HSBC Global Research

Free to View
Equities

United Kingdom | Thematic research

March 2023

www.research.hsbc.com

By: Rahul Chopra and Dylan B Whitfield

SPOTLIGHT

Decrypting Cybersecurity

Beyond the Endpoint

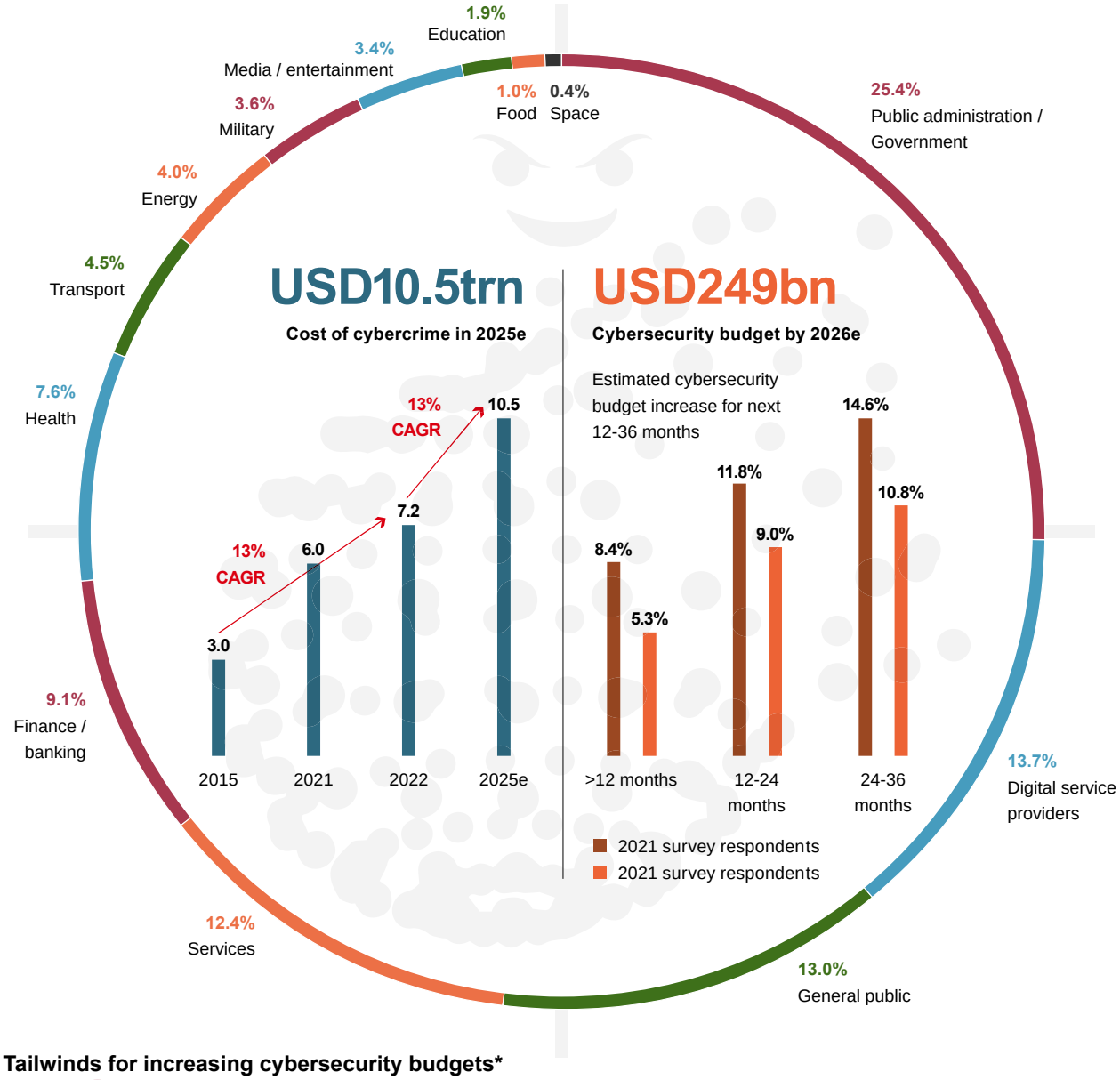
With cyberattacks growing in number and sophistication, spending on cybersecurity is only expected to grow

In this report, we look at the different cybersecurity issues and key trends, the cost of cyberattacks and the evolving threat landscape

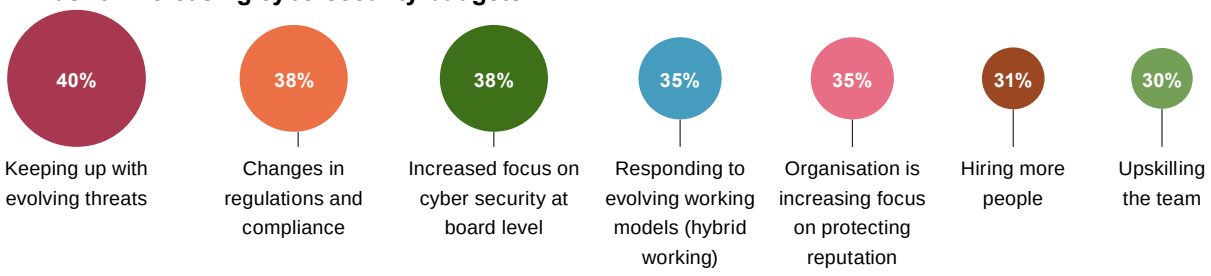
This is a redacted Free to View version of a report with the same title published on 22 March 2023. Please contact your HSBC representative or email AskResearch@hsbc.com for more information.

Cost of cybercrime and cybersecurity spend

Targeted sectors based on number of incidents (Jul-21 to Jun-22)



Tailwinds for increasing cybersecurity budgets*



91%

Of cyber leaders believe that geopolitical instability will lead to a catastrophic cyber event in the next two years

323 days

Average time to identity a data breach, but reduces to 74 days when AI and automation are fully deployed

Source: European Union Agency for Cybersecurity (ENISA), Cybersecurity Ventures *S-RM Cyber Security Insights Report 2022, based on a survey of 600 C-suite and IT budget holders from organisations with a revenue >USD500m

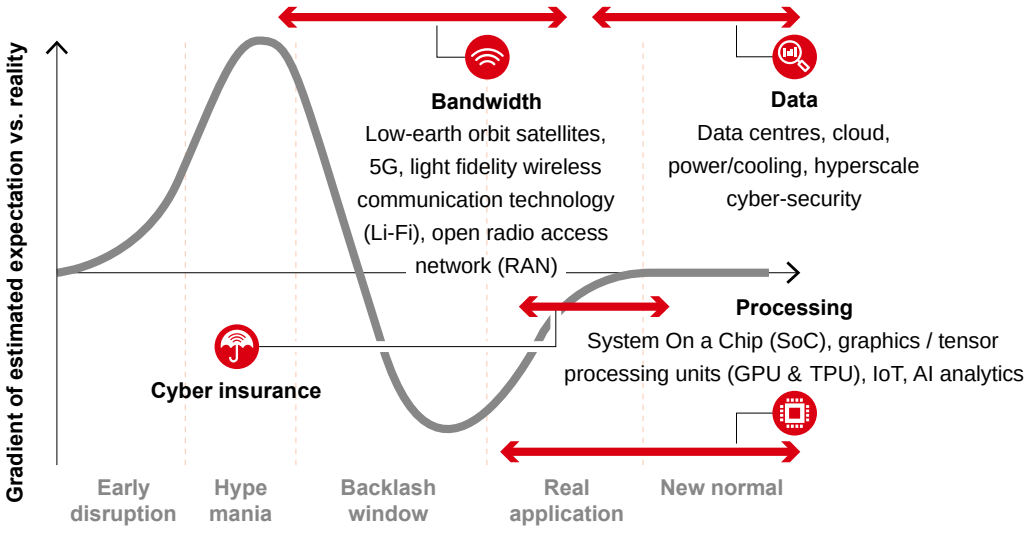
State of cybersecurity today

- Globally, cyberattacks increased 38% YoY in 2022
- Spending on cybersecurity has lagged the cost and frequency of attacks
- The cybersecurity market is a double-digit market which is set to reach USD249bn by 2026, at a 11% CAGR

HSBC Disruptive Framework and cybersecurity

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 COVID-19 pandemic has accelerated their adoption within 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 whether it is ready to become the new normal, disrupt business models and have economic implications.

HSBC Disruption Framework: Connectivity infrastructure



Source: HSBC

With the rise of data-centric businesses and the digital state, all connected, the value of data increases. 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 a 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 are in the “new normal” part of our framework, as cybersecurity is an essential part of

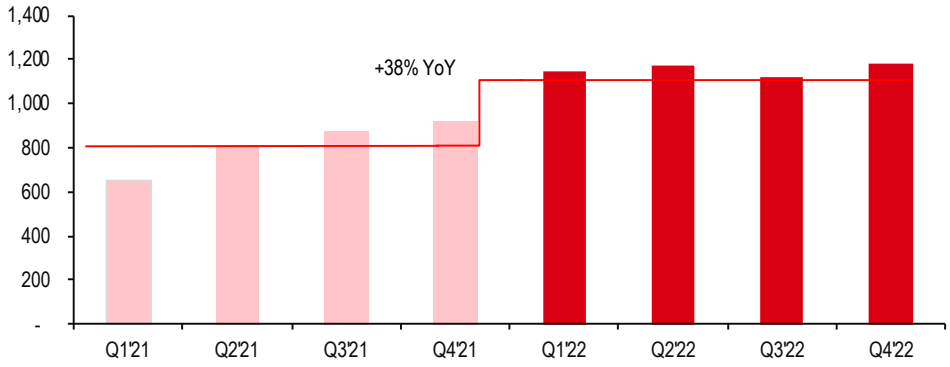
businesses with connectivity. For consumer-focused organisations, this means a higher risk of data breaches and loss if the right protocols and technologies are not in place. As a result, we expect to see product and platform security come to the forefront next year, particularly as organisations realise the value 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.

Cyberattacks increased 38% in 2022

Global cyberattacks increased by 38% in 2022

Global cyberattacks increased by 38% in 2022 versus 2021, with average weekly attacks at 1,168 in Q4'22. This was driven by attackers exploiting collaboration tools in WFH environments and targeting education institutions that shifted to e-learning post COVID-19, as well as increased attacks on healthcare organisations, which saw the largest increase in cyberattacks in 2022. According to Check Point Research, with the maturity of AI technology, the number of cyberattacks could accelerate further in 2023.

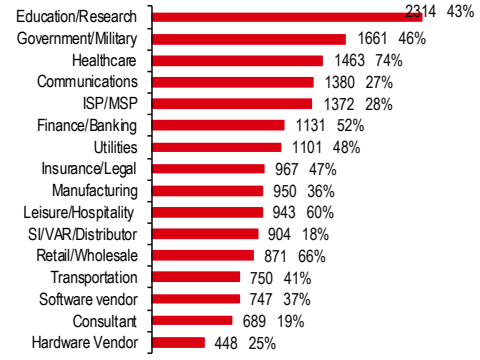
Average weekly attacks per organisation grew 38% in 2022 versus 2021



Source: Check Point

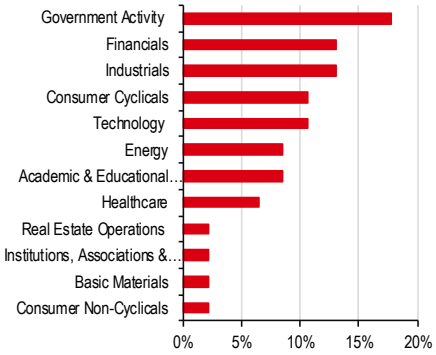
- According to Check Point, in terms of sectors, the top-three most attacked industries in 2022 were Education/Research (13% of total attacks), Government/Military (9%) and Healthcare (8%). Healthcare sectors saw the largest increase with a 74% YoY increase to 1,661 weekly cyberattacks per organisation.
- Whilst the statistics from NCC Group are based on its own clients and so are not reflective of global distribution of attacks, NCC Group has echoed a similar experience, with 'Government Activity' the most targeted sector (18% of total attacks) followed by Financials and Industrials at 13% each and Technology and Consumer Cyclicals at 11% each.
- According to the European Union Agency for Cybersecurity (ENISA), Government / Public administration had the largest number of incidents followed by Digital Service providers, General Public and Services companies (trailing 12m June 2022 data).

Average weekly attacks per organisation: All sectors suffered YoY double-digit attacks in 2022



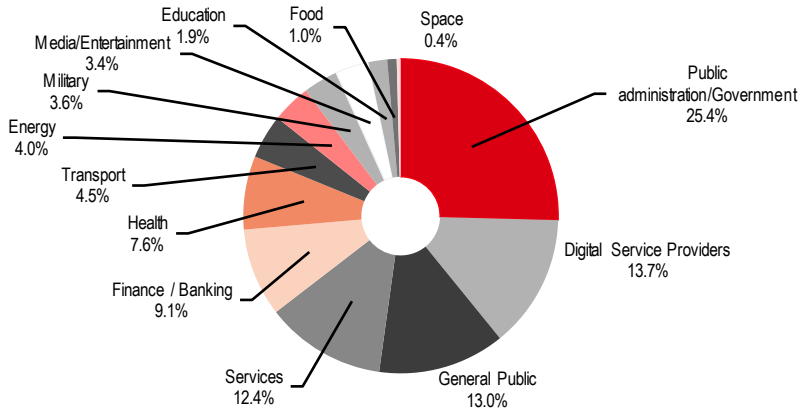
Source: Check Point

Most targeted sectors in 2022



Source: NCC Group Annual Threat Monitor 2022

Targeted sectors based on number of incidents (July 2021-June 2022)



Source: European Union Agency for Cybersecurity (ENISA)

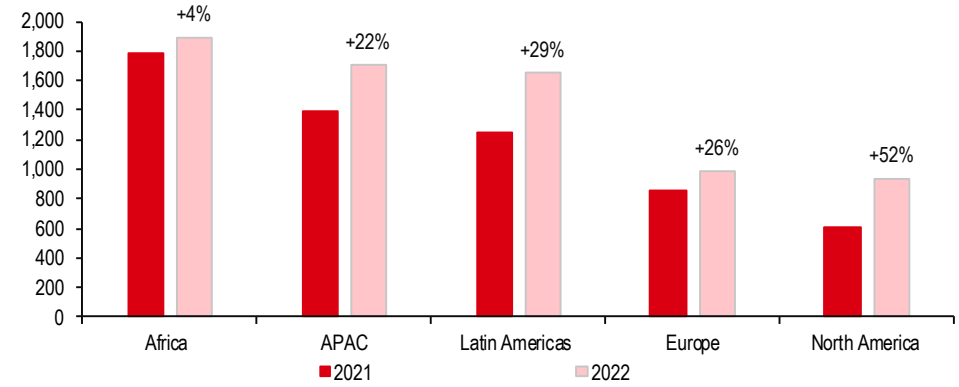
Africa experienced the highest volume of attacks

- In terms of geographies, Africa experienced the highest volume of attacks with 1,875 weekly attacks per organisation, followed by APAC with 1,691. North America (+52%) and Latin America (+29%) saw the largest YoY increase cyberattacks in 2022.
- Whilst Africa witnessed the largest number of attacks, cost per data breach in the US, at USD9.4m, is nearly 2.2x higher than the global average, making these attacks more impactful, and providing a greater incentive for cybercriminals.

43%

of organisation leaders think it's likely a cyberattack will materially affect their organisation – World Economic Forum

Average weekly attacks per organisation by regions

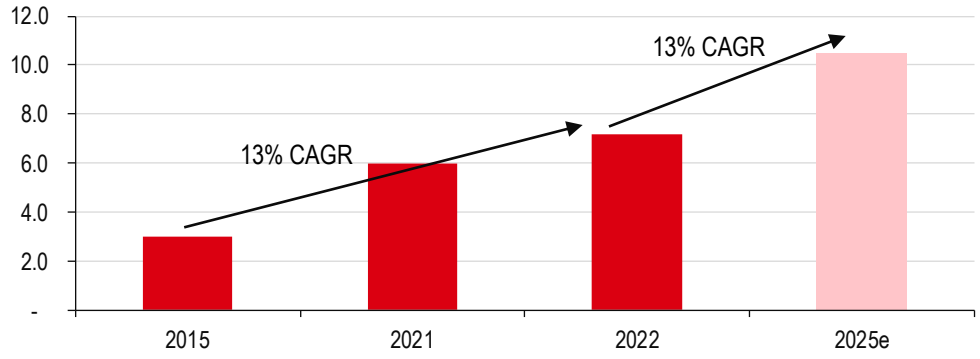


Source: Check Point

US had the highest cost per attack

In 2021, the cost of cybercrime estimated by Cybersecurity Ventures is about USD6.0trn. Putting this into perspective – if it were an economy, it would be the third largest in the world trailing only the US and China. The cost of cybercrime is expected to grow at a 13% CAGR, to reach USD10.5trn by 2025e.

Cost of cybercrime (USD trillion)



Source: Cybersecurity Ventures

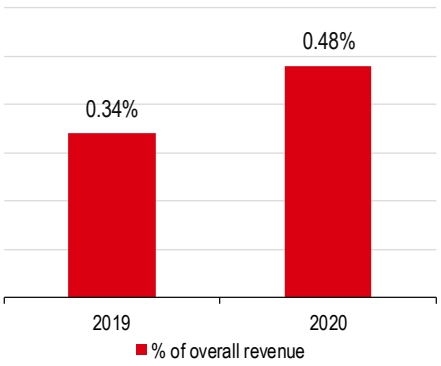
Spending on cybersecurity

IT spend is anywhere between 0.5% and 10% of revenues and cyber budgets 10-20% of IT spend

It is difficult to estimate the right amount that organisations need to spend on cybersecurity but as a good rule of thumb, business spend anywhere between 0.5% and 10% of revenues on IT. Within that share of pie, cybersecurity should be anywhere between 10% and 20% of total IT budgets. If one were to think in terms of cybersecurity budget per employee, this could range anywhere between USD1,000 and USD5,000 as a good proxy. In the end, cybersecurity costs depend upon size of organisation, level of digitalisation, complexity of supply chain, level of security desired, type of data being dealt and regulatory factors.

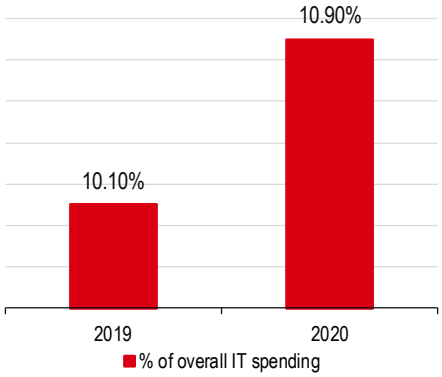
According to Deloitte, among the financial institutions, in 2020 the spend on cybersecurity as a percentage of revenue was 0.48%, with companies spending USD2,700 on average per full-time employee on cybersecurity (10.9% of IT budgets allocated to cybersecurity).

Cybersecurity spend as a percentage of revenues (Financial Institutions)



Source: FC-ISAC/Deloitte Cyber & Strategy Risks Service CISO survey responses, 2019 and 2020, Deloitte Centre for Financial Services analysis

Cybersecurity spend as a percentage of total IT budget (Financial Institutions)



Source: FC-ISAC/Deloitte Cyber & Strategy Risks Service CISO survey responses, 2019 and 2020, Deloitte Centre for Financial Services analysis

According to the HISCOX Cyber Readiness Report, the total proportion of IT budget for cybersecurity spending has increased across all major geographies, with US firms allocating 24% of their IT budgets to cybersecurity in 2022 and UK firms allocating 22%.

Cutting cybersecurity budgets creates a compliance debt…

Proportion of IT budget for cybersecurity (%)

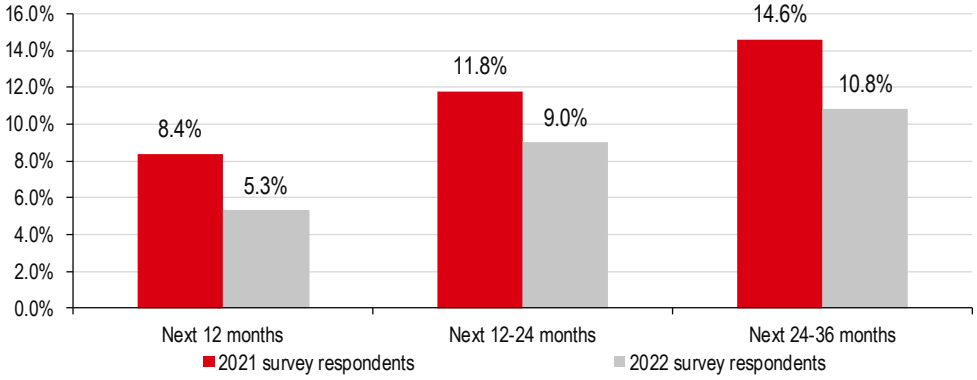
Region	2021	2022
Belgium	21%	24%
France	20%	22%
Germany	21%	24%
Ireland	21%	22%
The Netherlands	22%	24%
Spain	22%	24%
United Kingdom	20%	22%
United States	23%	24%

Source: HISCOX Cyber Readiness Report 2022 based on a survey of 5,181 professionals responsible for cybersecurity strategy from the USA, UK, France, Germany, Belgium, Spain, The Netherlands, the Republic of Ireland

…either in the form of pent-up spend for future periods or exposing them to attacks

According to a survey by S-RM, in 2021, respondents expect 14.6% increase in budget spending over the next 24-36 months. However, this figure dropped to 10.8% for 2022 due to a tougher macro environment and squeezed budgets due to cost pressure. Whilst actual budget spend for 2022 is not yet out, if there was in fact a drop, it is unsurprising that cyberattacks increased 38% YoY in 2022. In the end, companies may regret cutting cybersecurity budgets given that it creates a compliance debt which has to be paid for at a later date, or, worse, makes them more vulnerable to cyberattacks.

Estimated cybersecurity budget increase for next 12-36 months



Source: S-RM Cybersecurity Insights Report 2022, based on a survey of 600 C-suite and IT budget holders from organisations with a revenue >USD500m

Evolving threat landscape, regulation and increased board focus are main drivers of higher cyber budgets

- In SR-M's survey, '*keeping up pace with evolving threat landscape*' was the most commonly cited driver of budget increases, alongside '*changes in regulation and compliance*' as the second most important driver. '*Increased cybersecurity focus at the board level*' and '*hybrid working conditions*' were cited as other important reasons.

Drivers behind increase in cyber budget

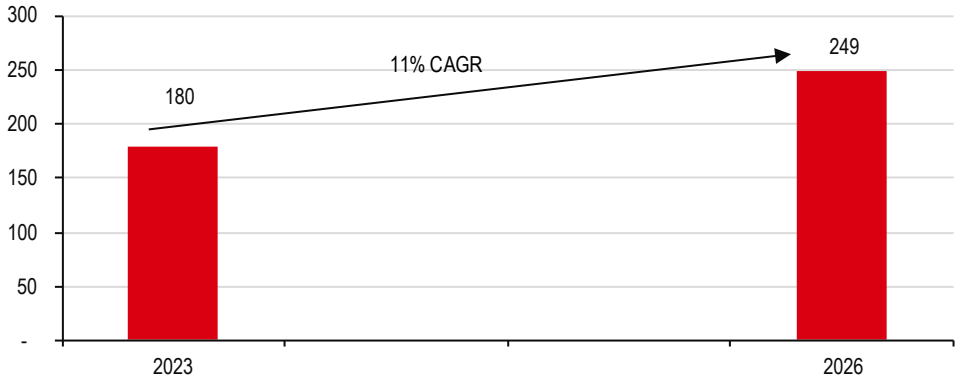
Source: S-RM Cybersecurity Insights Report 2022, based on a survey of 600 C-suite and IT budget holders from organisations with a revenue >USD500m

Cybersecurity spending is expected to grow at double-digit CAGR

Cybersecurity spend is expected to grow at double-digit CAGR

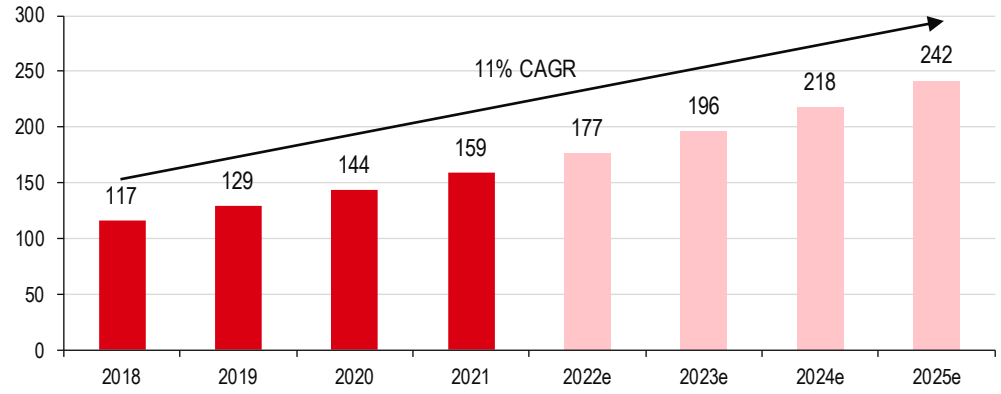
Cybersecurity spend is expected to grow at a double-digit CAGR (11%), reaching USD249bn by 2026e (Fortinet). Spending on Cybersecurity is not seen as an investment, but as a required spend. Increased regulation is resulting in boards and business leaders being far more aware of the risks, and this is flowing through to increased demand for cybersecurity solutions at record speeds. Given the expected increase in digital transformation, this level of cybersecurity is probably insufficient. Cybersecurity spending, even at 10% of the global cybercrime cost of USD10.5trn suggests a total market opportunity of USD1.5trn. We would not expect the market to reach this anytime soon, but it shows the huge potential opportunity for the cybersecurity market. Evolving cyberattacks, increased cost, the frequency and sophistication of attacks, rising geopolitical risks, tailwinds from regulation and increased levels of involvement from board members – these are all clear structural tailwinds for cybersecurity spending. We are still at the foothills of what the future cyber landscape could look like.

Total Addressable Market set to reach USD249bn at 11% CAGR (USDbn)



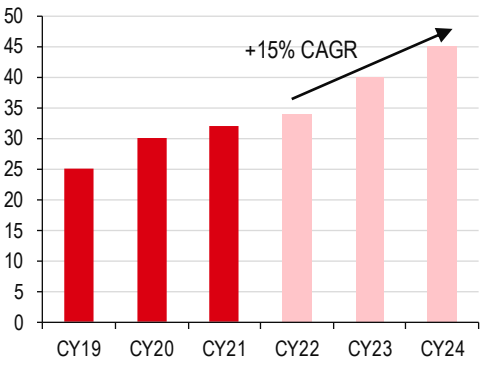
Source: Fortinet. Total Addressable Market includes Enterprise Networking (Network Firewall, SD-WAN, WLAN-LAN, SASE/SSE/ZTNA), Cybersecurity (Endpoint Security, Identity and Access, SIEM.SOC, email, WAF) and OT Security

Cybersecurity total addressable market (USDbn)



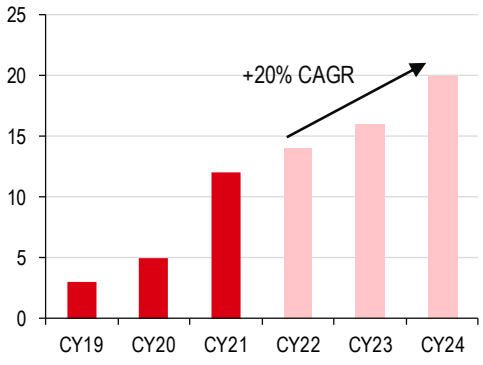
Source: NCC 2021 annual report

Network Security spending (USDbn)



Source: Palo Alto Networks Investor day presentation, September 2021

Cloud Security spending (USDbn)



Source: Palo Alto Networks Investor day presentation, September 2021

The full report also discusses various other aspects of Cybersecurity – from the key themes of Cybersecurity, to the role AI will play in the future of Cybersecurity to what the threat landscape looks like and much more. Also included are ways investors can play this theme. Below we summarise the key themes, the AI angle, and the threat landscape.

Key themes of Cybersecurity

Cybersecurity is moving from a reactive to a predictive approach. We are seeing SMEs increasingly turning towards managed security service providers and an increase in vendor consolidation for larger organisations. A push from regulation, geo-political tensions and a more proactive involvement of corporate boards mean cyber risks are being taken more seriously than ever before.

Key themes for cybersecurity landscape

Theme	Implications
Transition towards cloud, complex supply chains and flexible working	Blurring of digital borders with larger digital perimeter, with lack of visibility for Chief Information Security Officer (CISO). A shift away from traditional endpoint network security approach.
Cybersecurity approach moving from a reactive to predictive approach	Incorporating behavioural aspects for threat detection including use of AI / Machine learning. Traditional Security Information and Event Management (SIEM) platforms are less relevant. Shift away from Security Operations Centre (SOC) analysis to Endpoint Detection & Response (EDR), Managed Detection & Response (MDR) and Extended Detection & Response (XDR)
Growth in Managed Security Service Providers (MSSP)	Shift away from in-house security operations centre (SOC) towards cost-effective outsourced management of security services
The rise of Wipers	Profound effect of cyber being woven into cyberwarfare.
Geopolitical instability reshaping cybersecurity strategies	Heightened threat landscape a catalyst for structural growth driver for cybersecurity spending; increased public-private partnership and organisations taking cyber risks more seriously than ever
Step-up in spending required for SMEs	A catch-up of historical underspend on cybersecurity by SME would require increased spending on cybersecurity
Regulatory Push	Enhanced regulation a catalyst for cybersecurity disclosures and spending.
Industrialisation of cybercriminal ecosystem	Franchising of the cybercrime economy has lowered the 'skill level' required to perform intrusions. Data increasingly used as a 'double extortion' strategy. Increase in 'Cyber Incident Response'.
Shortage of cybersecurity professionals	Wage inflation and scarcity driving increased automation and use of AI
Increasing vendor consolidation	Better efficiencies by integrating multiple components, especially for larger organisations. Given the growth in Managed Security Service Providers which relies on multiple vendors, cyber landscape will continue to have room for multiple vendors, large and small but expect increased consolidation in the sector.
ESG implications	Increased involvement from the board, both driven by regulation and increased awareness of cyber risks being acknowledged higher up

Source: HSBC

There is also a regulatory push for cybersecurity disclosures and discussions higher up. For example, on 9 March 2022, The Securities and Exchange Commission (SEC) amended its rules to enhance disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

SEC proposed rules around disclosures of cybersecurity

The Securities and Exchange Commission proposed rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies ("registrants") that are subject to the reporting requirements of the Securities Exchange Act of 1934.

Specifically, the proposal would:

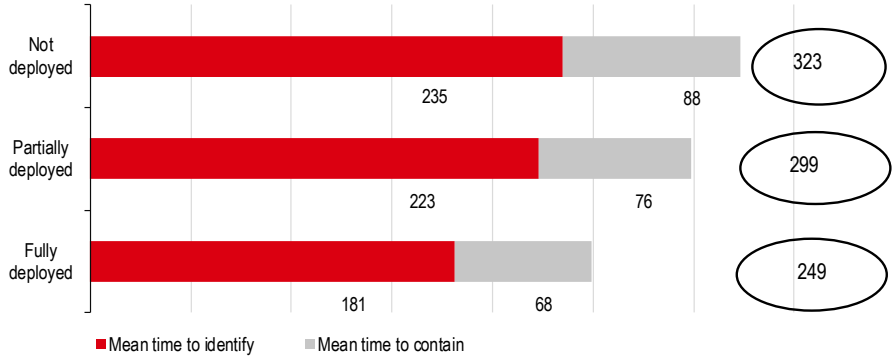
- Require current reporting about material cybersecurity incidents on Form 8-K;
- Require periodic disclosures regarding, among other things:
  - A registrant's policies and procedures to identify and manage cybersecurity risks;
  - Management's role in implementing cybersecurity policies and procedures;
  - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
  - Updates about previously reported material cybersecurity incidents; and
- Require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

Source: US Securities and Exchange Commission

Role of Artificial Intelligence

The core of a Cyber AI platform relies on behavioural datasets and machine learning and is a sharp contrast to traditional security service providers that rely on rules-based technology. AI application identifies and analyses all the relevant contextual data in the client's entire digital ecosystem, not just data historically associated with information security, which increases the likelihood of identifying unusual activity that could indicate the presence of a threat. According to IBM, the use of security AI and automation increased from 59% in 2020 to 70% in 2022.

Average time (in days) to identify and contain a data breach by level of security AI and automation



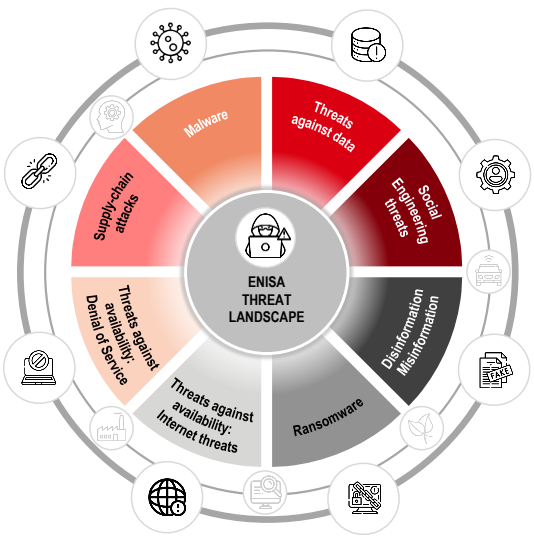
Source: IBM Security, Cost of a Data Breach Report 2022. Based on a study involving 550 organisations that suffered a data breach between March 2021 to March 2022.

The cyber threat landscape

Attacks are becoming more sophisticated and complex. In the past, a hacker would target a single vector such as a firewall port, but they are now increasingly targeting multiple vectors. For example, from a remote location, a hacker could log into the organisation network and then access the Active Directory system, changing a user's privileges in order to start downloading data from a server. In a traditional security system, these aggregate indicators might be viewed as false positives in isolation but in reality they are all part of a single attack.

Whilst there are different ways to group cyber-attacks, The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2022 focuses on eight main threats: 1) Ransomware; 2) Malware; 3) Social Engineering threats; 4) Threats against data; 5) Denial of Service; 6) Internet threats; 7) Disinformation – misinformation; and 8) Supply-chain attacks.

Threat Landscape



Source: European Union Agency for Cybersecurity, Threat Landscape 2022

Glossary of terms

Summary glossary of terms

Abbreviation	Full Term
AI	Automated Intelligence
SMB's	Small and Medium Businesses
DOS	Denial of Service
DT	Darktrace
EV	Enterprise Value
WFH	Work From Home
ENISA	European Union Agency for Cybersecurity
SME's	Small and Medium Enterprises
SIEMs	Security Information and Event Management platforms
NDR	Network detection and response
EDR	Endpoint detection and response
SOC	Security operations centre
UEBA	User and entity behaviour analytics
MDR	Managed Detection and Response
XDR	Extended Detection and Response
MSSP	Managed Security Service Provider
DDoS	Distributed Denial of Service
CISA	Cybersecurity & Infrastructure Security Agency
NSSC	National Cyber Security Centre
IOT	Internet of Things
EO	Executive Order
RaaS	Ransomware as a Service
CISO	Chief Information Security Officer
WEF	World Economic Forum
MSSP	Managed Service Security Providers
EO	Executive Order
BYOD	Bring your own device
VPN	Virtual Private Network
DLP	Data Loss Prevention
IPS	Intrusion Prevention Systems
2FA	Two-factor authentication
RDP	Remote Desktop Protocol
RCE	Remote Code Execution
BEC	Business Email Compromised
RPO	Remaining Performance Obligations
ASM	Attack Surface Management
POV	Proof of Value
ML	Machine Learning
ARR	Average Recurring Revenue
EaaS	Escrow as a Service
GPS	Global Professional Services
IPR	Intellectual property Rights
SaaS	Software as a Service
TOM	Target Operating Model

Source: HSBC

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: Rahul Chopra, CFA, Dylan Whitfield, FCA, Matthew Lloyd, Mark McDonald and Davey Jose

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 22 March 2023.

2 All market data included in this report are dated as at close 20 March 2023, 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)

[1210497]