WAVESTONE

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

June 2019

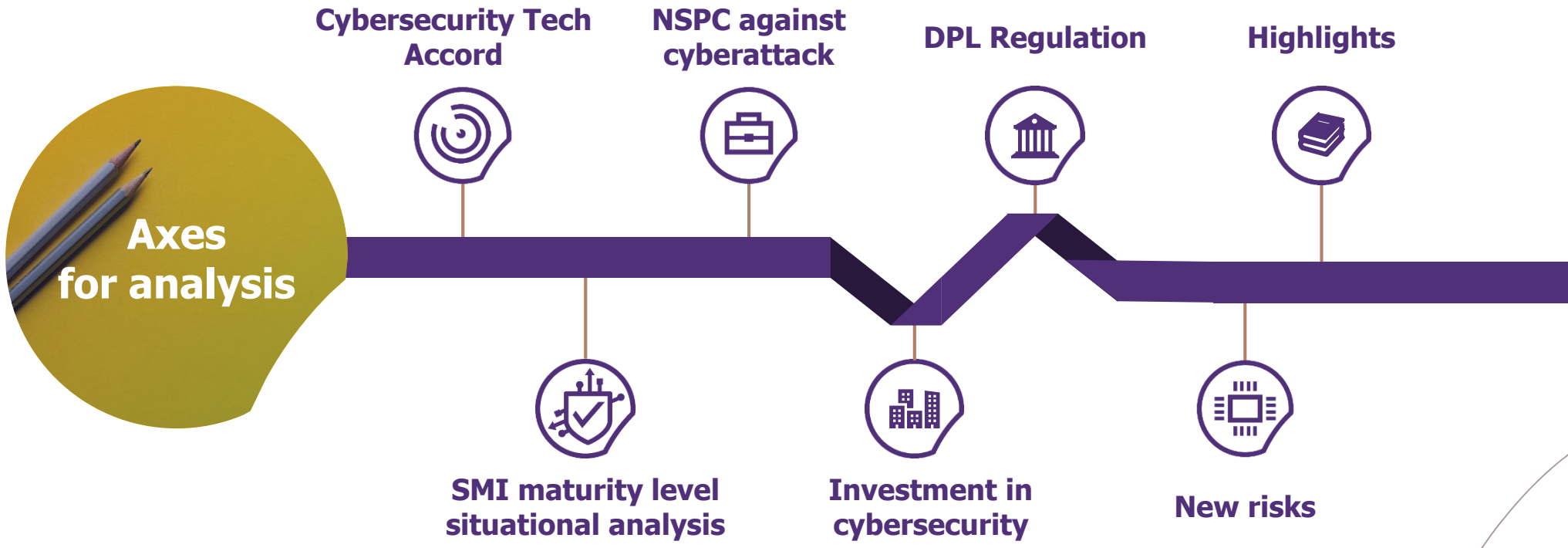
Harold Syfrig
Partner
harold.syfrig@wavestone.com
+41 22 544 7668

Valéry Pialat
Senior Manager
valery.pialat@wavestone.com
+41 22 544 7695

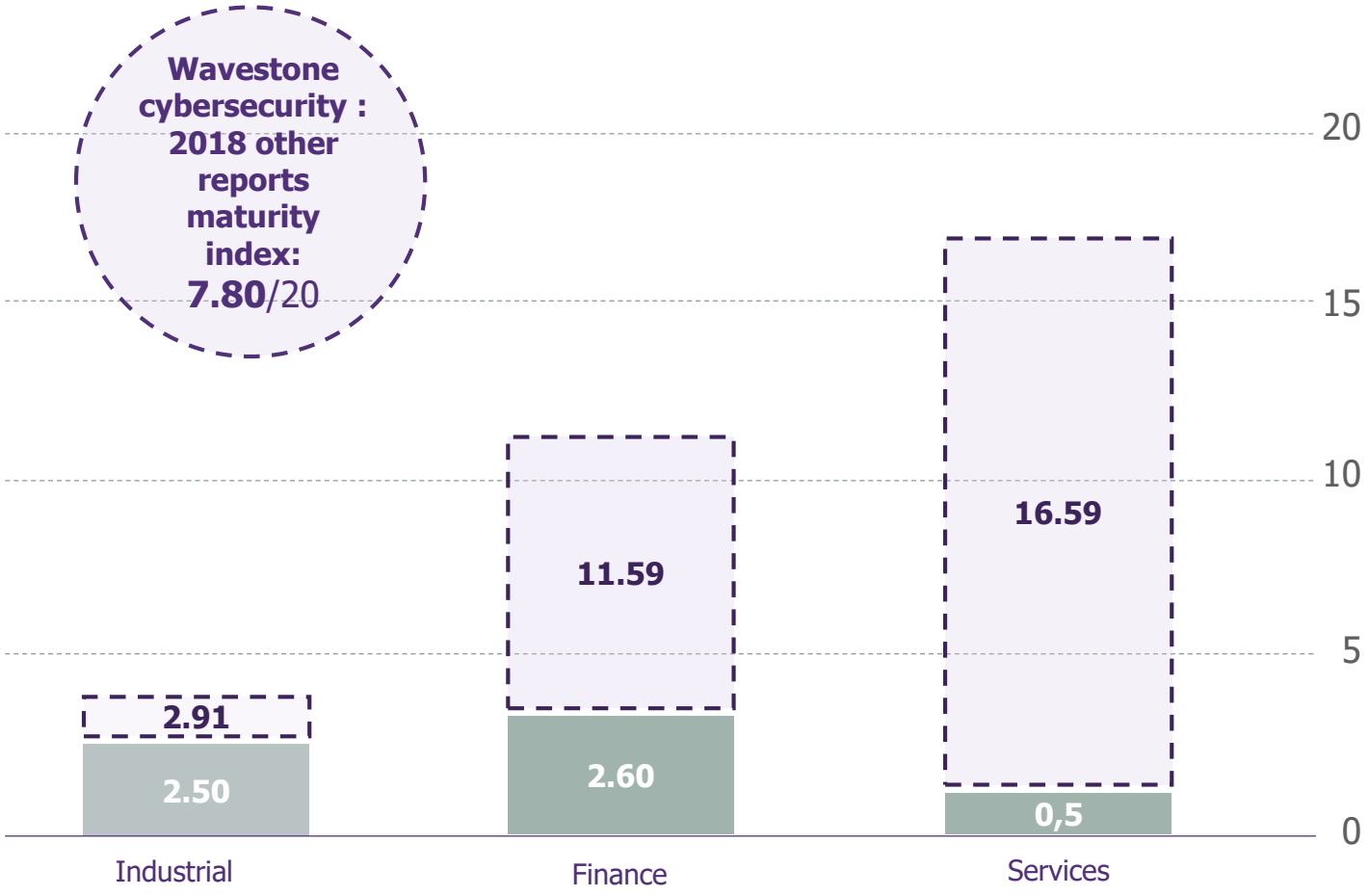
How mature are the SMI annual reports in cybersecurity?

Method: this study is based upon a factual analysis of the most recent annual reports and reference documents, published by the SMI companies on 06/01/2019.

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.



A maturity exalted out of the Annual Report



Analyse conducted in annual reports

Analyse conducted in other reports published by the companies : *sustainability reports. (CSR reports)*

Wavestone cybersecurity: 2019 annual reports maturity index

Annual reports maturity index provides an assessment of companies' maturity levels, based upon the content of their reference document. 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.

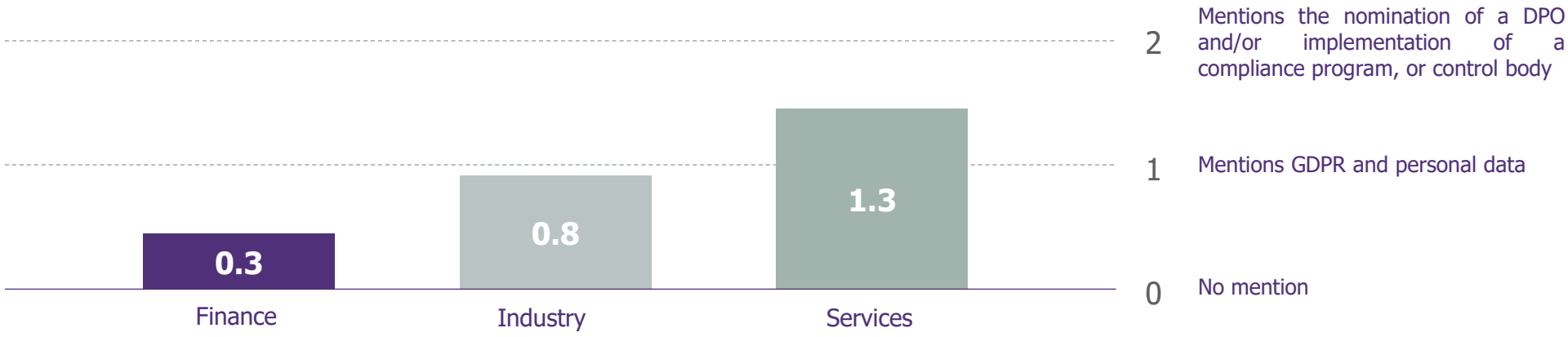
Governance and regulation
Executive Committee involvement, ISS governance, personal data protection, awareness and training, transparency vis-à-vis security incidents, regulations and respecting standards.

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

**The full assessment criteria are set out in the appendix*

Awareness of privacy and personal data

The SMI maturity has been led by the **services** sectors.



*GDPR: General Data Protection Regulation

Highlights observed for SMI actors

AWARENESS GOES OUTSIDE THE ANNUAL REPORT

A large part of SMI actors are concerned by the risks related to cybersecurity thematic.

They analysed the threats and classified them :

/ Critical data extraction

/ Critical system unavailability

/ Proxy data attack

/ Cryptocurrency risks

/ Online fraud

/ Destabilization operation

SMI actors management are responsible to demonstrate the importance of any risk. They choose to value them in their "sustainability reports" but not in annual reports.

CYBERSECURITY RESPONSIBILITY WILL INCREASE IN SWITZERLAND

The Swiss government wants to be the guarantor of internal security and gradually strengthens its cybersecurity measures. The aim of this measures is to increase the responsibility of local actors :

/ NSPC : National Strategy for Switzerland Protection against Cyber-risks (2018-2022)

/ DPL : Data Protection Law (2020)

/ Federal audit on telecommunication systems of control (since 2018)

/ TIC Norms (revised in 2018) : minimal norms to be respected per activity sector

SMI ACTORS VOLUNTEERS FOR CYBERSECURITY INVOLVEMENT

At the beginning of 2018, Switzerland answered to the French call for an international cooperation for trust and safety in the cyberspace. Major Cybersecurity agreements gather key market economic actors of the world, including SMI stakeholders.

To answer to the new challenges related to the cybersecurity risks, some of them made a deal with the Swiss EPFL to create a " Numeric Trust Center" in order to raise cybersecurity awareness at school.

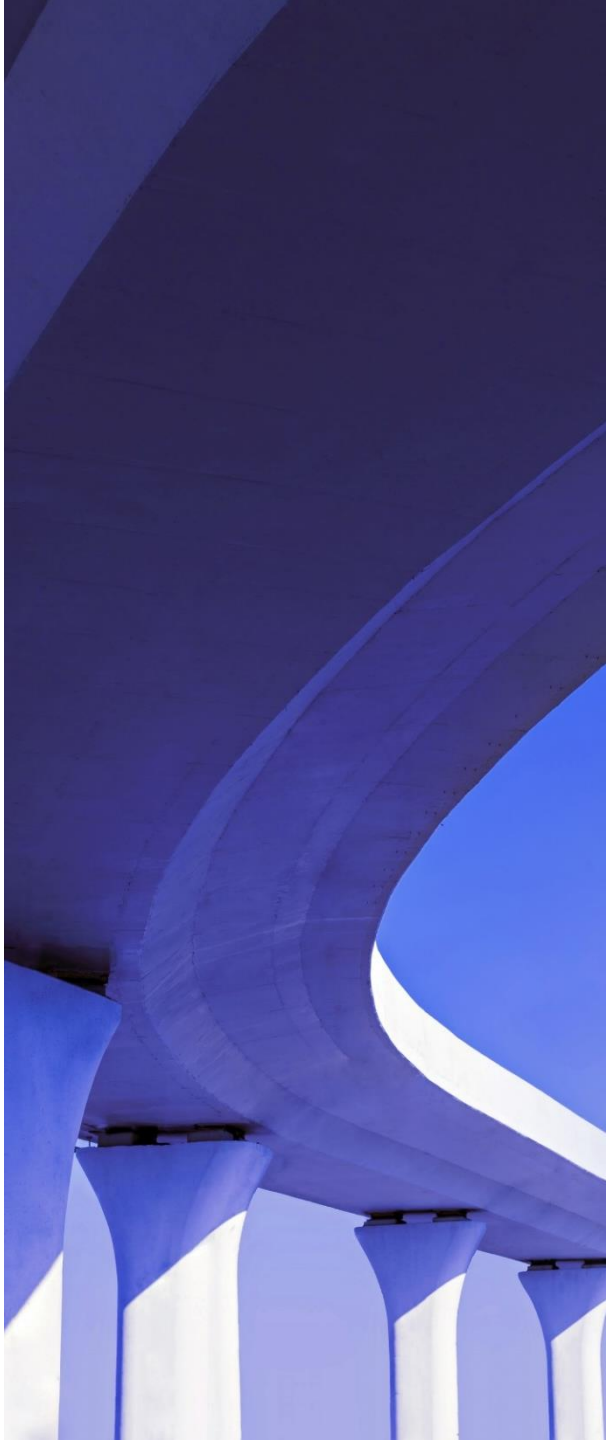
Finally, in 2020, many cybersecurity events are programmed to settle Switzerland involvement in the digital security.

And to conclude

Cybersecurity in Switzerland can not be fully assessed only based on the annual reports.

The Swiss legal authority is giving guidance to the SMI market players in order to improve their awareness and responsibility vis-à-vis cybersecurity risks.

For the coming year, an increased transparency on security incidents is expected following the application of GDPR, LPD, and NSPC.



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 programme and action plan	2	0 points No mention	+1 point Mention of action plans	+2 points Mention of significant investments via a programme (i.e. 10s of M€ 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
Information Systems Security (SSI) Governance	2	0 points No mention	+1 point Simple mention of the issues	+2 points Mention of the CISO's hierarchical position and how the organisation is set up 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

Harold SYFRIG
Partner

M +41 78 775 9383
Harold.SYFRIG@wavestone.com

Valéry PIALAT
Senior Manager

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