated Qualcomm chip in 2023, Digital Trends, 16 November 2022
[26] Qualcomm Brings Augmented Reality Closer To Reality With A New Chipset And Development Environment, Forbes, 17 November 2022
[27] Qualcomm Launches Snapdragon AR2 Designed to Revolutionize AR Glasses, Qualcomm, 16 November 2022
[28] Qualcomm Brings Augmented Reality Closer To Reality With A New Chipset And Development Environment, Forbes, 17 November 2022
[29] Snapdragon AR2 Chip Set To Accelerate AR Glasses, Forbes, 16 November 2022

Disclosure appendix

The following analyst(s), who is(are) primarily responsible for this document, certifies(y) that the opinion(s), views or forecasts expressed herein 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: Henry Ward, Davey Jose, Faizan Lakhani, Nicolas Cote-Colisson and Frank Lee

This document has been issued by the Research Department of HSBC.

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.

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*.

Additional disclosures

1 This report is dated as at 20 December 2022.

2 All market data included in this report are dated as at close 19 December 2022, 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

Issuer of report
HSBC Bank plc

This document has been issued by HSBC Bank plc, which has based this document on information obtained from sources it believes to be reliable but which it has not independently verified. Neither HSBC Bank plc nor any member of its group companies ("HSBC") make any guarantee, representation or warranty nor accept any responsibility or liability as to the accuracy or completeness of this document and is not responsible for errors of transmission of factual or analytical data, nor is HSBC liable for damages arising out of any person's reliance on this information. The information and opinions contained within the report are based upon publicly available information at the time of publication, represent the present judgment of HSBC and are subject to change without notice.

This document is not and should not be construed as an offer to sell or solicitation of an offer to purchase or subscribe for any investment or other investment products mentioned in it and/or to participate in any trading strategy. It does not constitute a prospectus or other offering document. Information in this document is general and should not be construed as personal advice, given it has been prepared without taking account of the objectives, financial situation or needs of any particular investor. Accordingly, investors should, before acting on it, consider the appropriateness of the information, having regard to their objectives, financial situation and needs. If necessary, seek professional investment and tax advice.

The decision and responsibility on whether or not to purchase, subscribe or sell (as applicable) must be taken by the investor. In no event will any member of the HSBC group be liable to the recipient for any direct or indirect or any other damages of any kind arising from or in connection with reliance on any information and materials herein.

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. Some of the statements contained in this document may be considered forward looking statements which provide current expectations or forecasts of future events. Such forward looking statements are not guarantees of future performance or events and involve risks and uncertainties. Actual results may differ materially from those described in such forward-looking statements as a result of various factors.

This document is for information purposes only and may not be redistributed or passed on, directly or indirectly, to any other person, in whole or in part, for any purpose. The distribution of this document in other jurisdictions may be restricted by law, and persons into whose possession this document comes should inform themselves about, and observe, any such restrictions. By accepting this report, you agree to be bound by the foregoing instructions. If this report 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. The document is intended to be distributed in its entirety. Unless governing law permits otherwise, you must contact a HSBC Group member in your home jurisdiction if you wish to use HSBC Group services in effecting a transaction in any investment mentioned in this document.

Certain investment products mentioned in this document may not be eligible for sale in some states or countries, and they may not be suitable for all types of investors. Investors should consult with their HSBC representative regarding the suitability of the investment products mentioned in this document.

HSBC and/or its officers, directors and employees may have positions in any securities in companies mentioned in this document. HSBC may act as market maker or may have assumed an underwriting commitment in the securities of companies discussed in this document (or in related investments), may sell or buy securities and may also perform or seek to perform investment banking or underwriting services for or relating to those companies and may also be represented on the supervisory board or any other committee of those companies.

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.

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)

[1205789]