WAVESTONE

How mature are annual reports of the BEL20 regarding cybersecurity?

June 2020

Maryam AHSINA
Analyst
maryam.ahsina@wavestone.com

Noëmie HONORE
Manager
noemie.honore@wavestone.com
+32 (0)484 67 84 29

Marie SCHMIDT
Analyst
marie.schmidt@wavestone.com

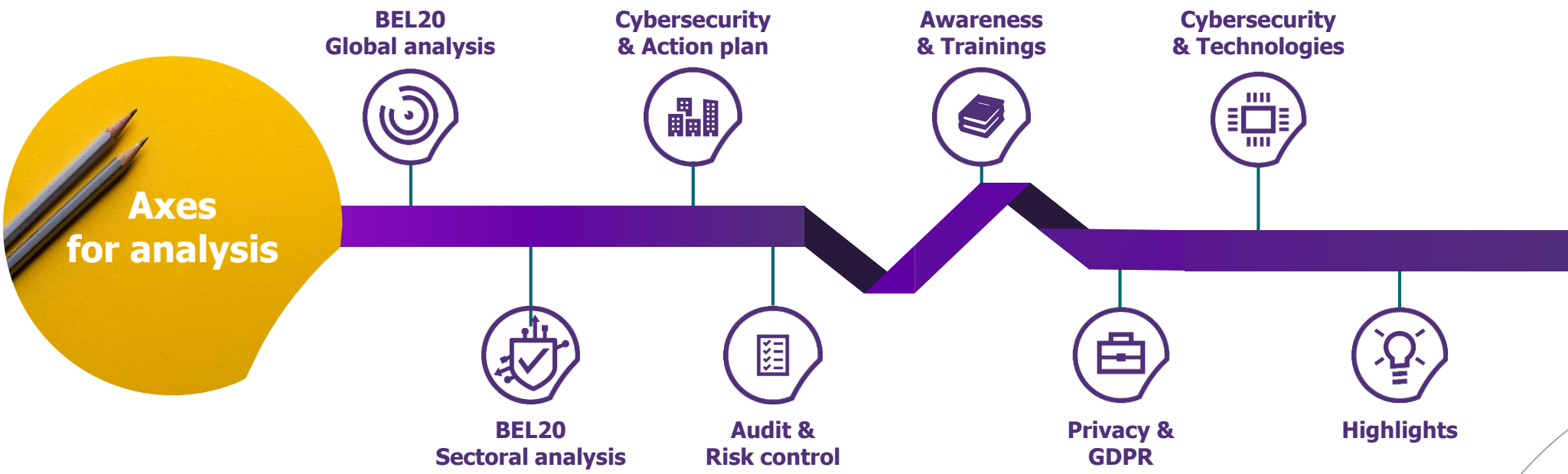
Marc VAN OENE
Consultant
marc.van-oene@wavestone.com
+32 (0)484 67 78 38

How **cybersecurity mature** is the **BEL20**?
2020 Edition

Method: this study is based upon a factual analysis of the most recent annual reports, published by the BEL20 companies up to **June, 1st 2020**.

Since the **method** and **BEL20 companies haven't changed** from last year, the 2020 BEL20 cybersecurity maturity edition gives us a great **opportunity to compare trends** and **evolutions** in the field of cybersecurity.

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.



BEL20 cybersecurity index 2020
Global analysis

Wavestone's Top Companies Cybersecurity Index: 2020 Annual Reports provides an assessment of companies' maturity level, 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 program, securing business systems, audits and controls

*For anonymity reasons, the **BEL20** companies have been grouped into **5 different sectors**: Consumer Goods & Retail, Finance, Industry, Information Technology and Real Estate.*

2020 edition shows an **average increase of 1,07** points compared to 2019 edition

In 2020, **100%** of the BEL20 are **mobilized** on **cyber issues**

Compared to **95%** in 2019

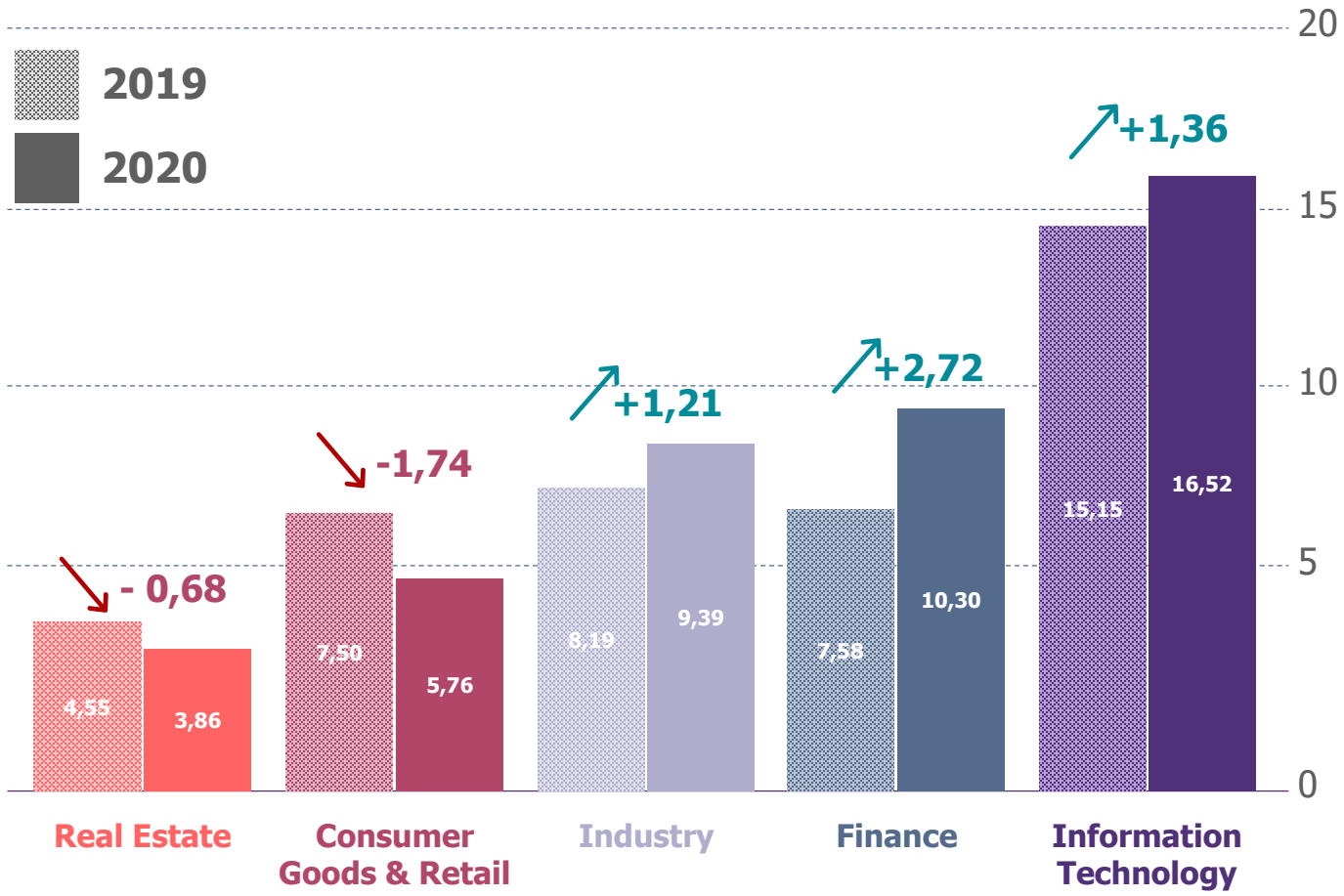
- **BEL20 companies have remained the same** compared to 2019 which reinforces the analysis and allows a more detailed comparison on the evolution of certain trends
- **13 companies improved their score** (by 2.5 points on average), 4 companies have an even score and 3 companies have a lower score (by -3,64 points on average)
- Despite an upward trend, **only 9 companies have a score above 10/20**, which indicates that further efforts need to be made to ensure a full scope cyber-maturity

*The full assessment criteria are set out in the appendix

BEL20 Sectorial Analysis
A widening gap between sectors

- **Information Technology** companies are still - by a substantial lead - in first position with a score **increase** of **1,36**
- **Finance sector**, which was in 3rd position in 2019, takes 2nd position with the biggest score increase. This trend can be explained by an increase in **security of business-specific systems** (anti-fraud mechanisms, payment systems, etc.)
- Compared to last year, **the gap** between the former and the latter **is widening**, with even a decrease in the score for **Consumer Goods & Retail** and **Real Estate** sectors

  They could lower the gap by being more explicit about the cybersecurity measures taken. Especially in terms **of cyber awareness** and **standards & regulations compliance**



*The full assessment criteria are set out in the appendix

Significant increase in companies' investment in **cyber risk action plans**

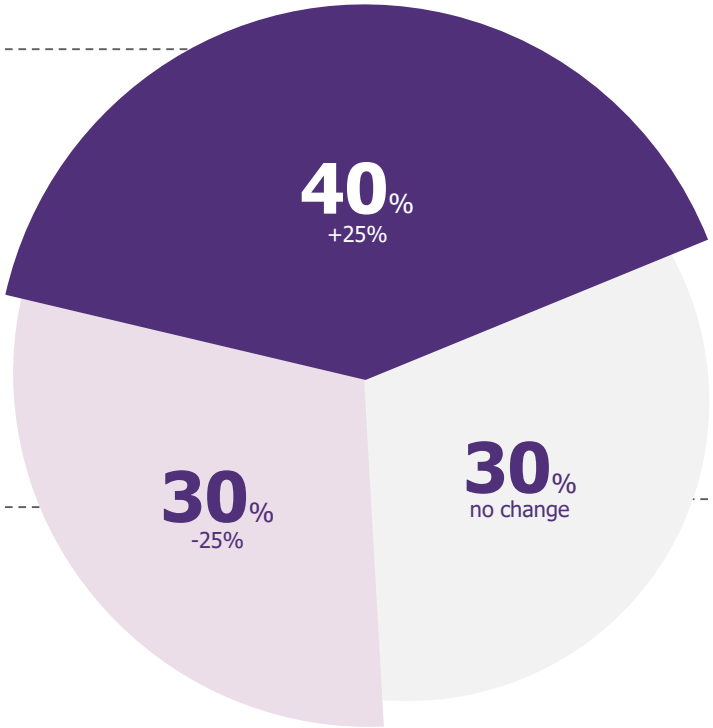
+25% of the BEL20 companies have invested in **cyber programs** to **protect** themselves from threats

70% of BEL20 companies mentioned an action plan to be able to respond to **cybersecurity incidents**. The **14** companies mobilized are not the same as last year, some have moved backwards but others have moved forward and we even observe a **25% increase** in the number of companies who have invested in a **significant program** to protect themselves from cyber risks.

IT and **Finance** are among the most advanced companies that have made the most progress in implementing **continuity action plans**. But the entire **Real Estate** sector is among the 30% of companies that **do not mention** anything about action plans against cyber risks.

Detailed cybersecurity action plans

Security programs involving **significant investments** are mentioned.



Standalone action plans

There are mentions of action plans implemented in order to deploy security measures.

No mention

30% of BEL20 companies **did not mention any action plans** to respond to cyber incidents.

Increase of mentions of **broad control plans** for information security **audits & risk controls**

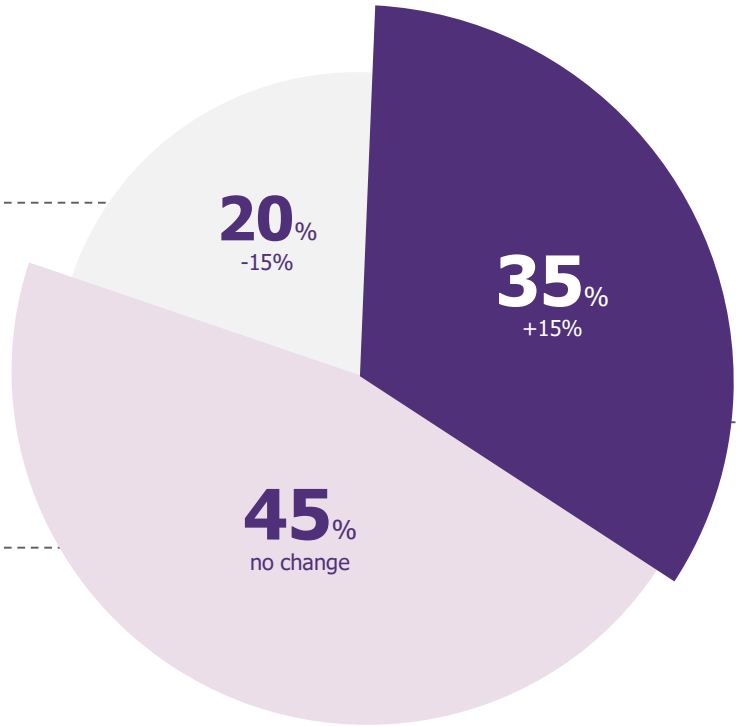
80% of the BEL20 companies have mentioned information security **audits & risk controls** in their 2020 annual reports

5/7 companies who mentioned **broad control plans** (such as dedicated cybercrime response team, Enterprise Risk Management for internal controls) are from the **Finance** and **Information Technology** sectors

6/9 companies who mentioned **cyber risk coverage measures** are from the **finance** and **industry** sectors

No mention

The annual reports do not mention any information on audit and cyber risk coverage measures



Broad control plans

The annual report mentions a specific significant or broad control plan led by the cybersecurity team

Audit and Cyber Risk Coverage Measures

The annual reports mention measures for audits and cyber risk coverage

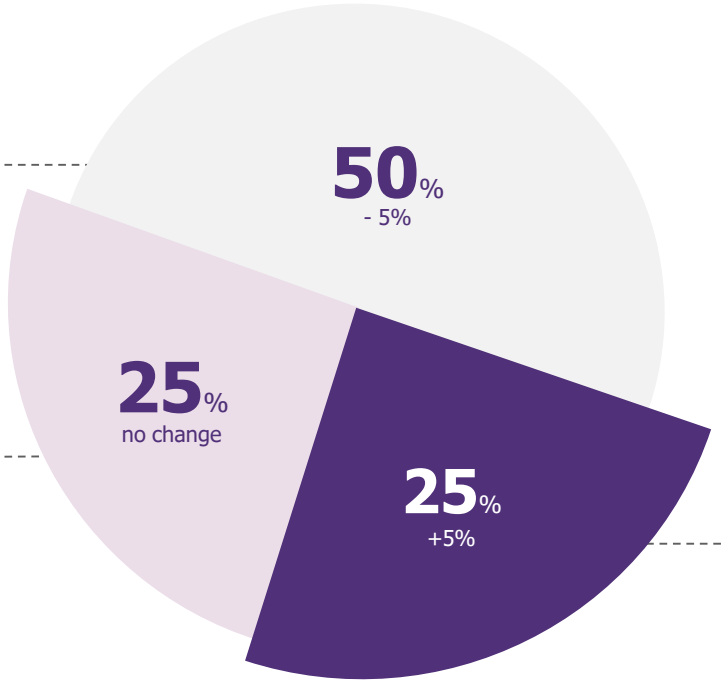
Stagnation of **awareness & training programs** on cyber issues

50% Of the BEL20 companies have mentioned **staff awareness or large-scale awareness & training initiatives** in their 2020 annual reports.

Furthermore, **4/5** companies who mentioned **large-scale awareness and training initiatives** are from the **Finance** and **Information Technology** sectors while none of the companies from the **Consumer Goods & Retail** and **Real Estate** sectors have made any mentions, indicating a disparity between sectors.

No mention

The annual report does not mention any information on security training or awareness programs



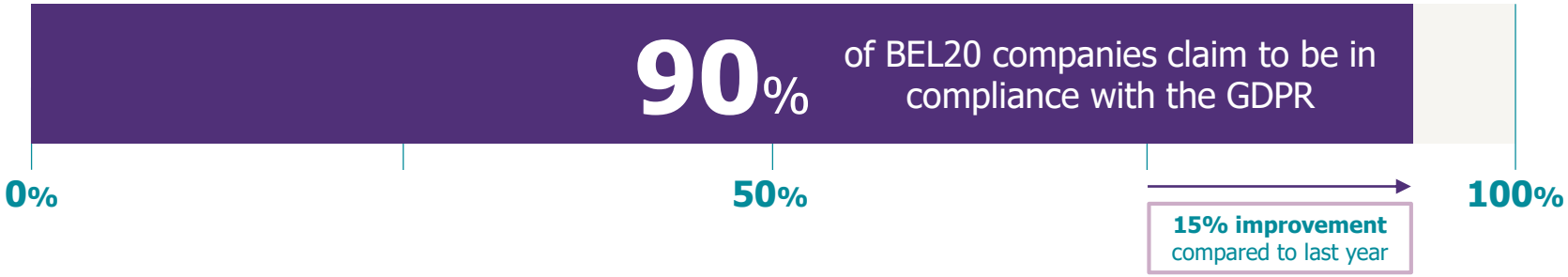
Staff awareness

The annual report mentions staff or executive committee awareness

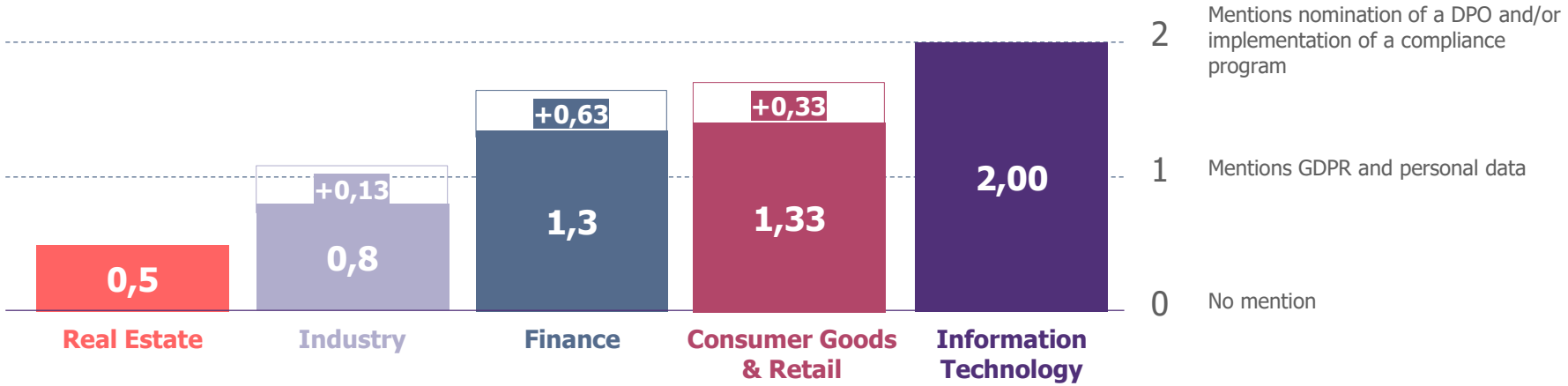
Large-scale awareness and training initiatives

The annual report mentions large scale awareness or training initiatives

Solid continuity on the consideration of **data protection** and **GDPR***



Once again, the **Information Technology** sector stands out in the **cybersecurity maturity index** by declaring **full compliance** with the **GDPR,** only **2** companies did not mention anything about it this year.



NB: Our analysis is based on the content of the reports, which do **not always specify the detailed implemented actions** to reach compliance.

GDPR: General Data Protection Regulation

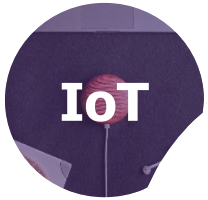
Low mentions of **Cybersecurity** in relation to **Emerging Technologies**

+5%

45% Of BEL20 companies mention launching Artificial Intelligence projects

0% 50% 100%

2 of them link it to **cybersecurity**



-5%

15% Of BEL20 companies mention launching Internet of Things projects

0% 50% 100%

1 of them links it to **cybersecurity**

no change

15% Of BEL20 companies mention launching blockchain-related projects

0% 50% 100%

0 of them link it to **cybersecurity**

10% Of BEL20 companies mention launching blockchain-related projects

0% 50% 100%

1 of them link it to **cybersecurity**

Only **a few companies** (Information Technology and Financial sectors) make the link between **emerging technologies** and **cybersecurity**. This is reinforced by the fact that the annual reports only mention those technologies as cybersecurity enablers but they don't detail the resources and the process behind those innovations.

Highlights observed in the reports

80% OF BEL20 COMPANIES IDENTIFIED CYBER RISKS AS A MAJOR RISK

16 of the 20 BEL20 companies identified cyber risks as a **major risk** in their annual report.

All companies who have mentioned cyber risks as a major risk have classified them under the umbrella of **operational risks**.

100% OF THE COMPANIES IN THE BEL20 ARE **MOBILIZED ON CYBER SECURITY ISSUES**

This year, **100%** of companies in the **BEL20** are mobilized on **cybersecurity issues.**

It demonstrates that cybersecurity is a topic of ever-increasing importance. Belgium's largest companies are embracing the new challenges our digital world has to offer.

FINANCE AND **IT** TAKE THE LEAD

Companies from both sectors mention more cybersecurity-related topics in their annual reports than the other sectors in the study.

Meanwhile, **Real Estate** and **Consumer Goods & Retail**, are globally the ones who are the most in retreat in this study, very little present on the issue of investment against cyber risks, awareness, data protection or innovation.

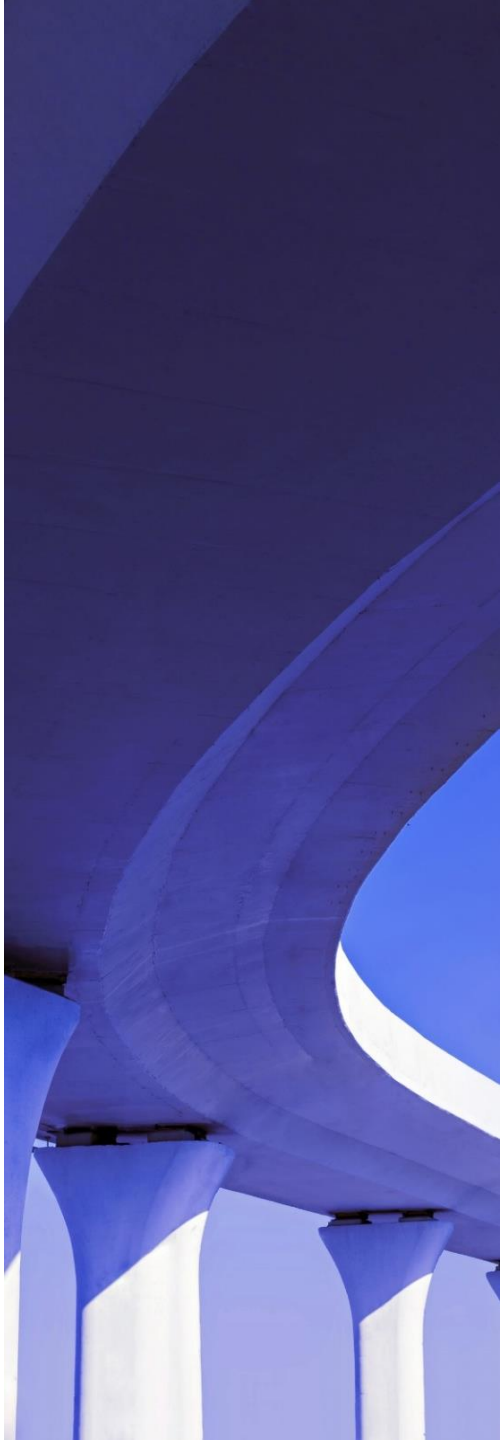
And this year, **2** BEL20 companies declare that they are in compliance with the **NIS directive**

And to conclude

As expected, the **second year** of the **BEL20 cybersecurity maturity index** demonstrates an **increasing level** of **consciousness** regarding cybersecurity issues. Indeed, this is the first year where **100% of BEL20 companies** are mobilized.

Nevertheless, while the general trend indicates that companies are taking heed of cybersecurity issues, some aspects of this mobilization displayed **stagnation** or even a **decline**.

Indeed, **awareness and training** on **cyber issues,** as well as the link to emerging technologies, has been stagnating this year. A trend to be observed in the coming years.



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