



# How mature are annual reports of the BEL20 regarding cybersecurity?

June 2019



**Noémie HONORE**

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



**Marc VAN OENE**

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



In a world where permanent evolution is the key to success, Wavestone's mission is to enlighten and partner with business leaders in their most critical decisions.



Tier one clients  
leaders in their industry



3,000 professionals  
across 8 countries



Among the leading independent  
consultancies in Europe

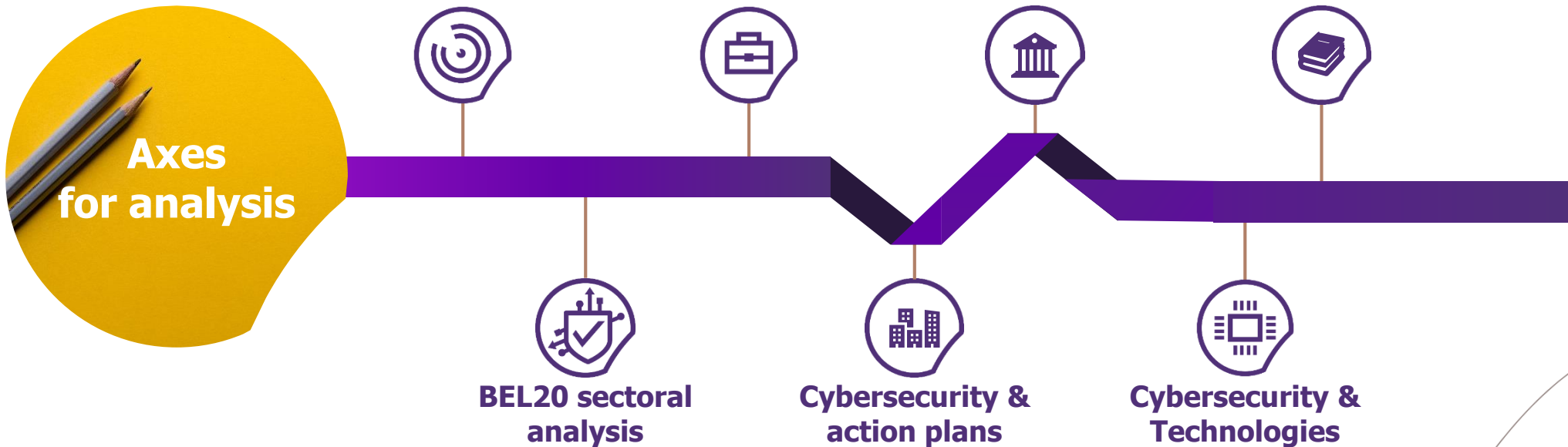
Paris | London | New York | Hong Kong | Singapore\* | Dubai\* | São Paulo\*  
Luxembourg | Madrid\* | Milano\* | Brussels | Geneva | Casablanca | Istanbul\* | Edinburgh  
Lyon | Marseille | Nantes

# How **mature** is the **BEL20** in cybersecurity?



**Method:** this study is based upon a factual analysis of the most recent annual reports and reference documents, published by the BEL20 companies on **01/06/2019**.

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.



# Wavestone cybersecurity: 2018 annual reports maturity index

The **Wavestone cybersecurity 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

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



95%

of the BEL20 are **mobilized** on **cyber issues**



Nevertheless, there is a great **diversity** in terms of cybersecurity **investments** and **awareness** amongst the **BEL20** actors

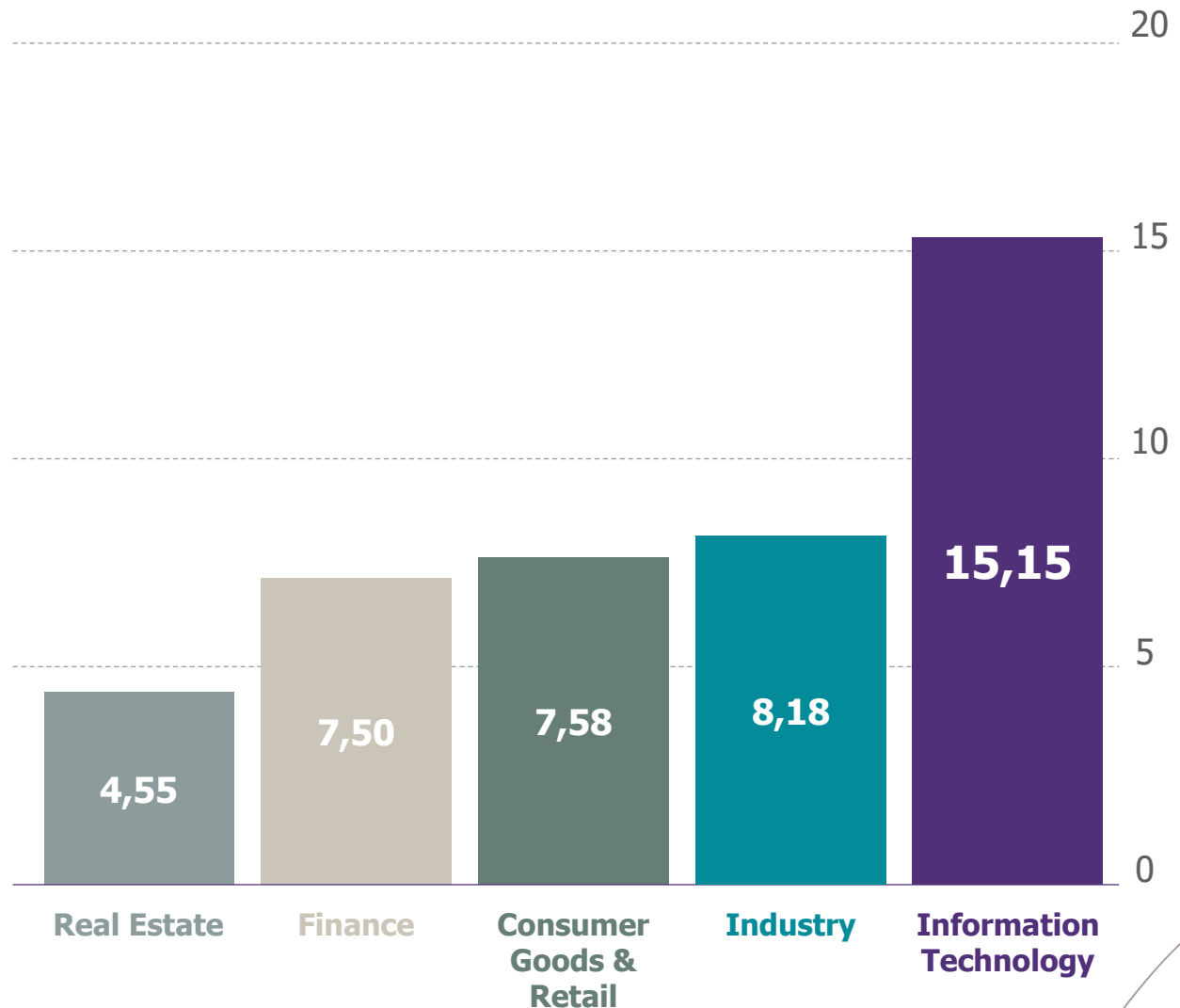
# Sectoral analysis of the BEL20 cybersecurity maturity index

When we look at the average score by sectors, **Information Technology** arrives - by far - in **the first position**.

**Industry**, **Consumer Goods & Retail**, & **Finance** have a fairly **close average** but the rating remains well below the Information Technology sector.

**Real Estate** arrives on the last position of the ranking with a score **under 5/20**.

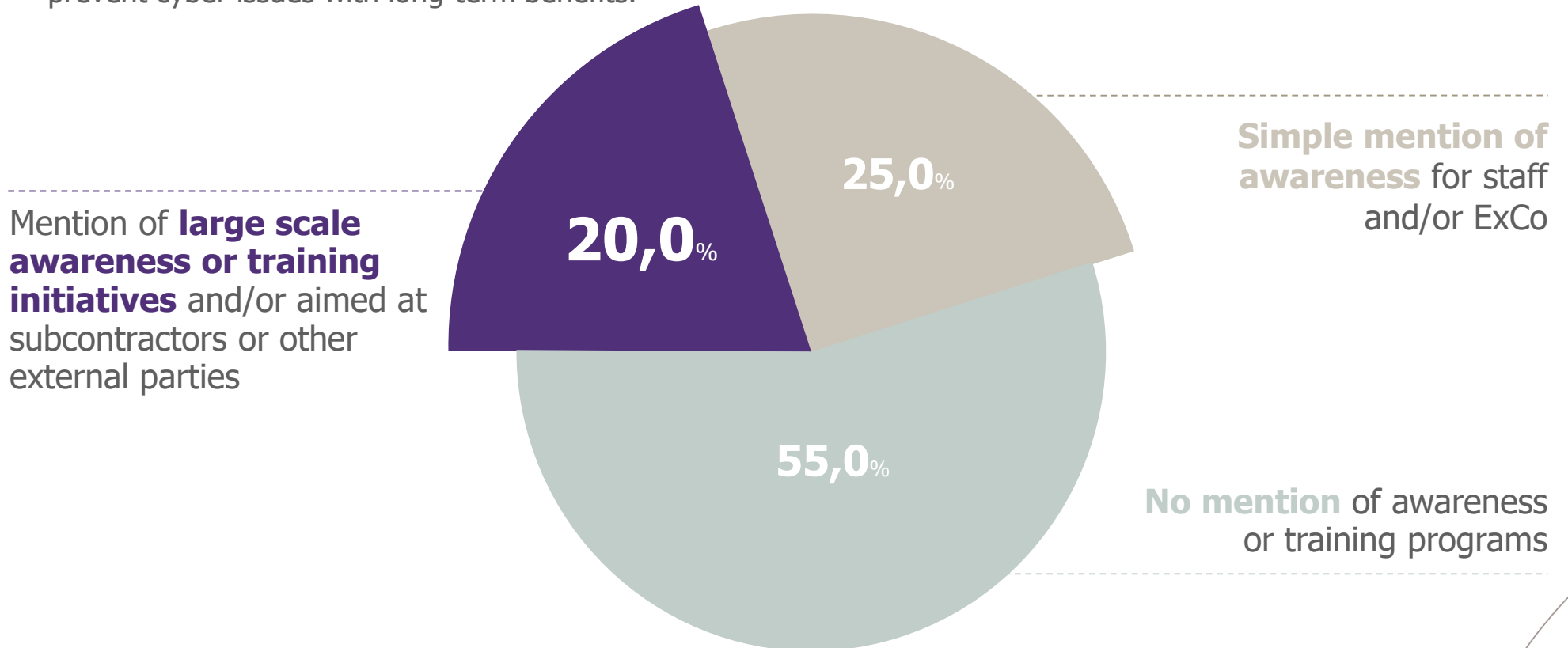
In order to **increase their score**, BEL20 actors could be more explicit about the measures taken in terms of cybersecurity. In particular on aspects related to **cyber regulations** (e.g. NIS), **cyber standards** compliance such as ISO 27001 and **cyber insurance policy**.



# Awareness & Training

**45%** of BEL20 actors mention the presence of awareness and training programs on cyber issues. A **first move** is done but it still remains insufficient when we know that the majority of cyber attacks starts with phishing or social engineering more globally.

**20%** of companies mention **detailed programs** of wide scope. This **encouraging figure** reflects a **real understanding** of **awareness campaigns' benefits**. They should be considered as a **fundamental work** to prevent cyber issues with long-term benefits.



# Cybersecurity & action plans

**70%**

Of the BEL20 actors mention **cybersecurity action plans** in their annual reports

The results show that most of **BEL20 actors** understand the **need to be prepared and react quickly** when cybersecurity incidents happen.

The **most advanced** companies deployed dedicated **cybersecurity teams, continuity action plans, crisis event management, and security incident & event monitoring tools** to reduce the risks and impacts of cyber incidents.

## Detailed cybersecurity action plans

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

**15,0%**

## No mention

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

This point will **carefully be analyzed** on **the next year cybersecurity maturity index**.

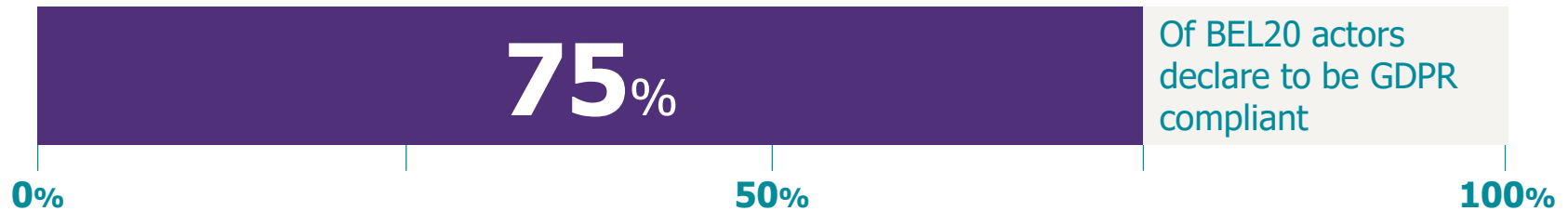
**30,0%**

**55,0%**

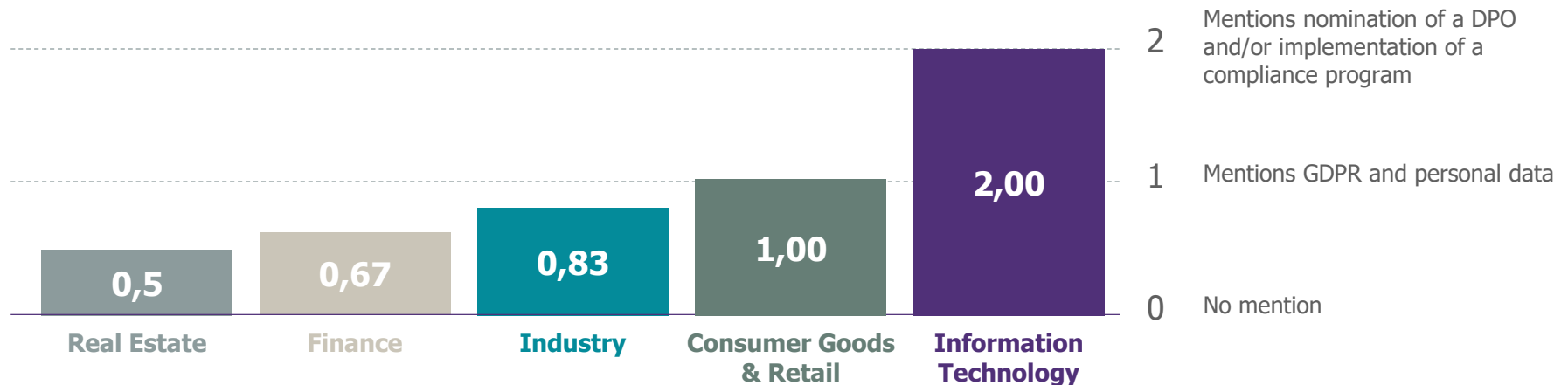
## Standalone action plans

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

# GDPR\* & Privacy



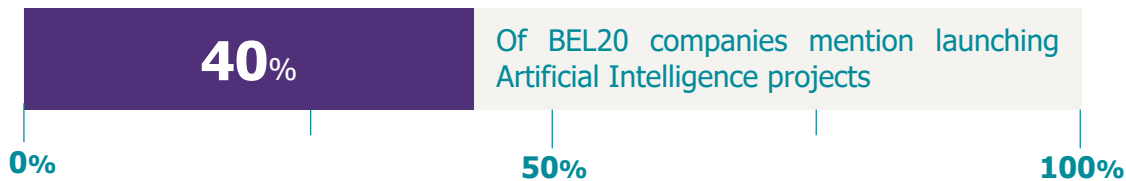
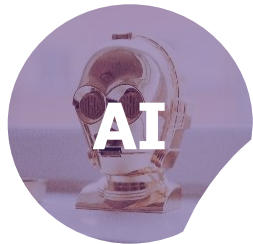
Once again **Information Technology** sector stands out in the **cybersecurity maturity index** by declaring being **fully compliant** with the **GDPR**



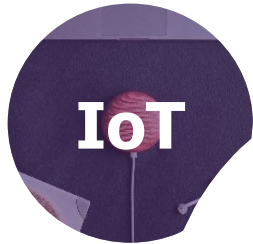
NB: Our analysis is based on the content of the reports, which do **not always specify the detailed implemented actions** to reach compliance.



# Cybersecurity & Technologies



**5** of them link it to **cybersecurity**












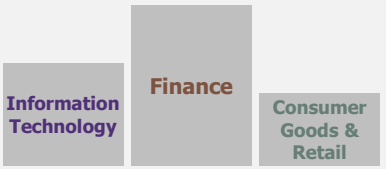

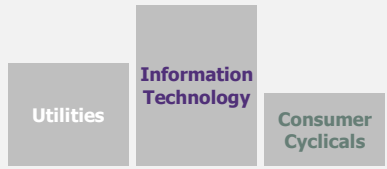
**1** of them links it to **cybersecurity**



**0** of them link it to **cybersecurity**

Only **a few actors** make the link between **new technologies** and **cybersecurity**. This is enforced 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.

# A comparative view of BEL20's cybersecurity maturity with its peers

	 	 	 	 
<b>Global score</b>	<b>8,57/20</b>	<b>10,15/20</b>	<b>10,07/20</b>	<b>9,09/20</b>
<b>Leading sectors</b>				
<b>Awareness &amp; Training</b>	<b>45%</b> of BEL20 is mobilized on the topic	<b>30%</b> of DJIA is mobilized on the topic	<b>60%</b> of CAC40 is mobilized on the topic	<b>60%</b> of FTSE100 is mobilized on the topic
<b>Cybersecurity &amp; action plans</b>	<b>70%</b> of BEL20 is mobilized on the topic	<b>90%</b> of DJIA is mobilized on the topic	<b>80%</b> of CAC40 is mobilized on the topic	<b>91%</b> of FTSE100 is mobilized on the topic
<b>GDPR &amp; Privacy</b>	<b>75%</b> of BEL20 is mobilized on the topic	<b>87%</b> of DJIA is mobilized on the topic	<b>100%</b> of CAC40 is mobilized on the topic	<b>71%</b> of FTSE100 is mobilized on the topic

# Highlights observed in the reports

## INVOLVEMENT OF EXECUTIVE COMMITTEES AND GOVERNANCE

**12** out of the **20** actors of the BEL20 have integrated cybersecurity issues into their **governance** and **6** companies have an **Executive Committee member** directly involved and responsible for **information security topics**.

This reinforces the idea that the **changes** in cybersecurity are **not superficial** but show a real willingness to **transform the business in depth**.

## A REAL WAKE-UP CALL ON CYBERSECURITY ISSUES

Out of the **95%** of BEL20 actors mobilized on cybersecurity issues, **50%** of them give **detailed explanations** of the issues, and the **risks and impacts** they could have on their business.

It shows that **cybersecurity** is not a secondary subject anymore. It's a **strong signal** that **Belgian largest companies** start to embrace the **new challenges** our **digital** world has to offer.

## RESPECT OF CYBERSECURITY STANDARDS AND CERTIFICATIONS

Out of 20 companies, **only 3** mention a **cybersecurity standard certification** (i.e. ISO 27001)

With the arrival of the **NIS** directive **based** on the **ISO 27001 for Belgian companies**, the road ahead seems still long.

# And to conclude



This **first year** of **BEL20 cybersecurity maturity index** shows an **encouraging level of consciousness** regarding cybersecurity issues



... but could be better if companies **highlight all their actions in the annual reports**



We are **optimist** that **100%** of the BEL20 will be **mobilized on cybersecurity** issues for the **next year**. But we stay focused on the task as we know the **cyber-journey** has **only started**

# 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

**Noémie HONORE**  
Manager

**M** +32 (0)484 67 84 29  
noemie.honore@wavestone.com

**Marc VAN OENE**  
Consultant

**M** +32 (0)4 84 67 78 38  
marc.van-oene@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