



WAVESTONE

How mature are annual reports of the FTSE 100 regarding cybersecurity?

July 2020



Florian POUCHET

Partner

florian.pouchet@wavestone.com

+44 7493 86 77 66



Olivia SPRINGATE

Consultant

olivia.springate@wavestone.com

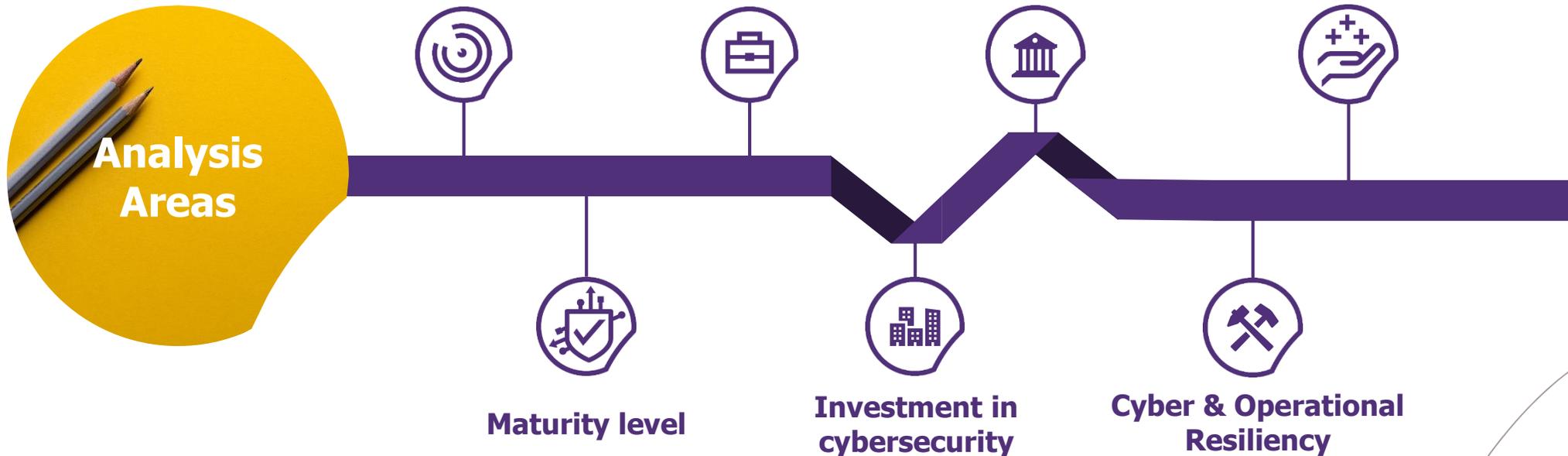
+44 7392 870 925

How mature is the FTSE 100 in cybersecurity?

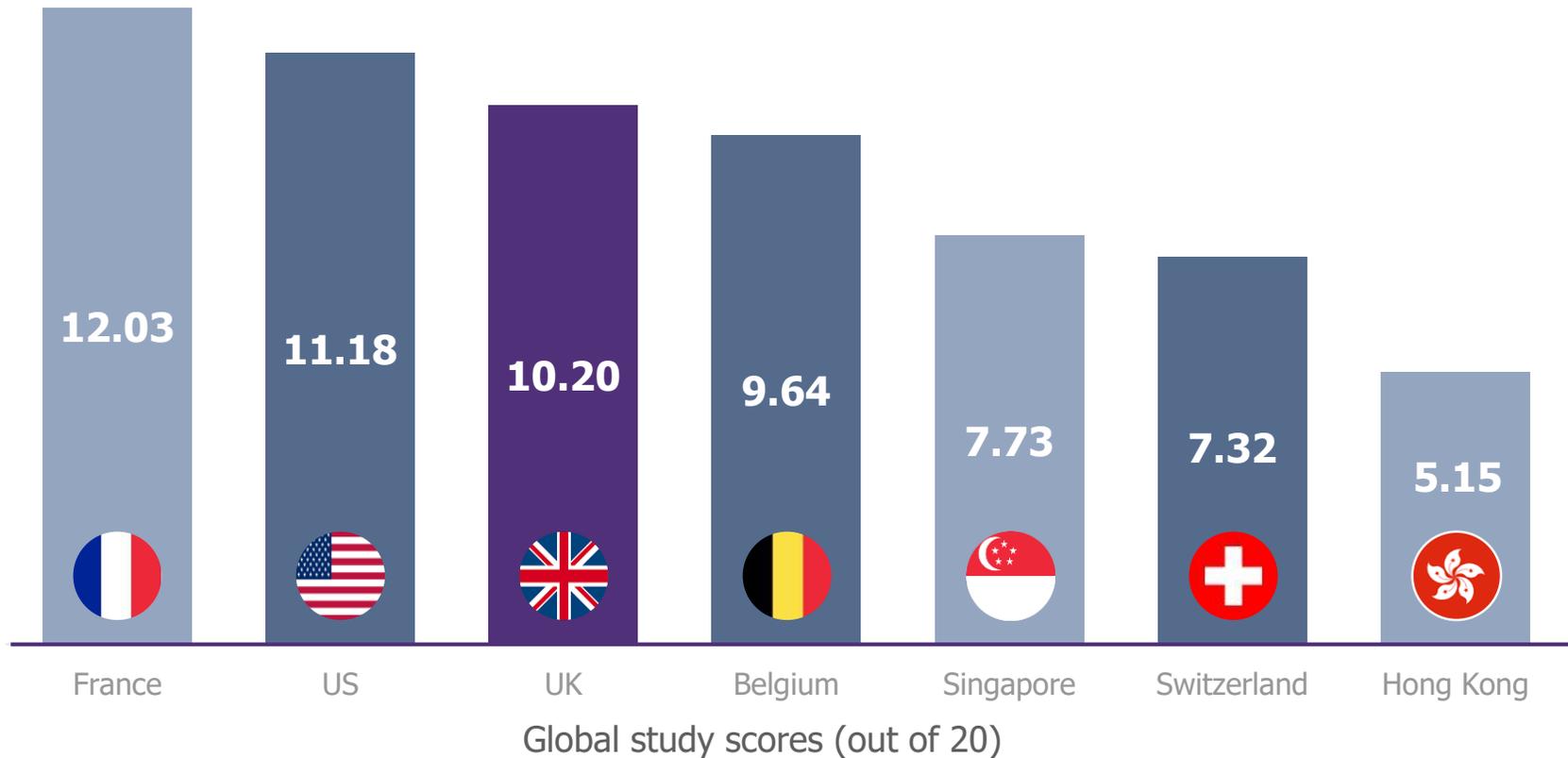


Method: this study is based upon empirical analysis of the most recent annual reports, published by the FTSE 100 companies up to 01/06/2020. It is one of six studies conducted across multiple Wavestone offices globally in Q2 of 2020.

The results of this study are only as accurate as the statements and disclosures made by each company in their annual reports. As a result it is possible that, in reality, any given company's cybersecurity maturity is better or worse than has been reported.



UK FTSE 100 scores third place in global study



The UK has scored third place for the second year in a row, with the FTSE 100 once again scoring just a couple of points behind the French CAC 40 and the US Dow Jones.

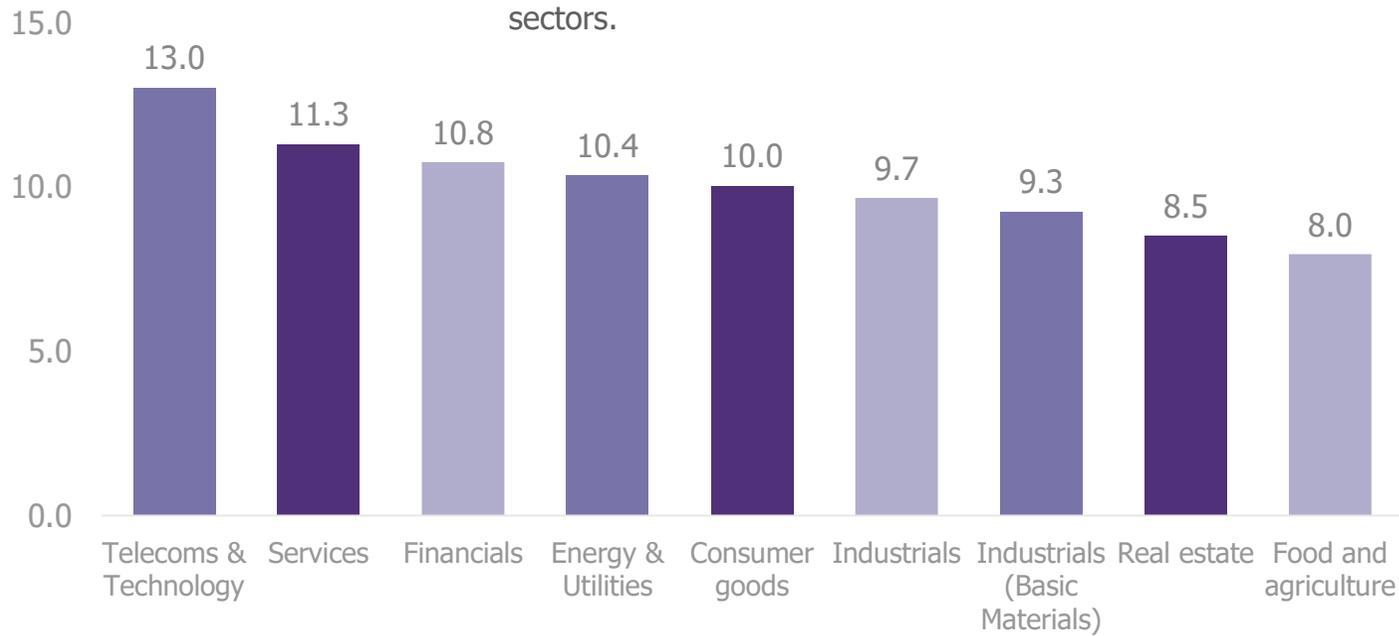
The Telecoms sector is a stand out performer for the second year; Basic Materials makes huge improvement



This year we saw an overall increase of more than one whole point (9.09/20 in 2019), revealing that the FTSE 100 companies are growing in cyber maturity as a whole.

We had score increases across the board, in every sector other than the stand out performer; Telecoms & Technology. Basic Materials jumped by three points this year due to heavy investment in cybersecurity programmes.

Both Real estate and Food and agriculture now falter behind the pack due to an increase in awareness seen in other sectors.



Wavestone's Top Companies Cybersecurity Index: 2020 Annual Reports

Wavestone's Top Companies Cybersecurity Index provides an assessment of companies' maturity levels, based upon the content of their annual reports. This index, scored out of 20, is based on 14 criteria weighted and marked between 0 and 2. These criteria² cover the following topics:

Issues and risks
Infosec issues, cyber risks and impacts, cyber insurance coverage, digital transformation and new technology security.

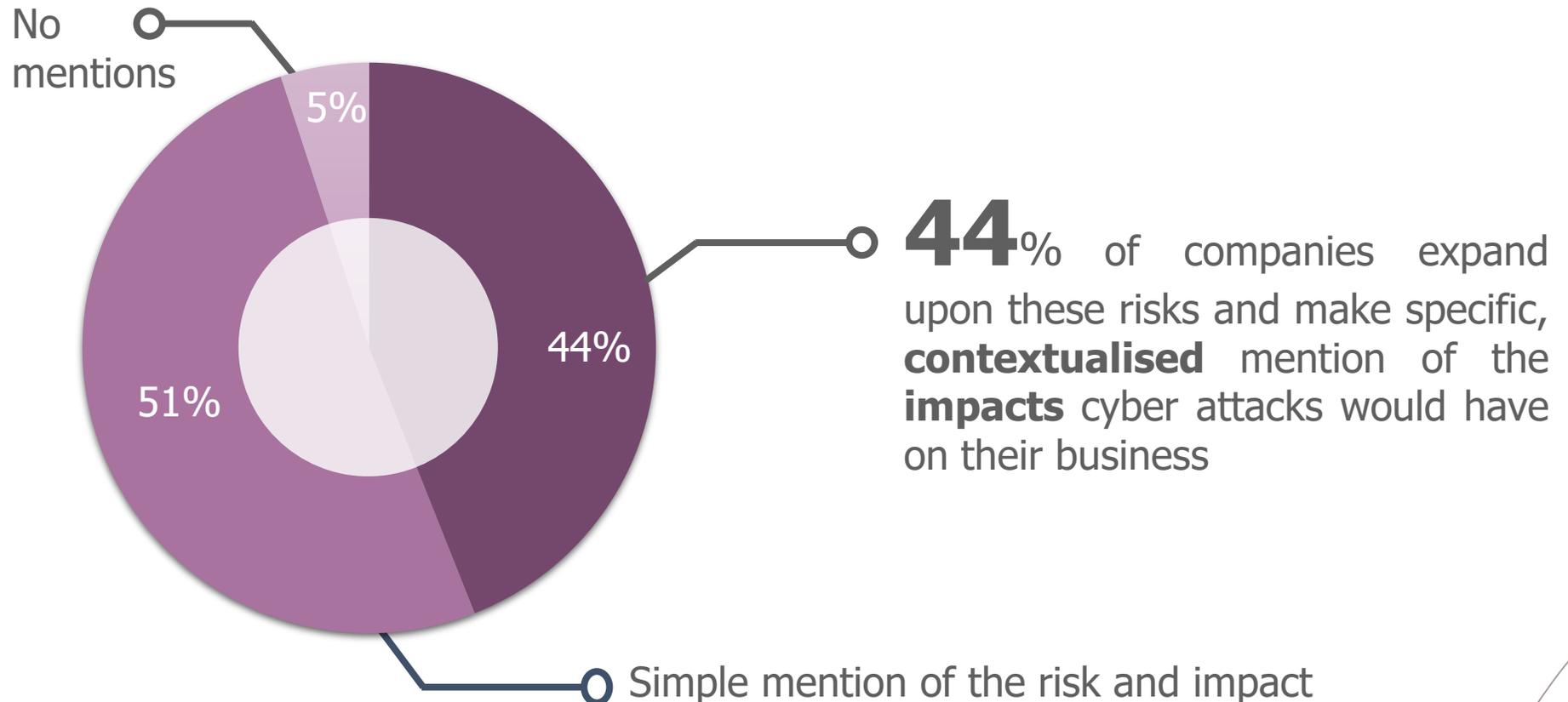
Governance and regulation
Executive Committee involvement, ISS governance, personal data protection, awareness and training, transparency with security incidents, regulations and conformity to standards.

Protection and Controls
Action plan implementation, cybersecurity programme, securing business systems, audits and controls.

*Mean average across all companies in all sectors
¹Sectors are defined in the Appendix ²Criteria are defined in the Appendix

Cybersecurity Risk and Big Impacts

95% of FTSE 100 companies acknowledge the impact a cyber attack or incident could cause.



Executive Committee is getting more updated

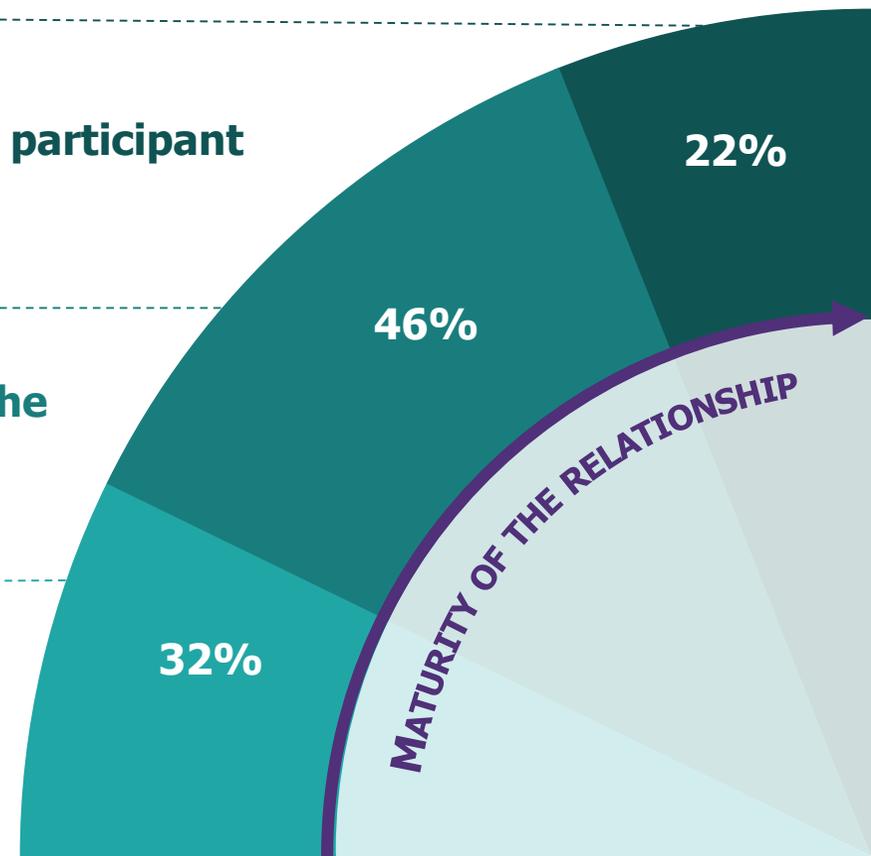
In 2020, Executive Committees are showing more of an interest in cybersecurity than ever before. With **68%** of FTSE 100 companies showing some form of Executive Committee interest, cybersecurity is still an ever increasing focal point in board meetings.

A small reduction in active participation also suggests that some Executive Committees are handing over the cybersecurity reins to different areas of the business, preferring to receive regular updates instead.

A member of the Executive Committee is an active participant in cybersecurity.

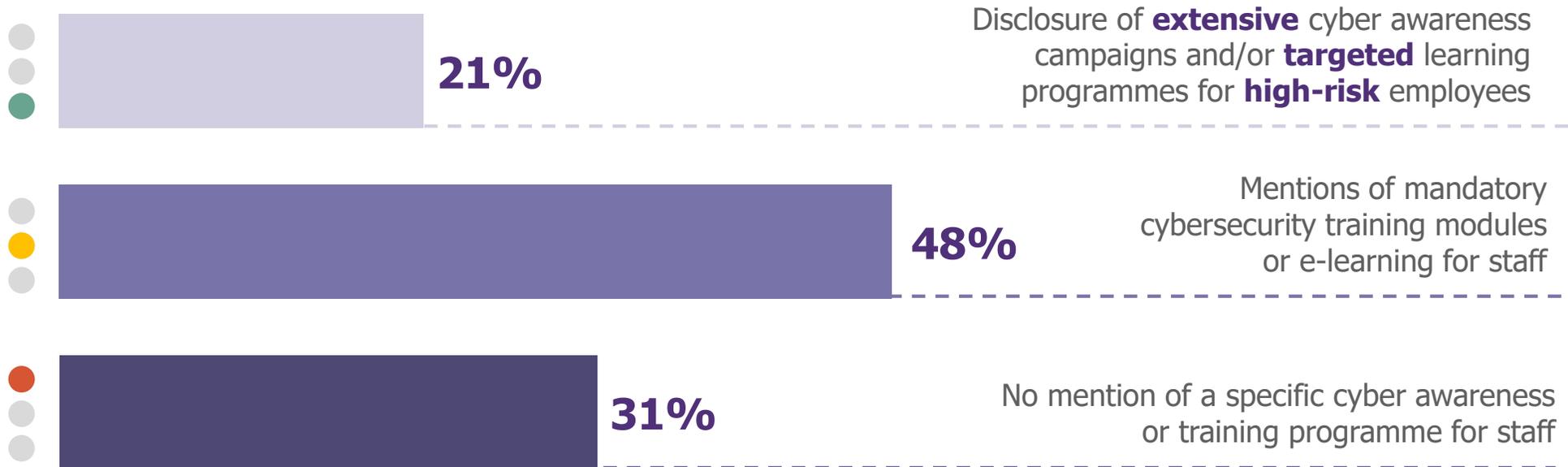
A governance body addresses cybersecurity with the Executive Committee on a regular basis.

Boards or Executive Committees are not engaged in cybersecurity



A big push for employee awareness

69% of companies in the FTSE 100 are taking steps to educate and inform their employees.



There was an extensive increase (9%) in mandatory cybersecurity training this year, demonstrating that more companies now understand the importance of having an alert workforce.

We saw surprisingly low scores in this criteria from some companies and suspect they may be training more than is mentioned in their annual report, considering regulations that make it mandatory for some of the sectors.

This year phishing awareness was a stand out topic, with multiple FTSE 100 companies simulating phishing attacks on their employees.

An increase in investment shows the ever expanding importance of cybersecurity

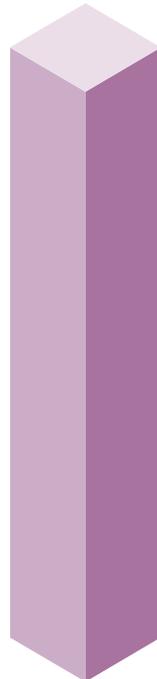
51%

Cybersecurity programmes

Security programmes involving significant investments and/or comprehensive attack response plans are mentioned.

A **5%** increase this year shows that now over half of FTSE 100 companies are heavily investing in Cybersecurity.

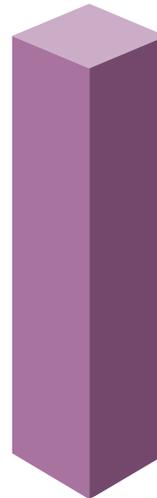
We are seeing a large amount of improvement in incident response capabilities, as well as penetration testing on internal networks.



43%

Standalone action plans

Mentions of action plans implemented in order to deploy security measures.



No mention

No mention of investments aimed to address cybersecurity risks.



6%

Personal Data Protection continues to gain corporate recognition



An extensive increase (**15%**) in the mention of Data Protection from last year shows that two years on from GDPR, companies are still maturing in the data protection domain.

How do companies understand the risks associated with personal Data Protection?



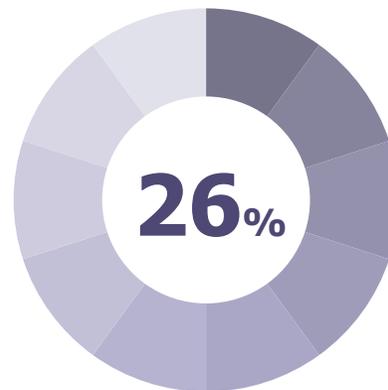
Cyber and Operational Resiliency moves to the forefront

With closer scrutiny from financial services regulators, it's no surprise that companies are starting to deploy cyber resiliency measures. We are seeing development in Disaster Recovery plans and a move to Cloud computing to ensure continuity in core business processes.

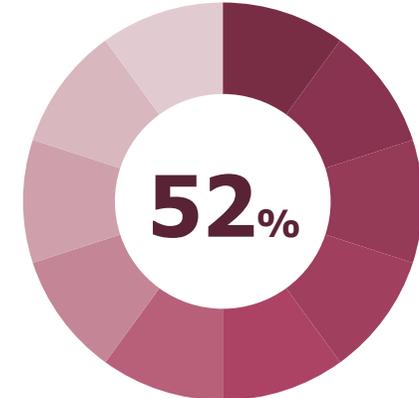
We are also seeing more investment in Operational Resiliency, as top companies are realising the importance of a flexible supply chain, the threat of climate change and the management of the recent Covid-19 outbreak.



of companies mention **Cyber Resiliency** in relation to a cyber attack or breach



of companies mention **both Cyber and Operational Resiliency**



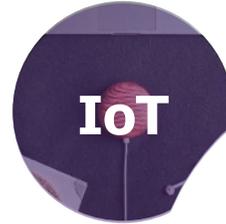
of companies mention **Operational Resiliency** and the impact on core business processes

Rise in top innovation

How to build a safer future? Companies continue to develop with innovative technologies, yet are leaving cybersecurity out of the discussion, when it should be centrefold.



37 mention it,
5 consider cybersecurity



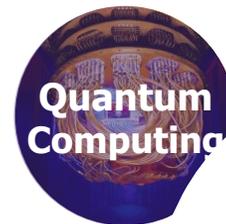
16 mention it,
1 considers cybersecurity



12 mention it,
2 consider cybersecurity



3 mention it,
1 considers cybersecurity



2 mention it,
0 consider cybersecurity

And to conclude



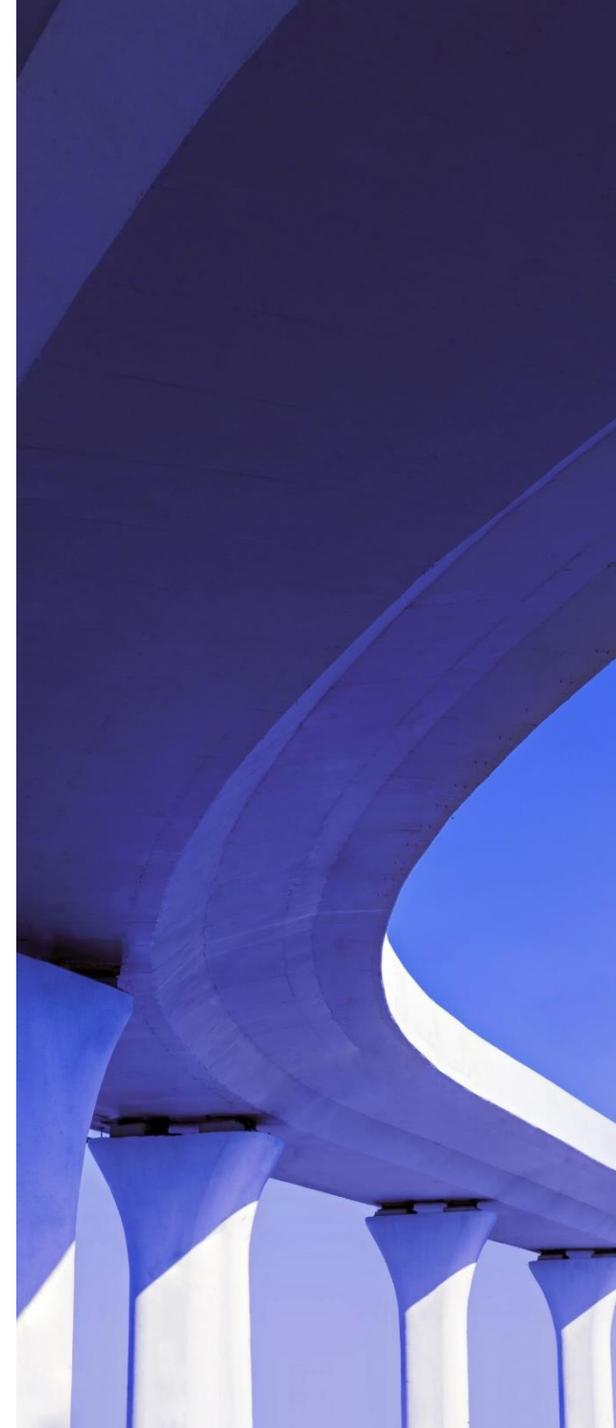
Overall the UK FTSE 100 improved on many dimensions across the board, with an average score increase of 11%. We saw the largest increases in both the data protection and training and awareness criteria.



However, the UK market as a whole obtained a maturity score of 10.2, still coming in third behind France CAC40 (12.03) and the US Dow Jones (11.18).



Whilst the FTSE100's overall performance trails the US and France, the UK demonstrates the highest commitment to investment (94%) for the second year in a row, displaying continued commitment to safe business practices.

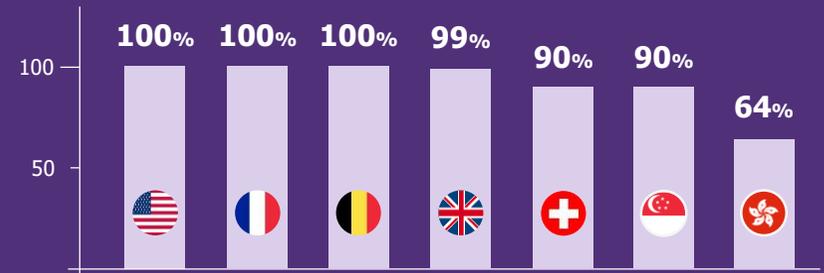


International analysis

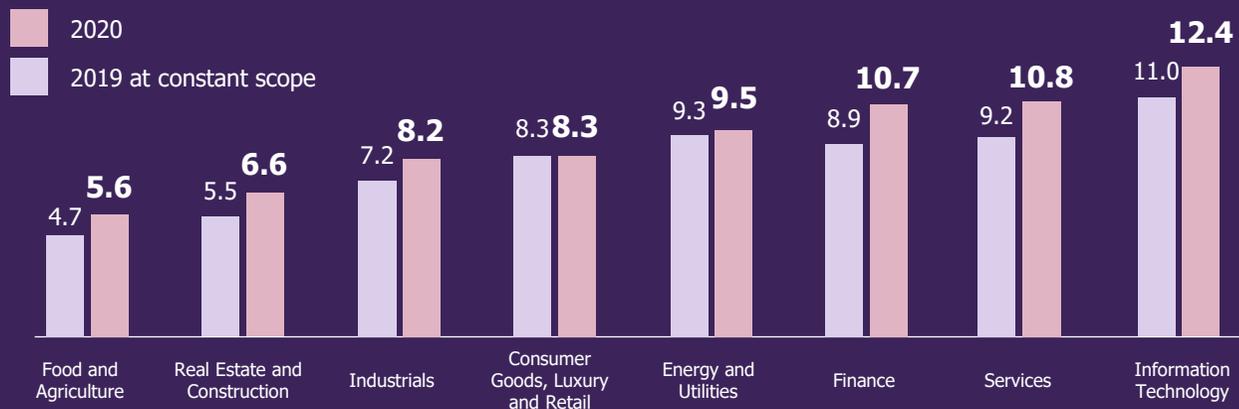
A great involvement at a global scale

The following figures are based upon a factual analysis of the most recent annual reports, published by companies up to June 1st, 2020 listed in the stock market indices in 7 global financial centres: Dow Jones (🇺🇸), CAC 40 (🇫🇷), FTSE 100 (🇬🇧), BEL20 (🇧🇪), SMI (🇨🇭), HSI (🇭🇰), STI (🇸🇬), representing a panel of 290 companies

92% of companies act on cybersecurity
+2 points VS 2019 at constant scope



The Information Technology sector leads the way alongside the services and finance sectors

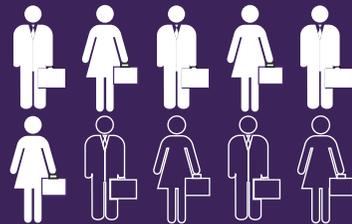


International analysis

Leading countries reach a maturity threshold

The bottom of the league is moving up

1.		France CAC 40	12.03	+1.97
2.		US Dow Jones	11.18	+1.03
3.		UK FTSE 100	10.20	+1.10
4.		Belgium BEL20	9.64	+1.07
5.		Singapore STI	7.73	+0.31
6.		Swiss SMI	7.32	+3.70
7.		Hong Kong HSI	5.15	+1.05



57%

address
cybersecurity at
Executive Committee
level

+3 points VS 2019 at constant scope

1.		UK FTSE 100	68%
2.		US Dow Jones	63%
3.		Singapore STI	63%



PRIVACY

80%

mention GDPR,
privacy or personal
data protection

+13 points VS 2019 at constant scope

1.		France CAC 40	100%
2.		US Dow Jones	93%
3.		Belgium BEL20	90%

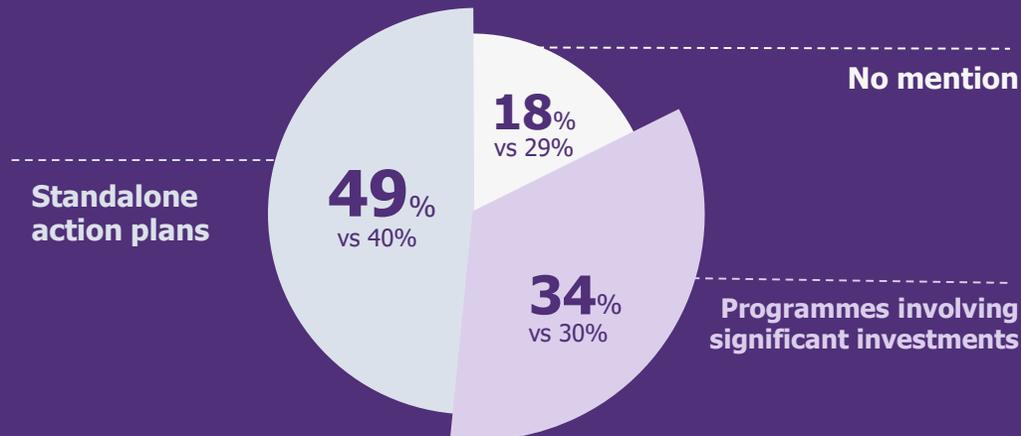
International analysis

Top performing countries #1 country per topic



Cybersecurity investments remain fragmented

Comparisons are provided at constant scope with last year



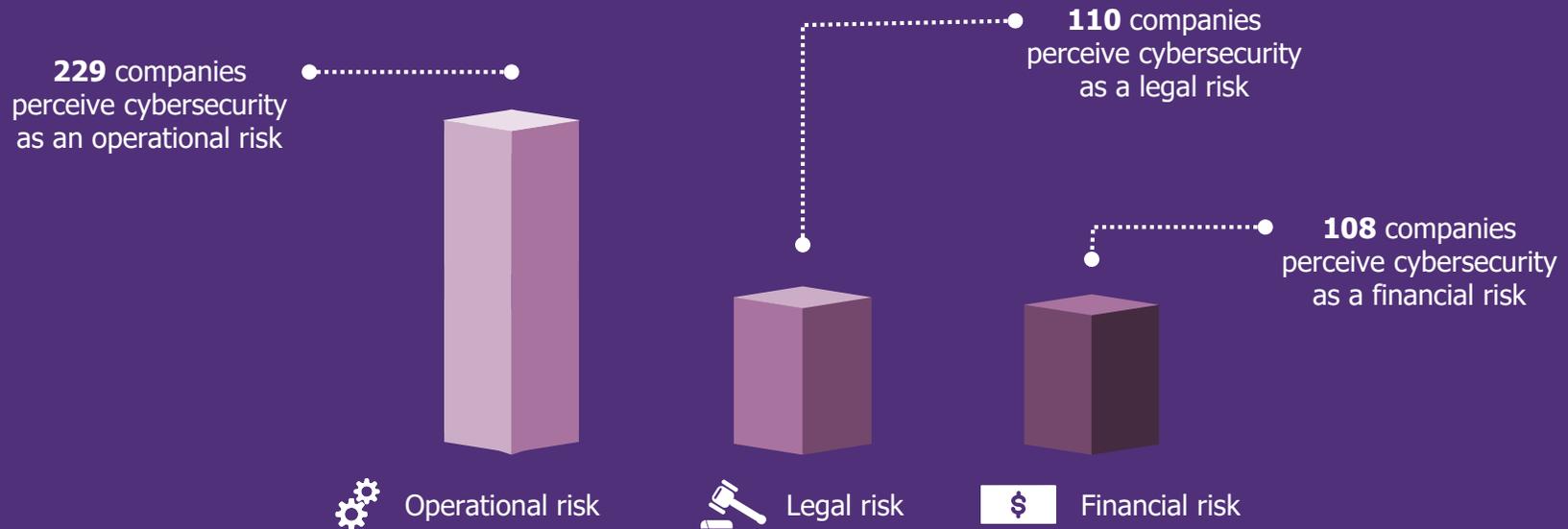
International analysis

Investments in innovative projects are still dynamic,
but cybersecurity is hardly part of the discussion, yet it should be.



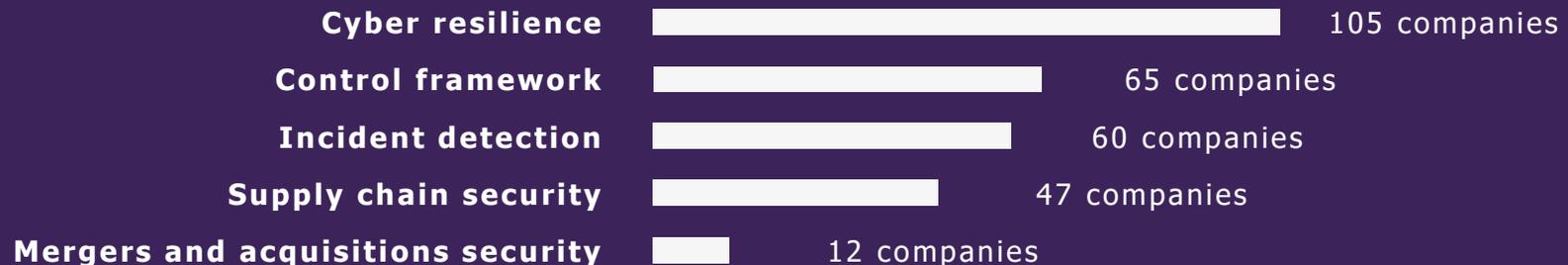
International analysis

Cybersecurity is mainly perceived as an operational risk



What are leading companies doing?

Emerging cybersecurity topics



APPENDIX

Study Caveats/Limitations

- / Many constituents of the FTSE 100 have differing financial years; they therefore release their respective annual reports throughout the calendar year. As a result, observations for some of the companies analysed may be up to a year out of date.
- / This study cannot guarantee to present any given company's cyber maturity as it exists in reality. This is because scores are based only on the information that companies wish to disclose.



Sector Definitions

Sector	Scope
Telecoms & Technology	Telecom providers, software & electronics
Financials	Banking, insurance, investment & asset management
Real Estate	Housebuilders, commercial construction/contractors
Industrials	Manufacturing, heavy/precision engineering, pharmaceuticals
Consumer Goods	Fast moving consumer goods, retail, supermarkets, tobacco
Services	Hospitality, travel, media, support services
Energy & Utilities	Oil & gas, electricity, water
Food & Agriculture	Foodstuffs
Industrials (Basic Materials)	Mining, packaging



Assessment chart (1/2)

	Weighting	Level 0	Level 1	Level 2
Information security issues and understanding of contextualised threat for the company	3	0 points No mention	+1 point Simple mention of the issues	+2 points Detailed mention of the issues including mentions of how the threat and/or information security specific risks have developed for the business
Cyber risks and its specific impacts on the company's business taken into account	3	0 points No mention	+1 point Mention of cyber risk	+2 points Detailed mention of risk and its impacts
Information security training and awareness	2	0 points No mention	+1 point Mention of awareness for staff and/or ExCo	+2 points Mention of large scale awareness or training initiatives and/or aimed at subcontractors or other external parties
Level of Executive Committee involvement in cybersecurity matters	2	0 points No mention	+1 point Mention of ExCo's involvement	+2 points Mentions the existence of an ExCo member directly involved and responsible for information security topics based on risk control (top owner of IS risk)
Cyber risk handling and coverage: cybersecurity investments, programme and action plan	2	0 points No mention	+1 point Mention of action plans	+2 points Mention of significant investments to cover cybersecurity risks (e.g. a multiyear cybersecurity programme, more than a hundred FTE dedicated to cybersecurity covering a substantial number of points of presence, tens of millions of Euros of cybersecurity budget or a rough estimate by Wavestone if not specified)
Integrating cybersecurity into digital transformation (AI, Machine Learning, IoT, Blockchain)	1	0 points No mention	+1 point Simple mention	+2 points Detailed mention of the specific risks of new technologies and/or specific securing actions
Cybersecurity governance	2	0 points No mention	+1 point Simple mention of the issues	+2 points Mention of the CISO's hierarchical position or mention of how the cybersecurity function is organised at Group level

Assessment chart (2/2)

	Weighting	Level 0	Level 1	Level 2
Security of business-specific systems (Industrial control systems, anti-fraud mechanisms, payment systems, etc.)	1	0 points No mention	+1 point Mention of business-specific risks	+2 points Mention of a significant programme and investments
Privacy: GDPR, Privacy, personal data protection	2	0 points No mention	+1 point Simple mention	+2 points Mentions nomination of a DPO and/or implementation of a compliance programme, a control body
Transparency and reaction to publicly announced cyber attacks or major incidents	0	-2 points No mention of a well known incident	-1 point Mention of an incident without its remediation actions	0 point Mention of incidents accompanied by action plans and/or changes made in remediation.
Taking out a cyber insurance policy	0	0 points No mention	+1 point Mentions taking out cyber insurance	+2 points Mention of a level of cyber insurance cover above €100M
Compliance with cybersecurity regulations (NIS, PCI-DSS, French LPM, HADS, NYDFS, etc.)	1	0 points No mention	+1 point Mentions regulations	+2 points Mentions plans to comply with the stated regulations
Respect of cybersecurity standards and certifications (ISO27001, NIST, FFIEC, CIS20, SANS, etc.)	1	0 points No mention	+1 point Mention IS standards	+2 points Mentions compliance, certification or alignment to the stated standards
Information security audit risk control	2	0 points No mention	+1 point Mention of audit and cyber risk coverage measures	+2 points Mentions a specific significant or broad control plan led by the cybersecurity team / internal audit / inspectorate general



WAVESTONE

Florian POUCHET
Partner

M +44 7493 86 77 66
florian.pouchet@wavestone.com

Olivia SPRINGATE
Consultant

M +44 7392 870 925
olivia.springate@wavestone.com

wavestone.com
@wavestone_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILANO *

BRUSSELS

GENEVA

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partners

WAVESTONE

