



WAVESTONE

Cybersecurity Index of Top Singapore Companies

July 2020



Chadi Hantouche

Partner, Head of Asia-Pacific

chadi.hantouche@wavestone.com

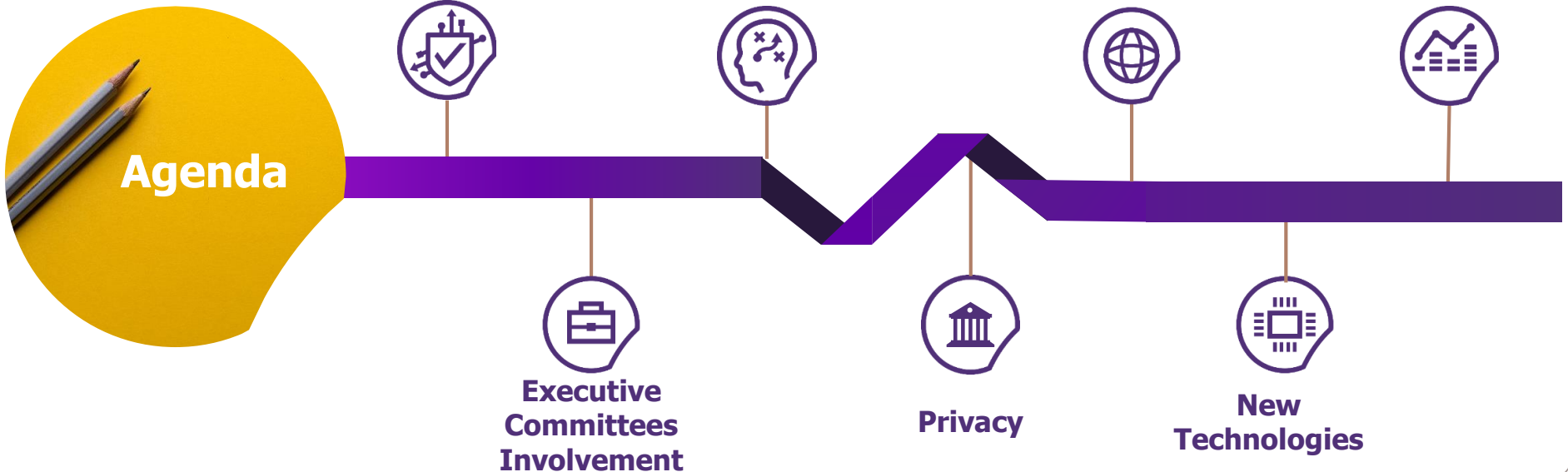
 @ChadiHantouche

How mature is the STI in Cybersecurity?



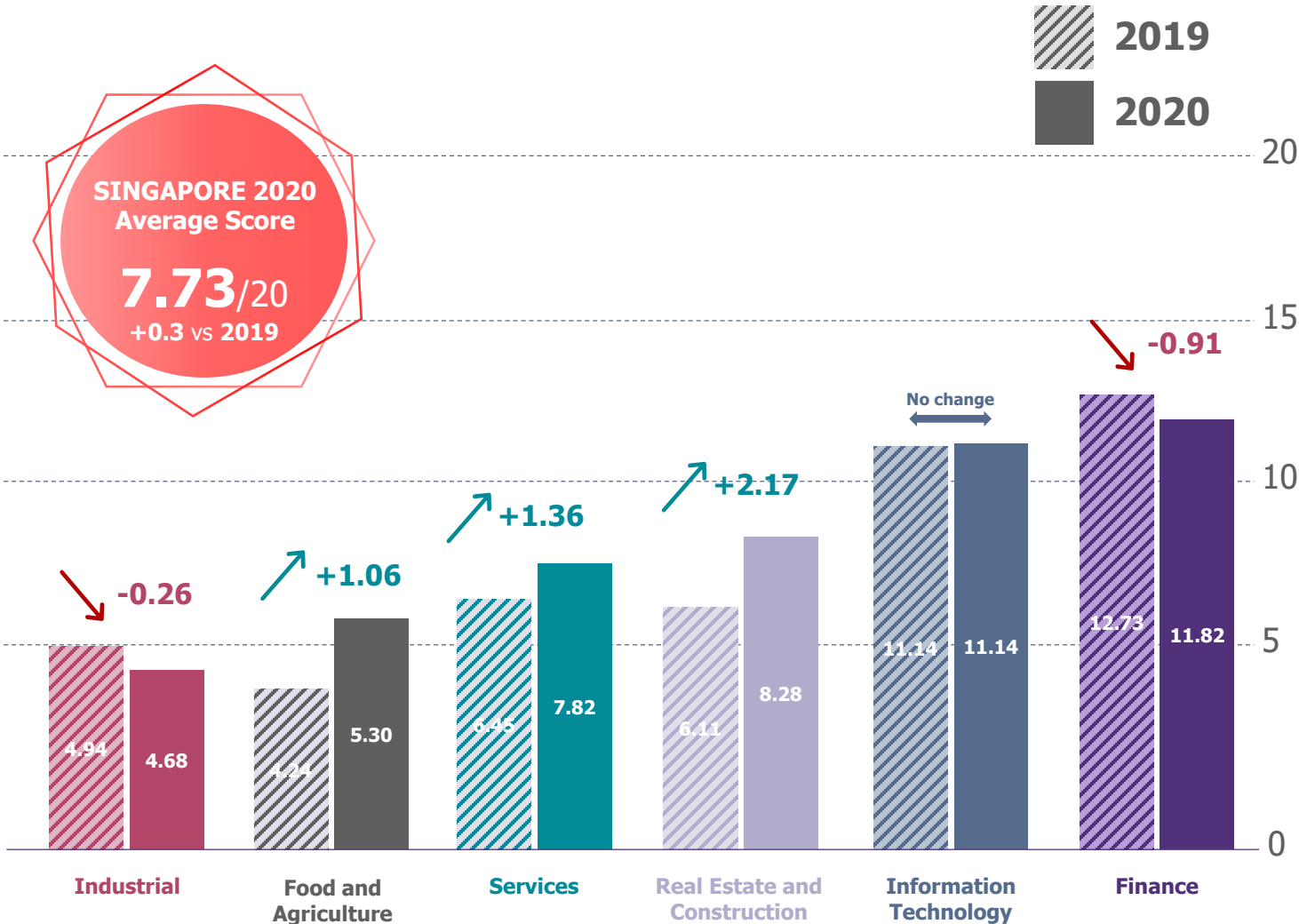
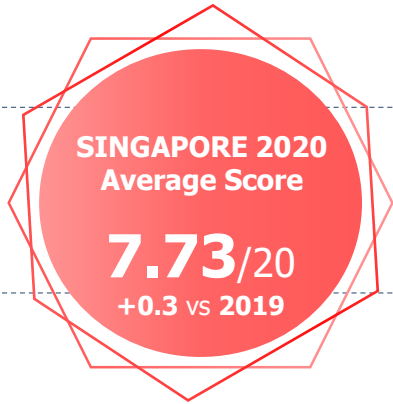
Methodology: This study is based upon a factual analysis of the most recent annual reports, published by the FTSE Straits Times Index (30 companies) up to June 1st, 2020. It is one of the studies conducted in June 2020 across 7 global financial centres: New York, London, Hong Kong, Paris, Singapore, Geneva and Brussels.

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



STI 30 Sectorial Analysis:

Finance and IT are leading the pack



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 criteria cover the following topics:

Risks and Challenges

Infosec challenges, cyber risks and impacts, cyber insurance coverage, digital transformation and new technologies' security.

Governance and Regulation

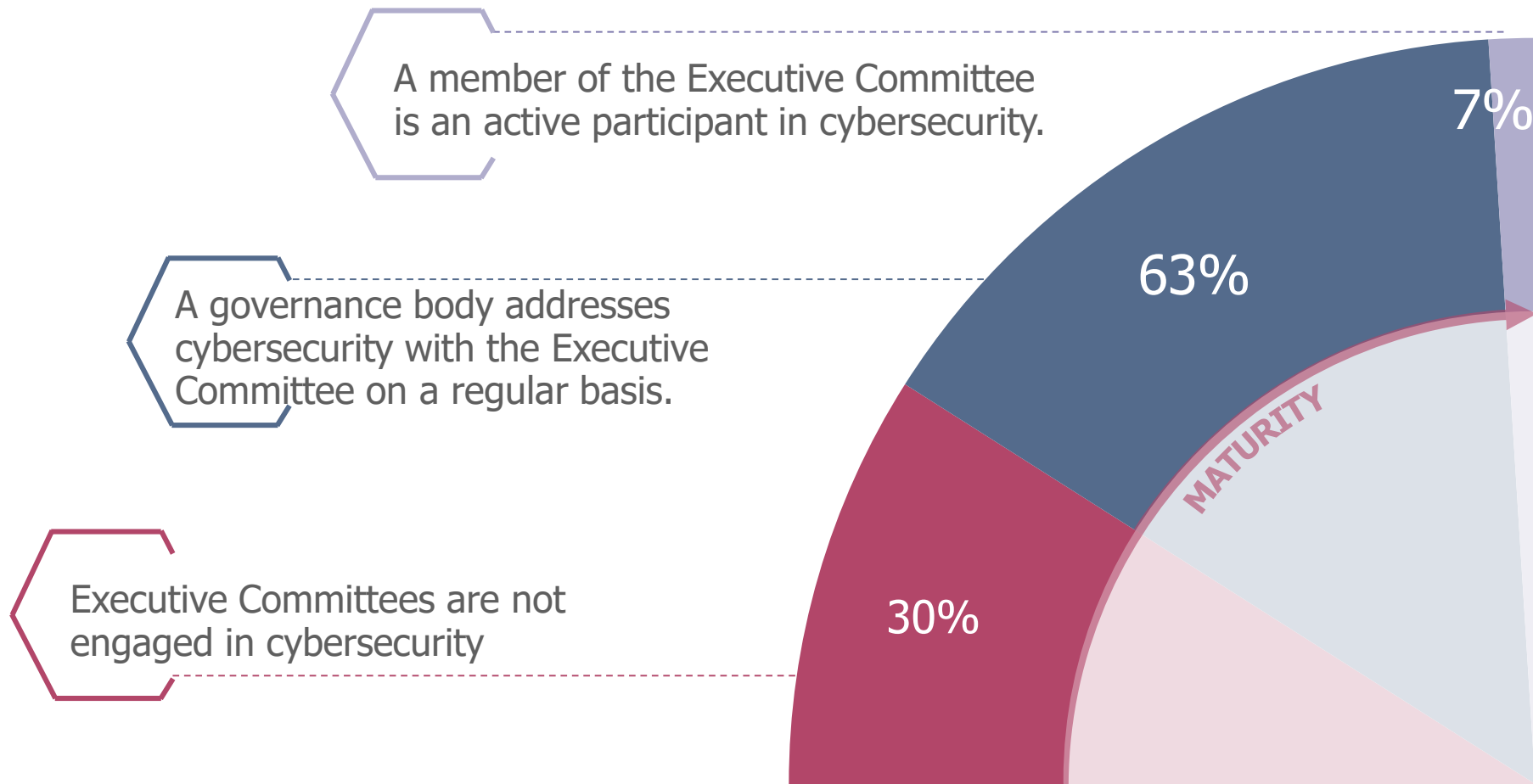
Executive Committee involvement, Information Security governance, Personal Data protection, Awareness and training, Transparency following security incidents, Compliance to regulations and standards.

Protection and Controls

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

Executive Committees are increasingly more involved

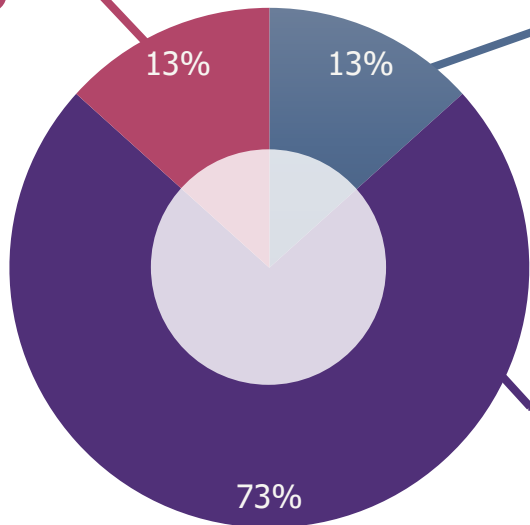
63% of STI companies address the question of cybersecurity at Executive Committee level.



Cybersecurity Risk and its Associated Business Impacts

87% of STI 30 companies acknowledge that they face cybersecurity risks
+11% vs 2019

No
mention

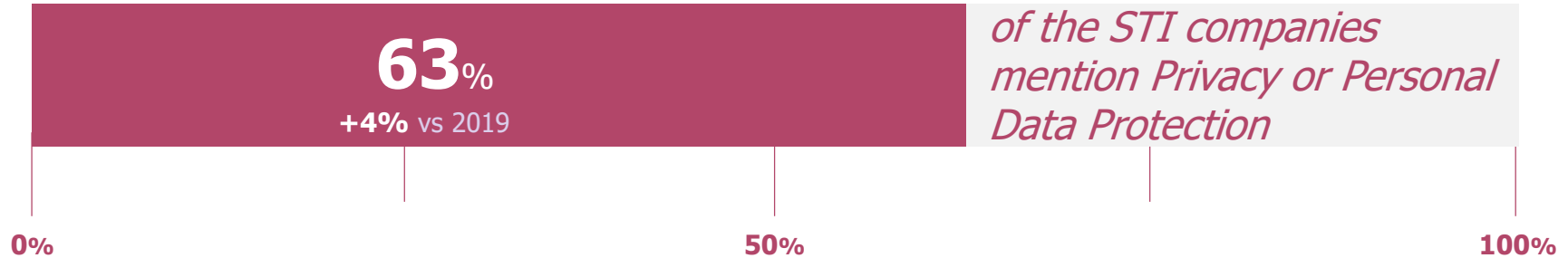


13% of companies expand upon these risks and make a specific, contextualized mention of its potential impacts on the business.

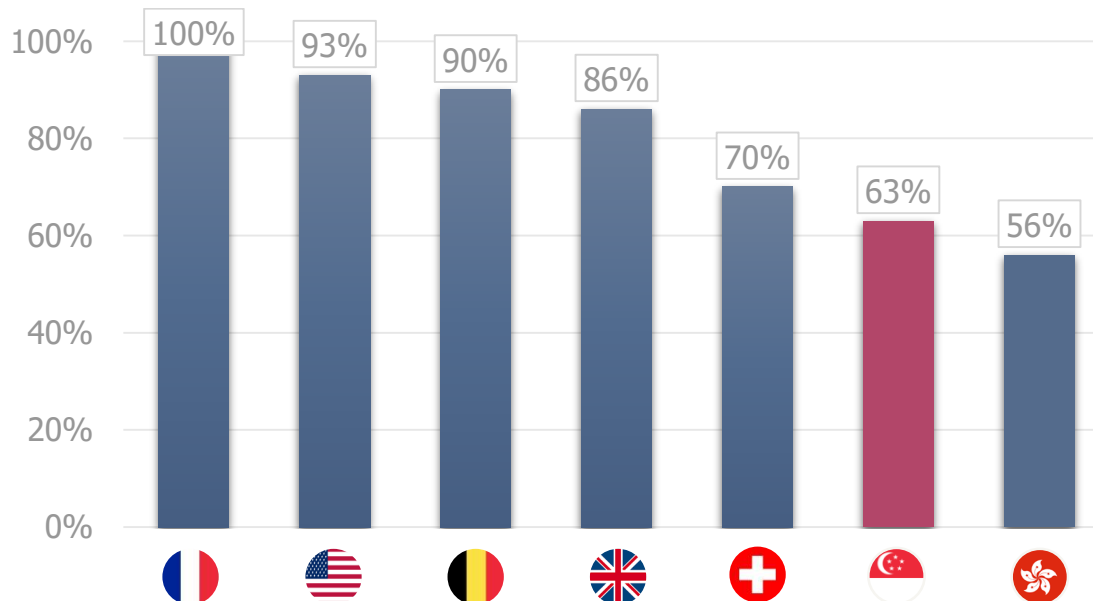
73% of companies have simple mentions of the risks

77% of companies state they take measures to tackle these risks.

Privacy and Personal Data Protection are still improving





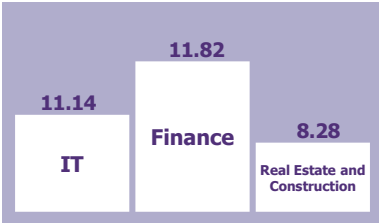
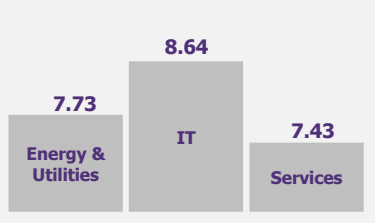
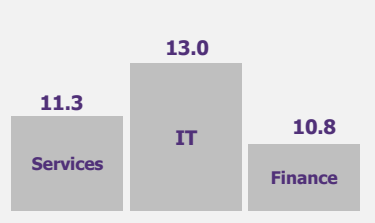
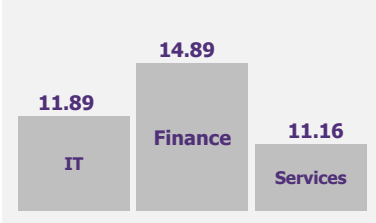


37% of companies make no specific reference to privacy and data protection regulations

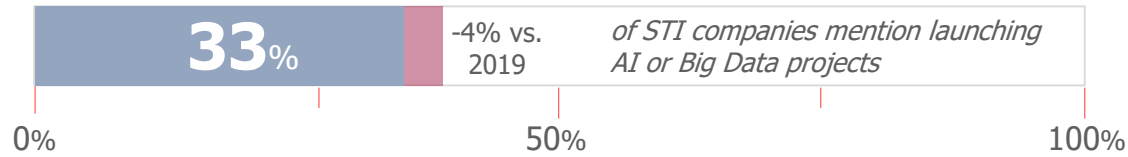


Compared to its international peers, Singapore is lagging behind in terms of Data Privacy.

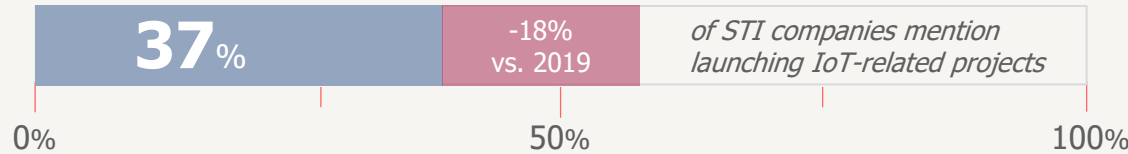
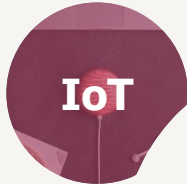
A comparative view of Singapore's STI Cybersecurity Index against global peers

				
Score	7.73/20	5.15/20	10.20/20	11.18/20
Leading Sectors	 <p>IT: 11.14, Finance: 11.82, Real Estate and Construction: 8.28</p>	 <p>Energy & Utilities: 7.73, IT: 8.64, Services: 7.43</p>	 <p>Services: 11.3, IT: 13.0, Finance: 10.8</p>	 <p>IT: 11.89, Finance: 14.89, Services: 11.16</p>
Awareness & Training	60% of STI firms address the topic	28% of HSI firms address the topic	69% of FTSE100 firms address the topic	33% of DJIA firms address the topic
Cybersecurity & Action Plans	77% of STI firms address the topic	58% of HSI firms address the topic	94% of FTSE100 firms address the topic	100% of DJIA firms address the topic
Privacy	63% of STI firms address the topic	56% of HSI firms address the topic	86% of FTSE100 firms address the topic	93% of DJIA firms address the topic

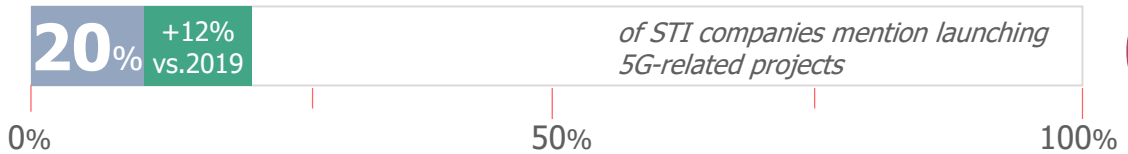
Cybersecurity is not part of Technological Innovations



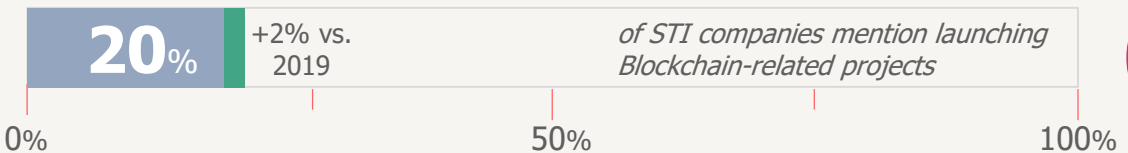
2 of them link it to cybersecurity



1 of them links it to cybersecurity



0 study the associated risks

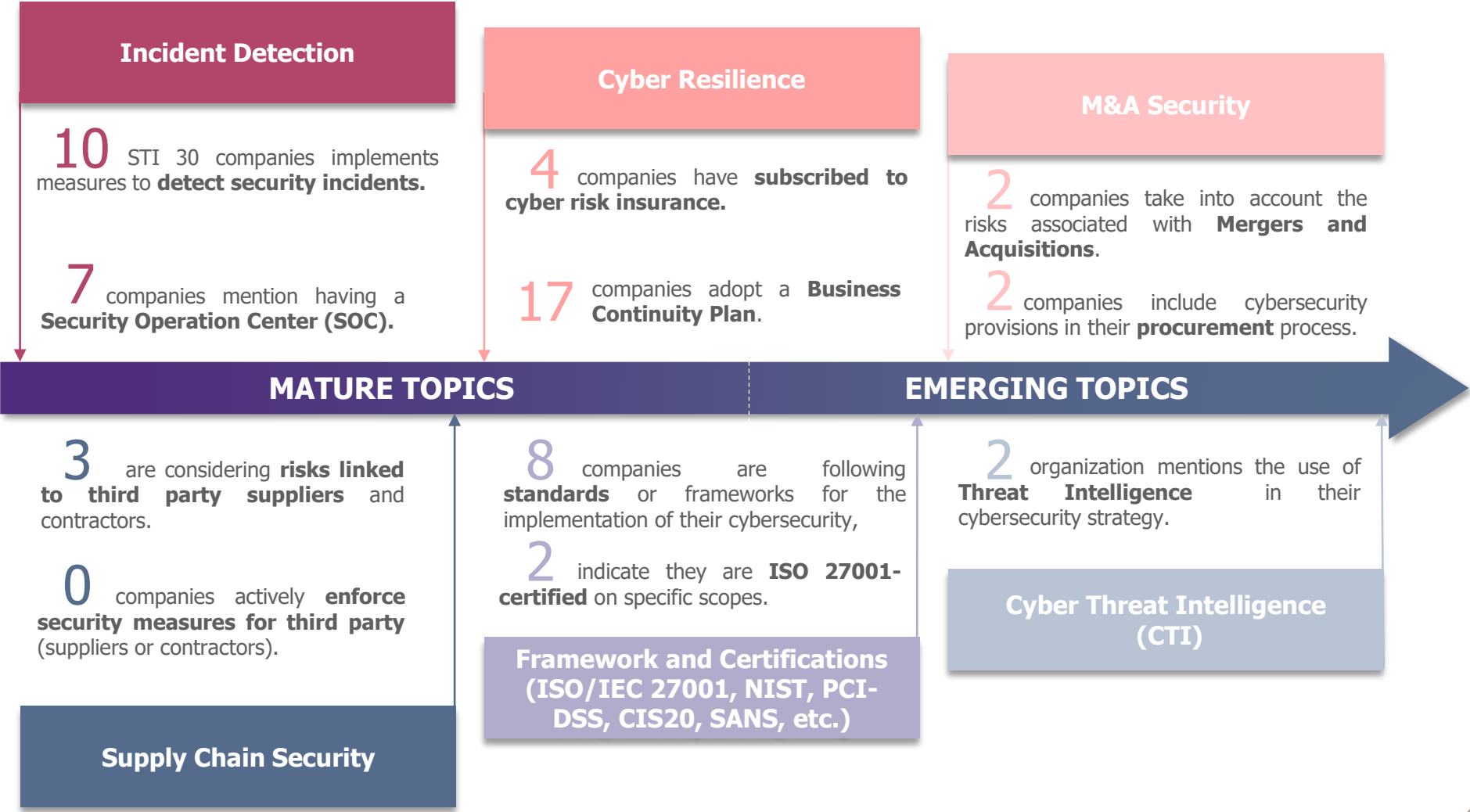


0 link it to better traceability, trust or transparency



0 of them link it to cybersecurity

Cybersecurity Trends within Singapore STI



Final Thoughts...



Singapore's STI companies demonstrate overall low scores across industries, with the exception of Finance and IT.



Singapore scores best on Cybersecurity Governance in our global study.



The numbers are slowly improving, and should continue to improve in the coming years, while companies' awareness rises.

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)

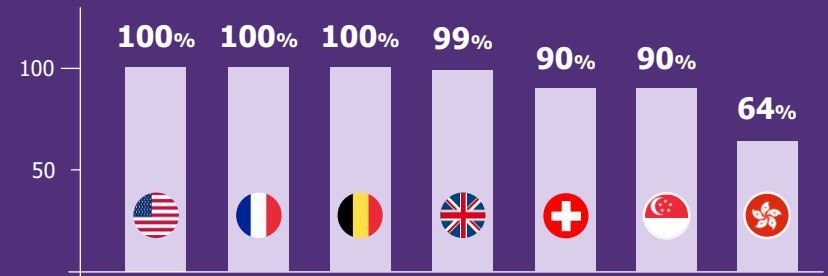
	Weighting	Level 0	Level 1	Level 2
Security of business-specific systems (Industrial control systems, anti-fraud mechanisms, payment systems, etc.)	1	0 points No mention	+1 point Mention of business-specific risks	+2 points Mention of a significant programme and investments
Privacy: GDPR, Privacy, personal 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

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%

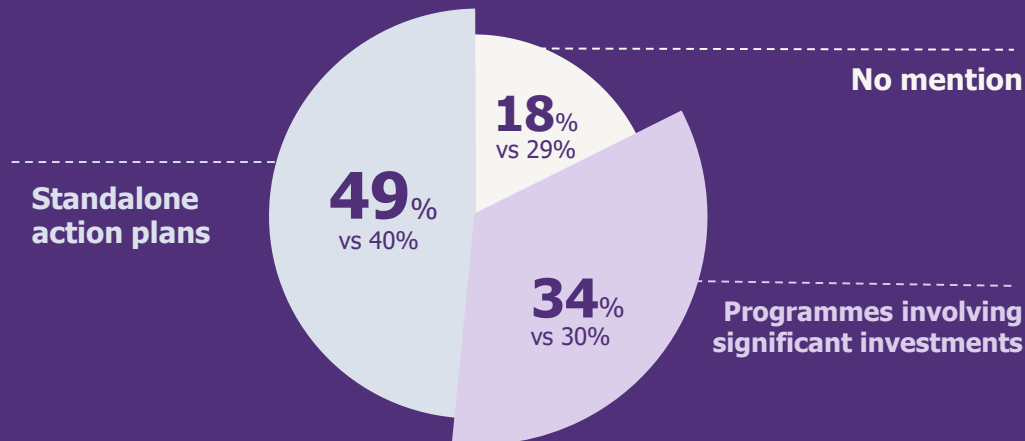
International analysis

Top performing countries #1 country per topic



Cybersecurity investments remain fragmented

Comparisons are provided at constant scope with last year



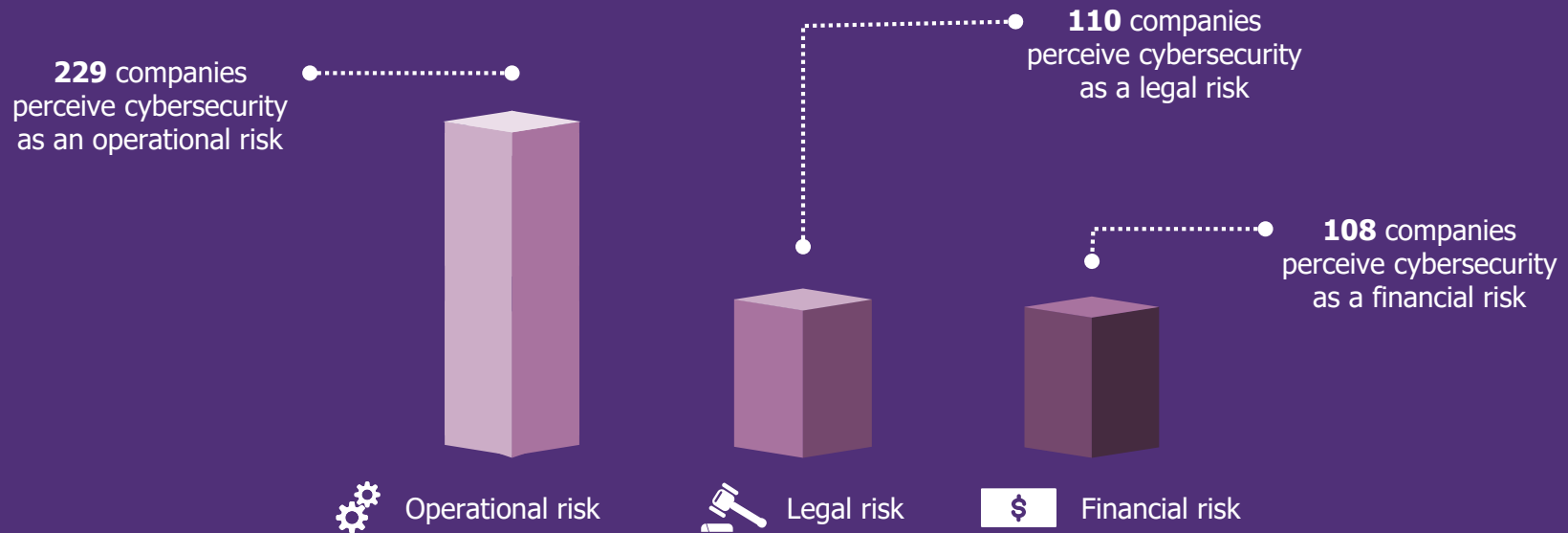
International analysis

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



PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILANO *

BRUSSELS

GENEVA

CASABLANCA

ISTANBUL *

EDINBURGH

LYON

MARSEILLE

NANTES

WAVESTONE

* Partnerships