

How mature are annual reports of the Swiss Market Index (SMI) regarding cybersecurity?

July 2020



Valéry Pialat

Director

valery.pialat@wavestone.com

+41 22 544 7695



Dominique Bonnard

Senior Consultant

dominique.bonnard@wavestone.com

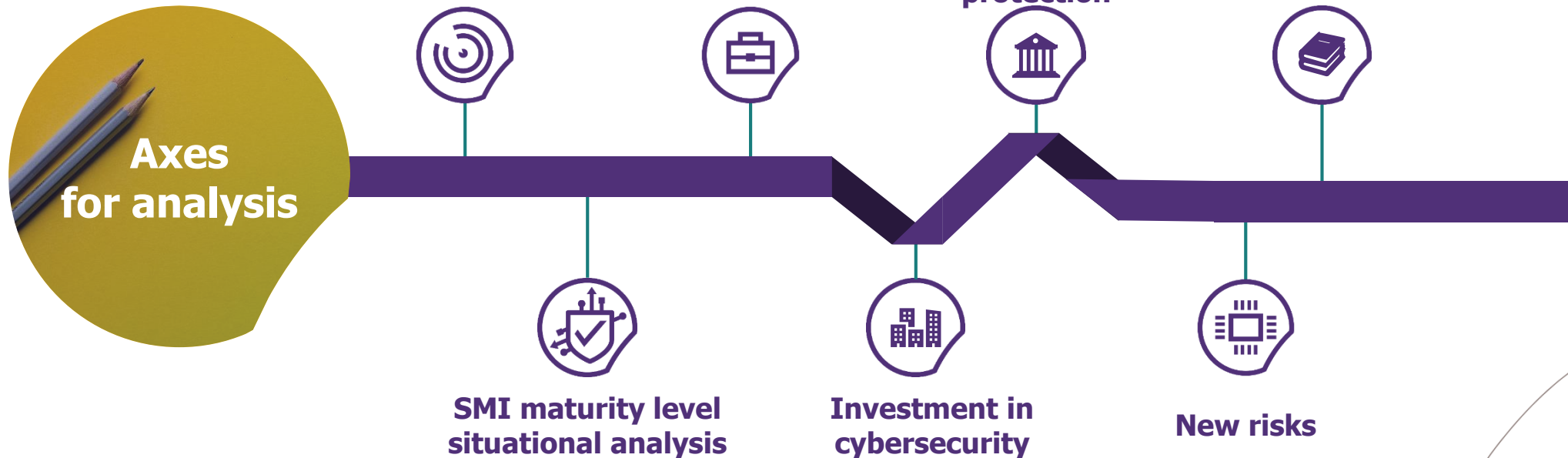
+41 78 245 2442

How mature are the SMI annual reports in cybersecurity?



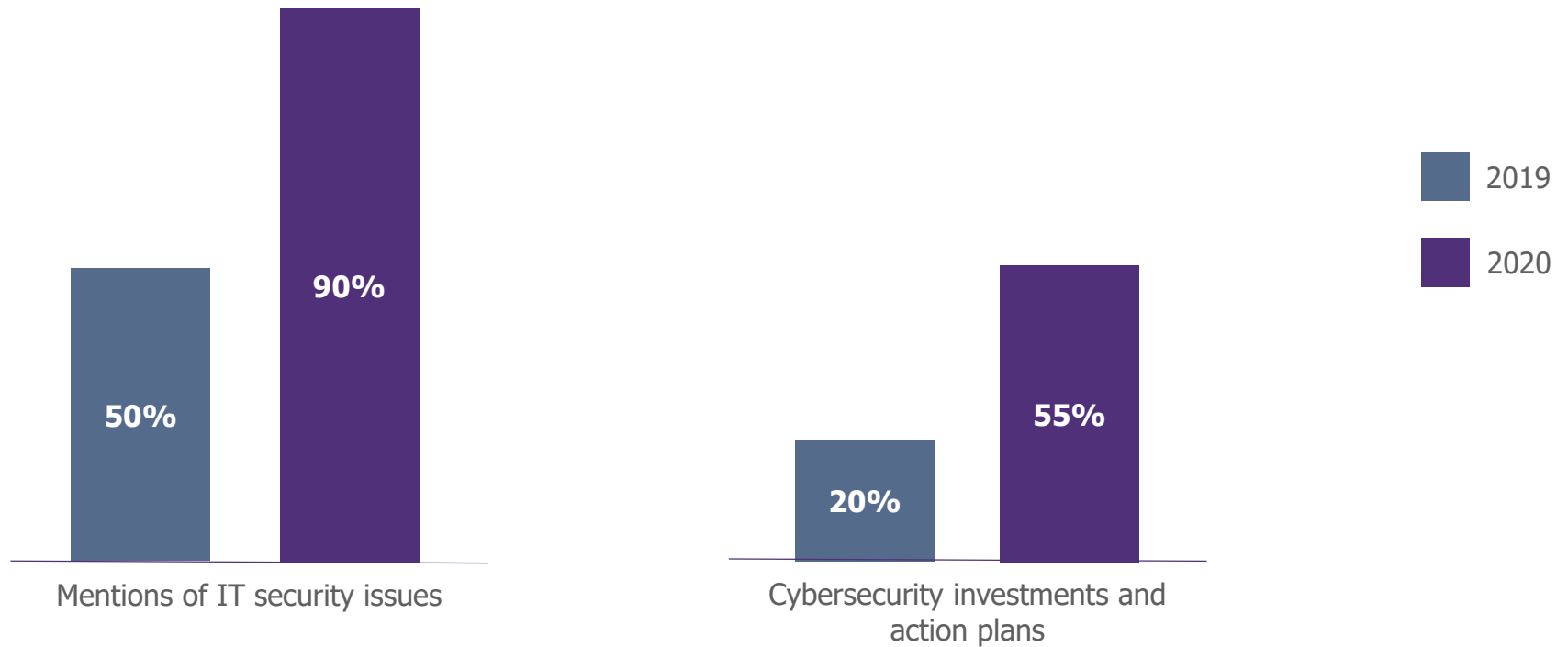
Method: this study is based upon a factual analysis of the most recent annual reports, published by the SMI companies up to 01/06/2020.

This analysis is based solely on the elements set out within these documents. It should be noted that they do not always reflect the completeness of actions underway in the field.



Finally 90%

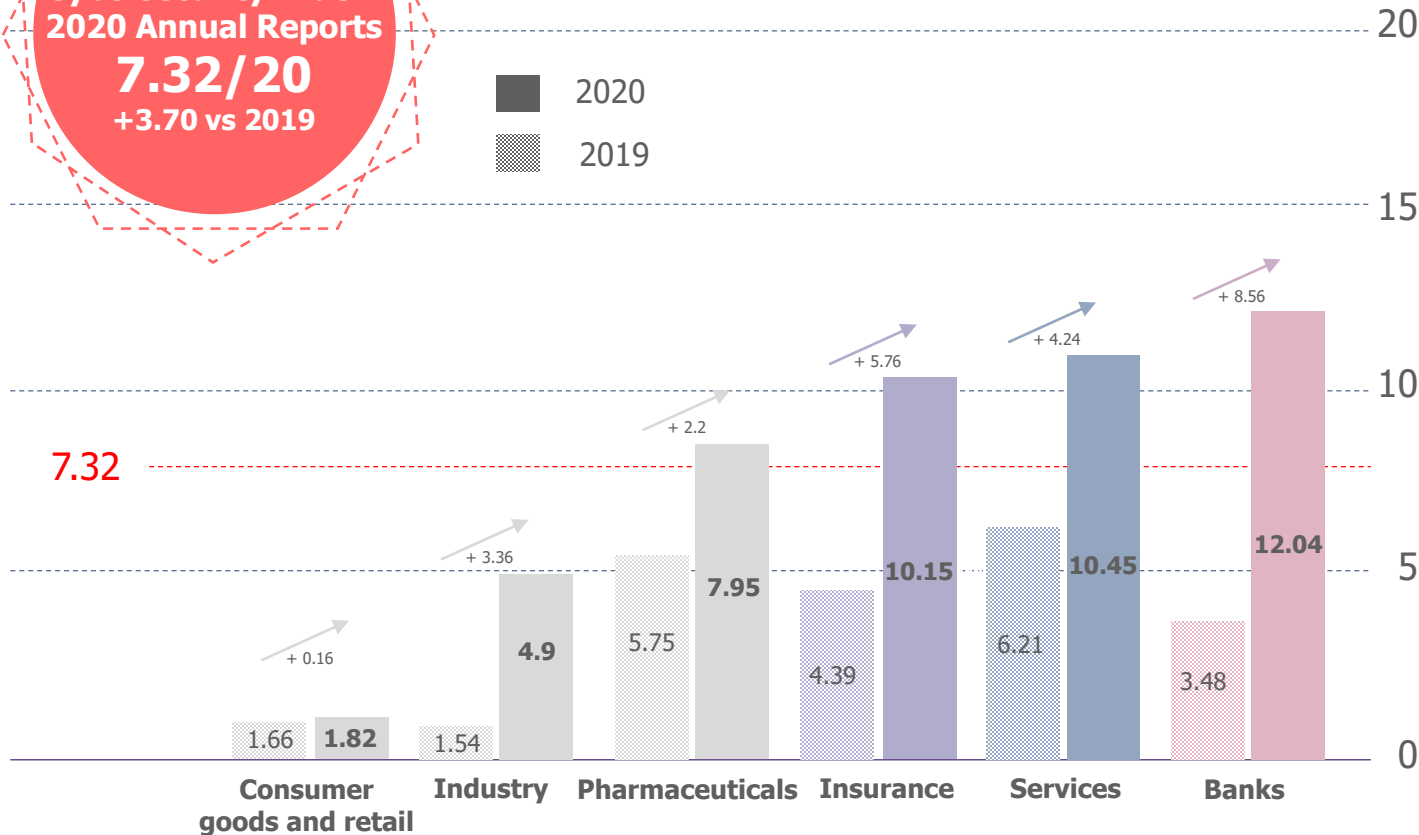
of SMI companies take cybersecurity into consideration



But many of them fail to turn it into concrete actions

Global awareness among all sectors, Financials and Services lead the pack

Wavestone's SMI
Cybersecurity Index:
2020 Annual Reports
7.32/20
+3.70 vs 2019



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 report. This index, scored out of 20, is based on 14 criteria weighted and marked between 0 and 2. These criteria* 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 vis-à-vis security incidents, regulations and respecting standards.

Protection and Controls

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

*The full assessment criteria are set out in the appendix

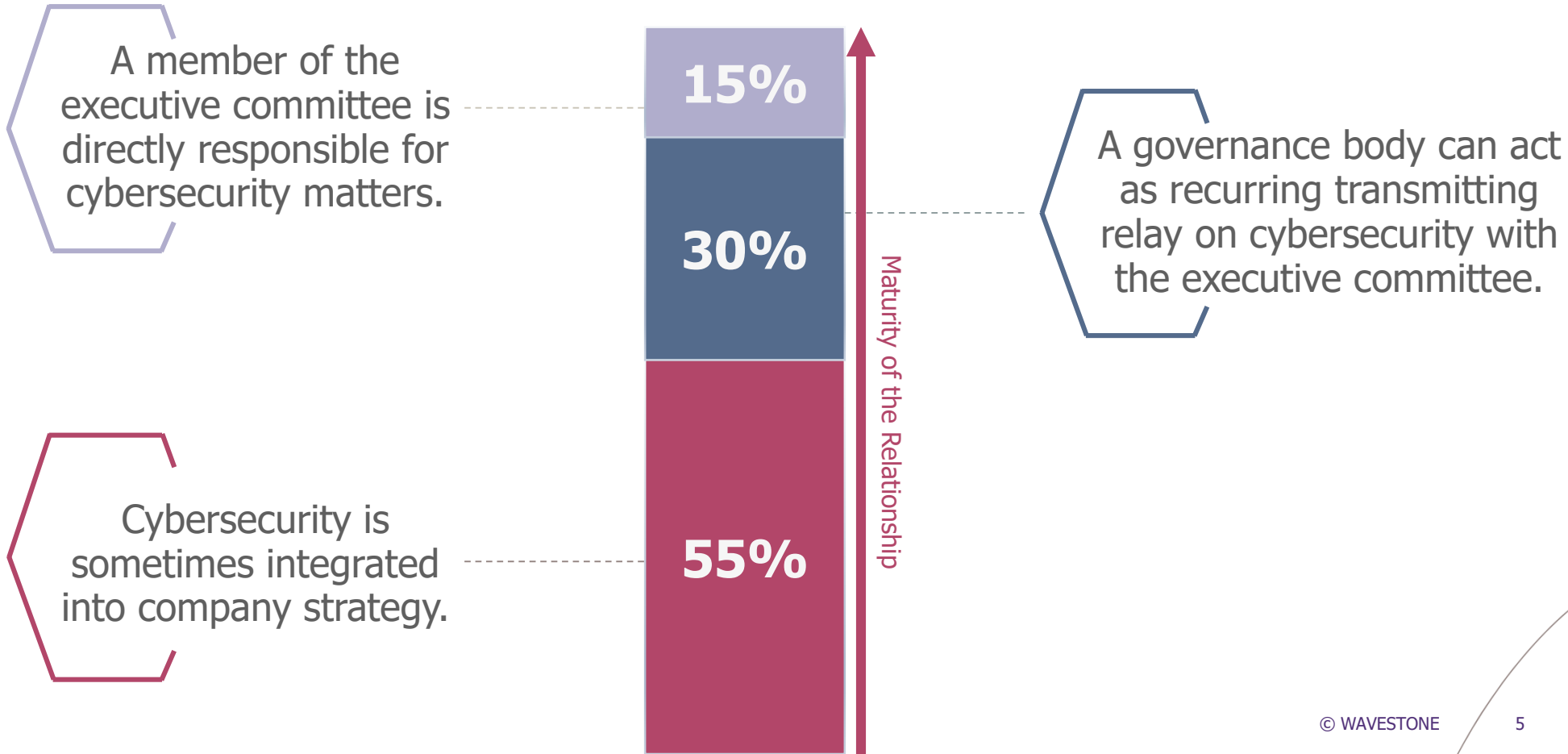
Executive Committees are more involved

40%

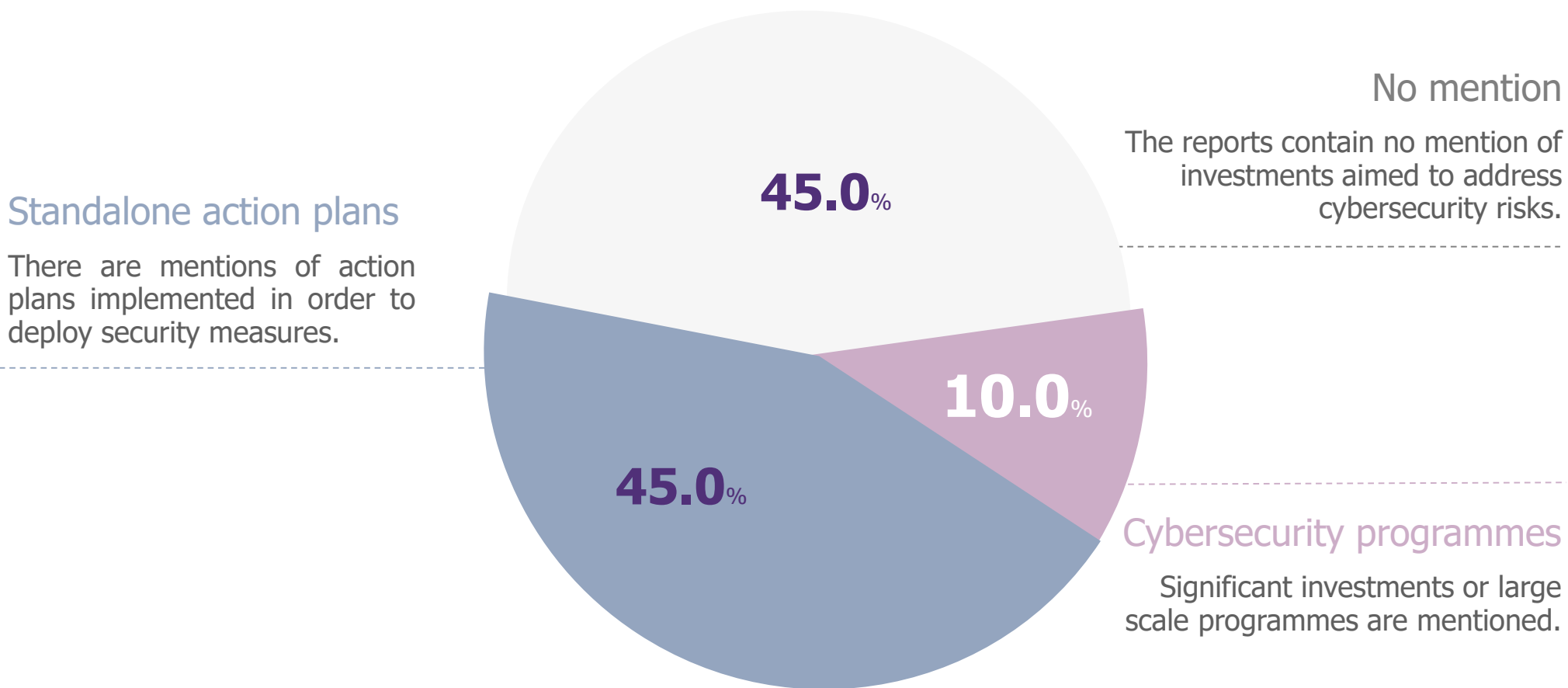
+25% vs 2019

of SMI groups address the question of cybersecurity at executive committee level according to their 2020 annual reports.

Their annual reports show that:

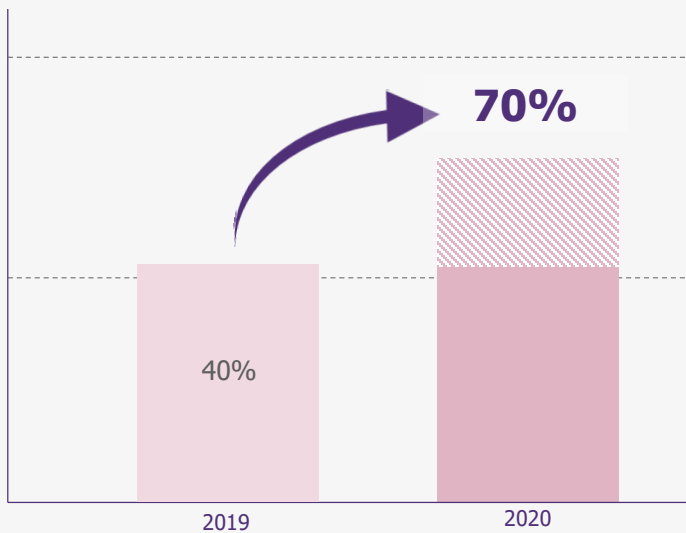


The handling of cyber risks remains fragmented

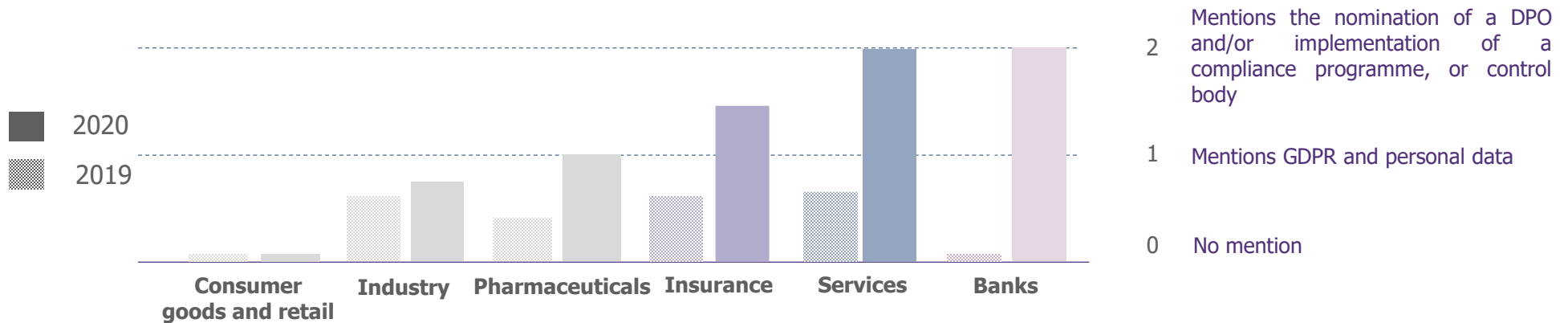


None of the SMI groups mentioned the amounts invested

Privacy and personal data: the global impact of privacy regulations



70% of SMI groups mention the GDPR* and personal data this year. This number has **increased by 30%** since 2019. Services and finance sectors show strong results.



*GDPR: General Data Protection Regulation

Highlights observed for SMI actors

CYBER RISKS NOW PART OF THE ANNUAL REPORT

SMI actors management is responsible for demonstrating the importance of any risk. Last year, they chose to value cyber risks in their “sustainability reports” rather than in their annual reports.

2020 marks the awakening of cybersecurity in the SMI annual reports. A vast majority of SMI actors are now concerned by the risks related to cybersecurity and address them in their annual reports. The gap between Switzerland has significantly closed with other countries included in our study in terms of cybersecurity maturity this past year.

CYBERSECURITY AWARENESS AND INVOLVEMENT INCREASES IN SWITZERLAND

For quite some time now, the Swiss government has shown a will to lead the change and to be the guarantor of internal security. By gradually strengthening its cybersecurity measures such as NSPC, DPL or TIC Norms, the level of responsibility of local actors has increased.

However, despite the raise in awareness and involvement, SMI groups do not yet mention specific cybersecurity regulations in their annual reports. Also, the vast majority dispenses with mentioning standards or certifications such as ISO27001, NIST or CIS20.

FINANCIALS AND SERVICES SECTORS LEAD THE PACK

The trend that was already observed in 2019 is confirmed this year. Both banks and insurance companies show significant progression in this year’s study. In particular, they demonstrate a great level of maturity with regard to privacy, data protection and the implementation of consistent cybersecurity programmes.

The World Economic Forum considers cyber strategy as an increasingly important part of any business strategy¹. We can expect regulators such as FINMA (Banks and Insurance companies) to keep moving in the same direction.

¹ <https://www.weforum.org/agenda/2020/01/what-are-the-cybersecurity-trends-for-2020/>

And to conclude



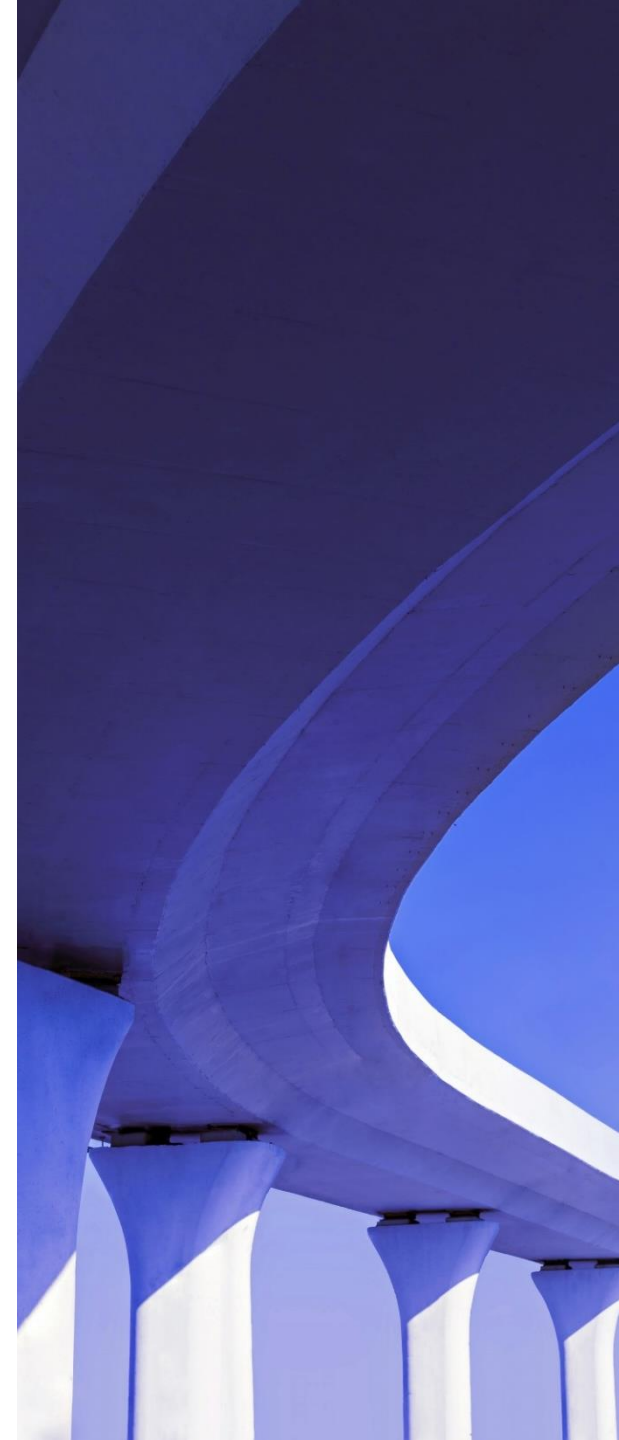
Cybersecurity in Switzerland is now taken into account by SMI companies in their annual reports. However, there is still plenty of room for improvement.



The guidance given by the Swiss legal authority (NSPC, DPL or TIC norms) seems to pay off as awareness has significantly risen this past year.



The coming year is crucial in consolidating the position of SMI groups in regard to cybersecurity. Capitalising on actions that have been taken is the key for continually improving it.

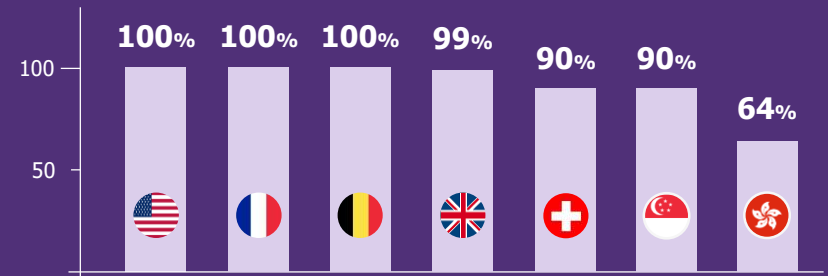


International analysis

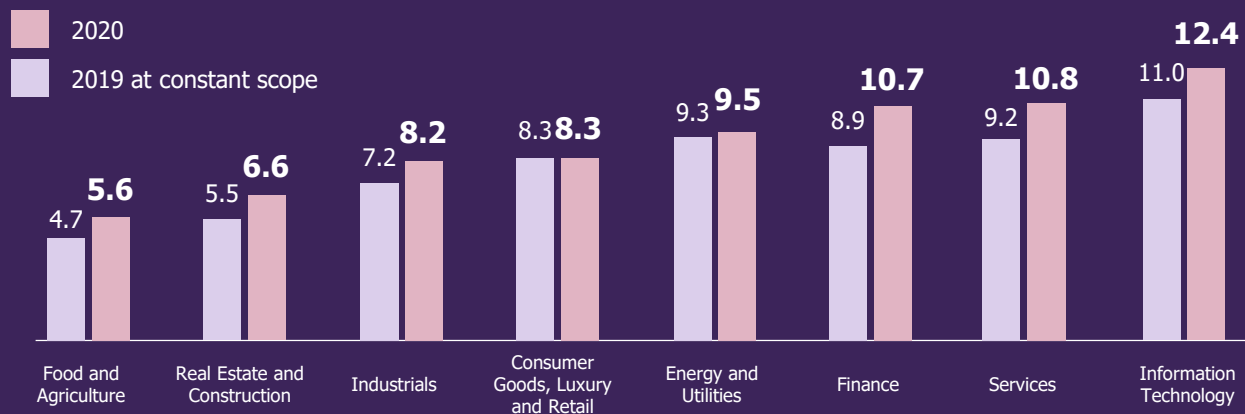
A great involvement at a global scale

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%

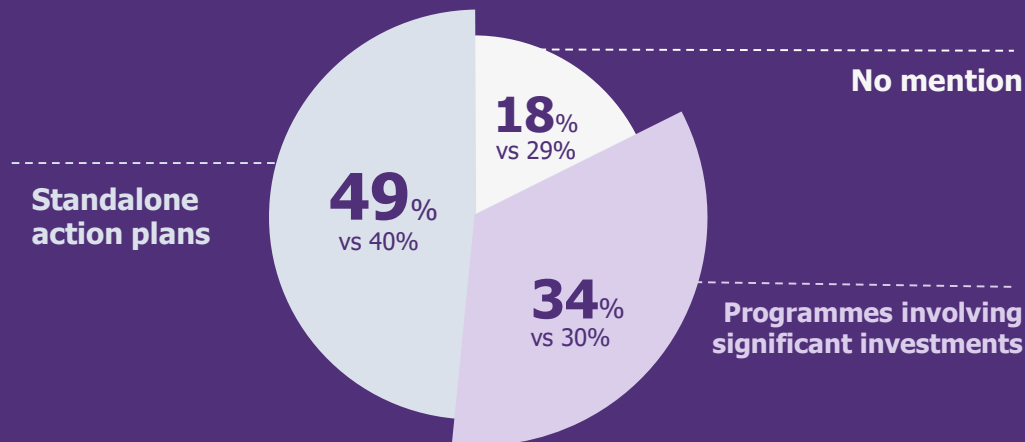
International analysis

Top performing countries #1 country per topic



Cybersecurity investments remain fragmented

Comparisons are provided at constant scope with last year



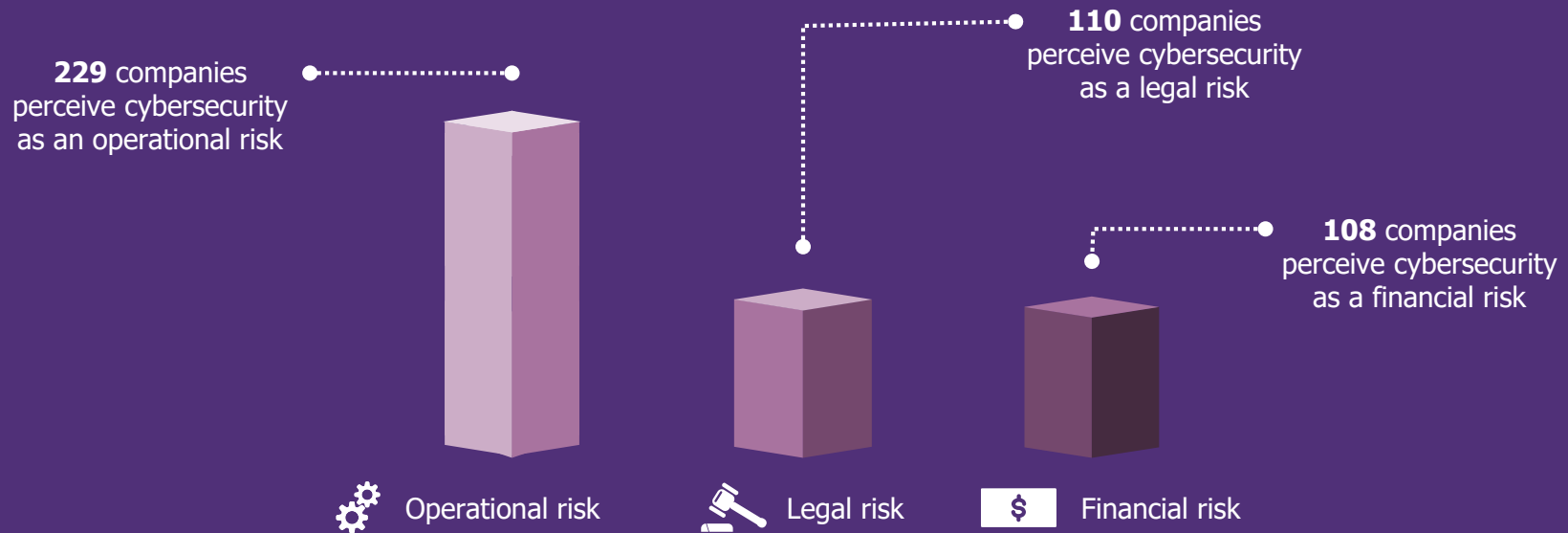
International analysis

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

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

The Positive Way

WAVESTONE

Valéry PIALAT
Director

M +41 78 748 9317

Valery.PIALAT@wavestone.com

Dominique BONNARD
Senior Consultant

M +41 78 245 2442

Dominique.BONNARD@wavestone.com



riskinsight-wavestone.com
@Risk_Insight



securityinsider-wavestone.com
@SecuInsider

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

