WAVESTONE

How mature are annual reports of the Dow 30 regarding Cybersecurity?

June 2019

Erwan LE LAN
Partner IT & Digital Transformation
erwan.lelan@wavestone.com
+1 347 880 2689

Baptistin BUCHET
Head of Cybersecurity & Digital Trust (AMER Region)
baptistin.buchet@wavestone.com
+1 (917) 346-3658

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,
n°1 in France

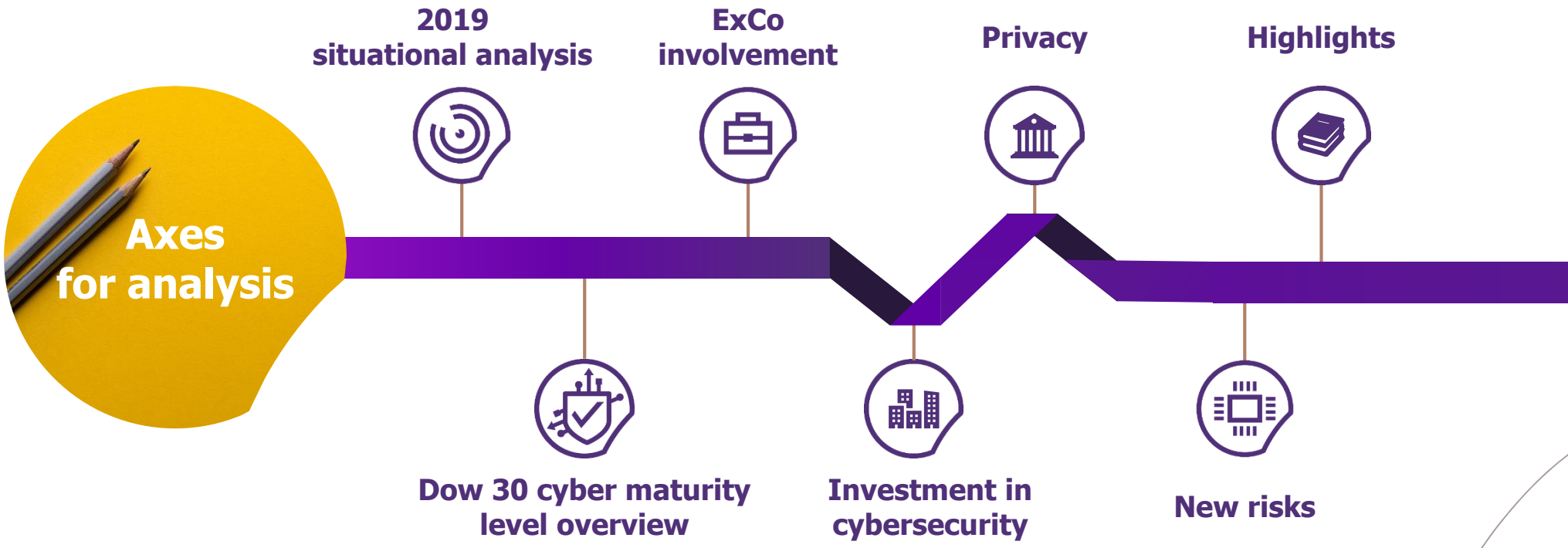
Paris | London | New York | Hong Kong | Singapore* | Dubai* | São Paulo*
Luxembourg | Madrid* | Milano* | Brussels | Geneva | Casablanca | Istanbul* | Edinburgh
Lyon | Marseille | Nantes

* Partners

How mature are the Dow 30 companies in cybersecurity?

Method: This study is based on a factual analysis of the most recent annual reports and proxy statements, published by the Dow 30 companies by 01/06/2019.

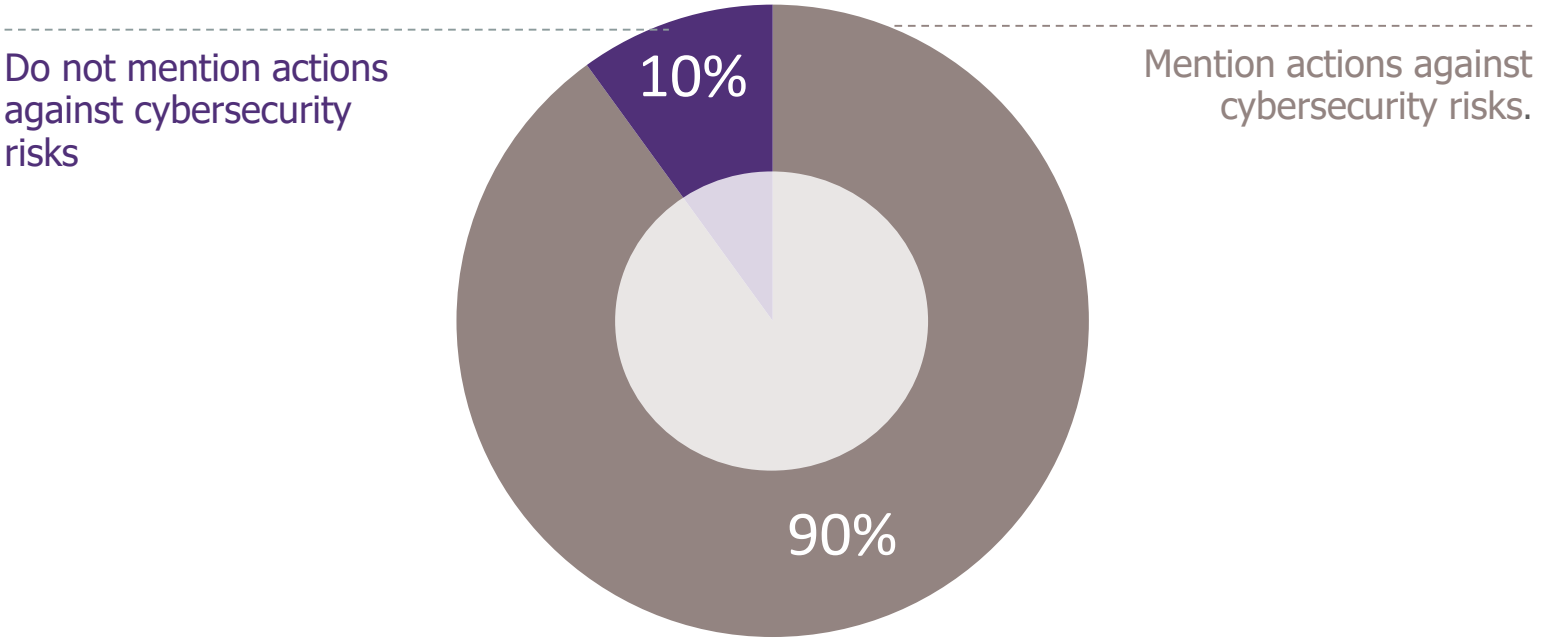
This analysis is based solely on the elements in these documents. It should be noted that it might not always reflect entirely the actions taken in the field.



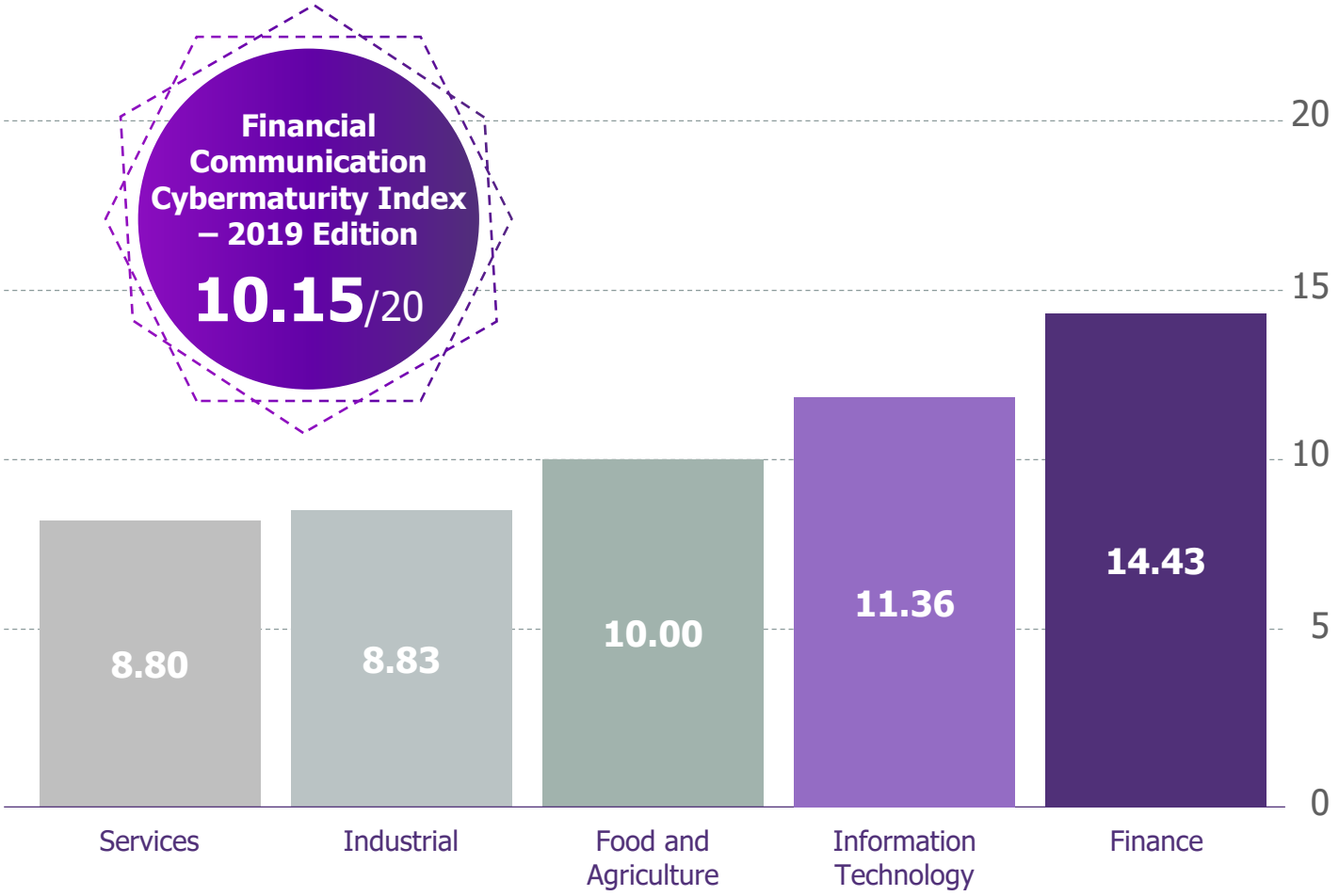
All the Dow 30 companies are aware of cybersecurity risks

100% of Dow 30 companies are aware of cybersecurity risks

90% of them take measures to control such risks



The finance sector stands out, followed by the IT companies



Wavestone cybersecurity: 2019 maturity index

The *Wavestone cybersecurity: 2019 annual maturity index* provides an assessment of companies' maturity levels, based upon the content of their 2018 annual reports and proxy statements. 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*

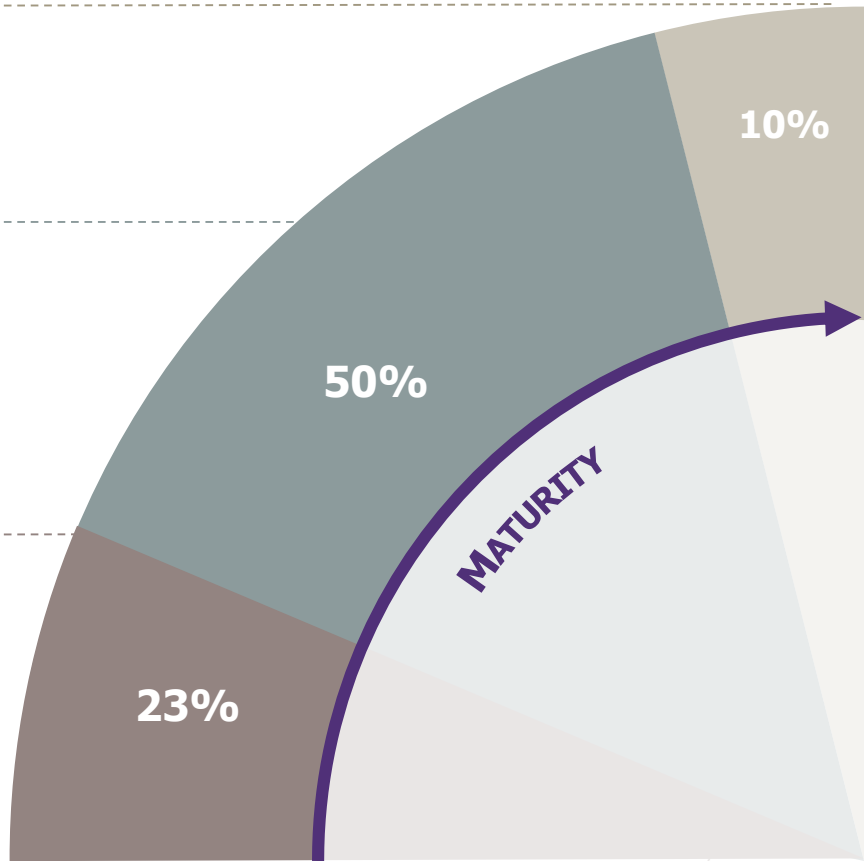
Executive committees are highly involved in cybersecurity governance

83% of Dow 30 groups address issues at executive committee level.

Executive Committees **play an active part**

Executive Committees **are regularly informed**

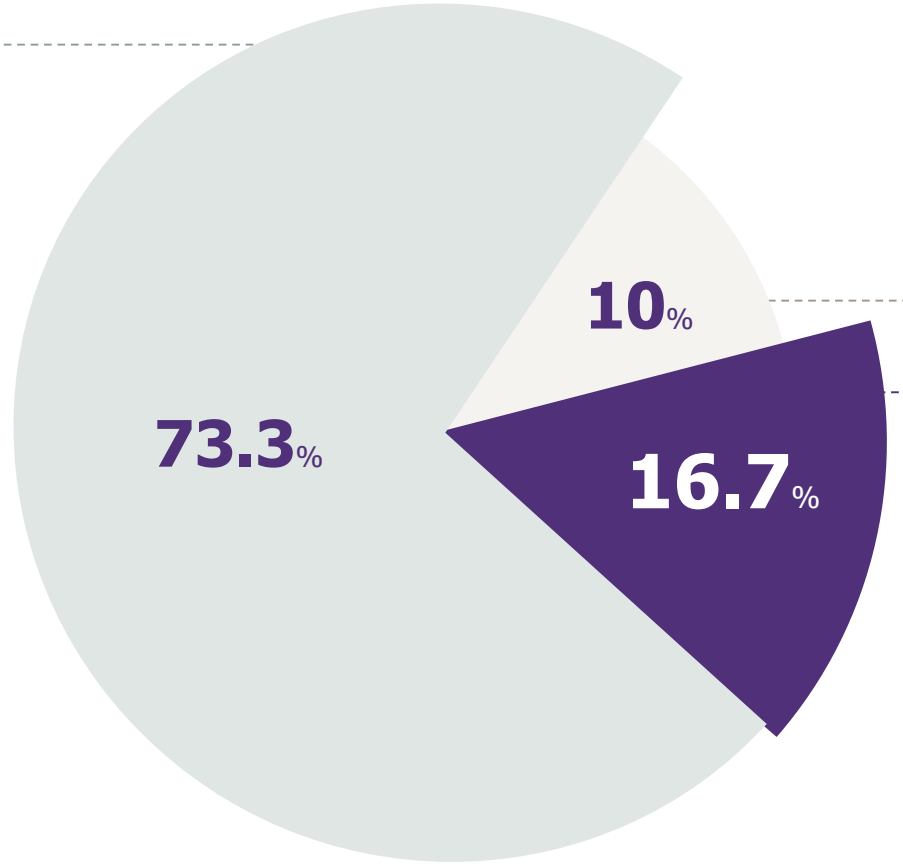
Executive Committees **consider the topic but their specific involvement is unclear**



Companies take actions to manage cyber risks, but not in a structured manner

Standalone initiatives

The reports mention actions against cybersecurity risks and deployment of security measures.



No mention

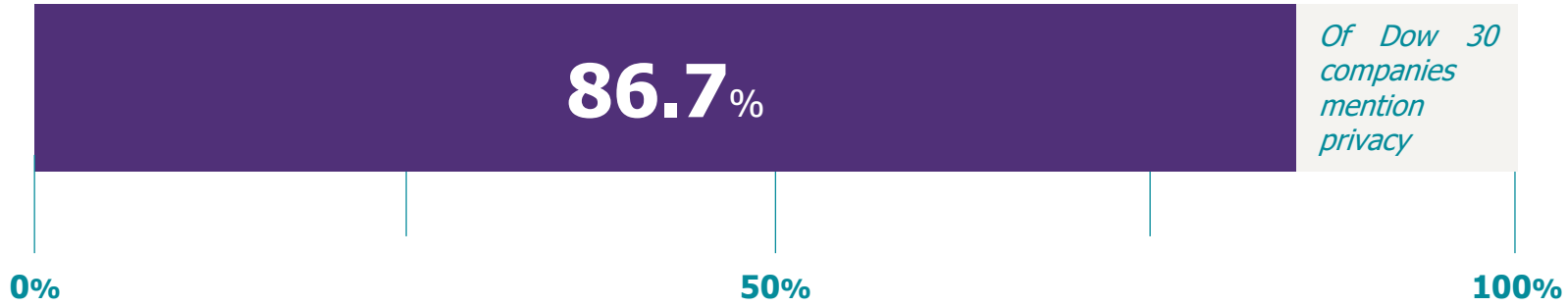
The reports contain no mention of actions aimed to address cybersecurity risks.

Cybersecurity programs

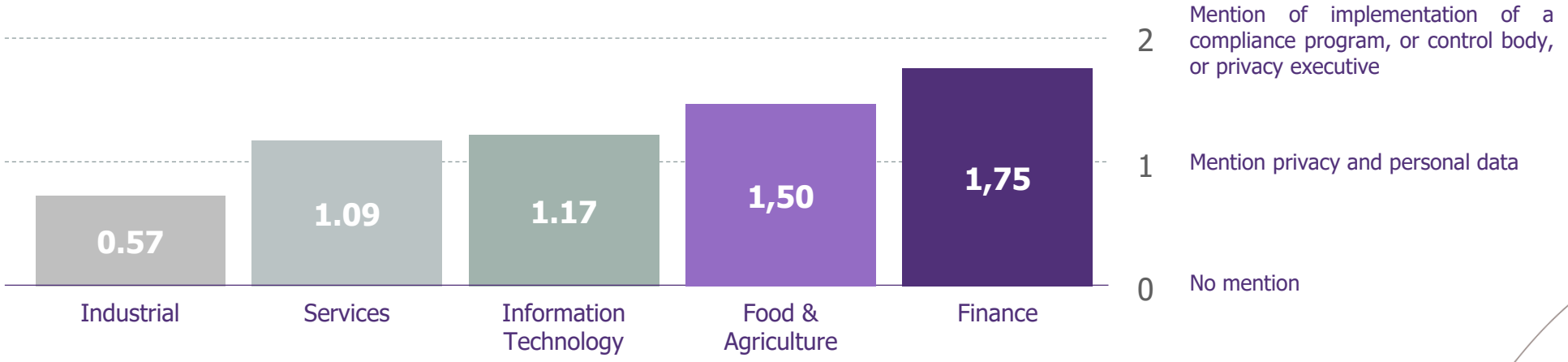
The reports delineate security programs with a structured governance and significant investments.

Only one company of the Dow 30 mentioned the amount of their investment but Wavestone estimates that Dow 30 companies spend on average $250 million on cybersecurity programs.

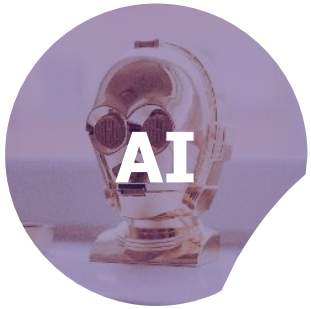
Amidst the rise of privacy regulations, companies are highly concerned about personal data protection



The finance sector once again leads Dow 30 privacy maturity level.



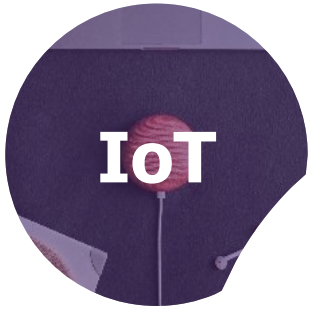
Cybersecurity issues are not prioritized in the development of emerging technologies



40% *Of Dow 30 companies mention launching Artificial Intelligence projects*

0% 50% 100%

2 companies link them to cybersecurity



23% *Of Dow 30 companies mention launching Internet of Things projects*

0% 50% 100%

0 company links them to cybersecurity

20% *Of Dow 30 companies mention launching blockchain-related projects*

0% 50% 100%

0 company links them to cybersecurity

Other highlights observed in the reports

BUSINESS RISKS INTEGRATE CYBERSECURITY

The digitalization of the economy reflects in cyber risks with specific business risks that are mentioned more and more often:

- Industry 4.0;
- Privacy;
- Fraud in financial services;
- Interruption of services

EXTERNAL AND INTERNAL COMMUNICATIONS ON CYBERSECURITY ARE STILL DIFFICULT FOR COMPANIES

Due to concerns about negative publicity, transparency around cyberattacks is still limited. Only 2 companies referred to specific incidents in their annual reports, while 8 others mentioned cyberattacks without disclosing any details.

Because of the significant investments required, internal communication is another area of improvement, with only 30% of the companies mentioning training programs that promote cybersecurity awareness.

COMPANIES STILL STRUGGLE TO STANDARDIZE CYBERSECURITY

Only 4 Dow 30 companies, mostly in the finance sector, mention international standards or certification, with 2 following the FFIEC and 1 mentioning the NIST, which are frameworks help companies to assess their cybersecurity readiness.

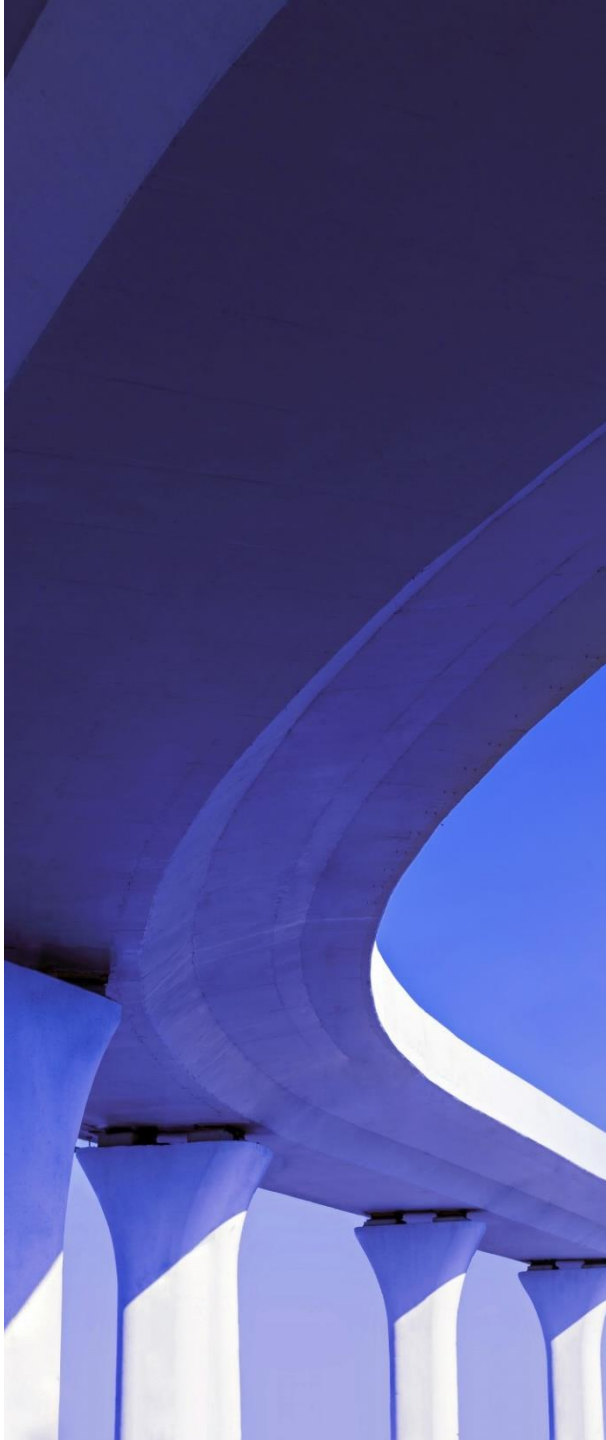
And to conclude

All Dow 30 companies are well aware of cybersecurity risks by mentioning them in their annual reports…

… and the majority prioritize them properly by considering their impact on business activity and involving executive committees on the topic …

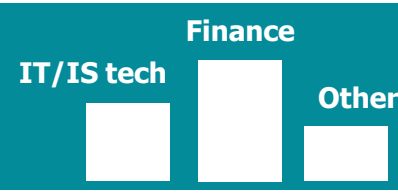
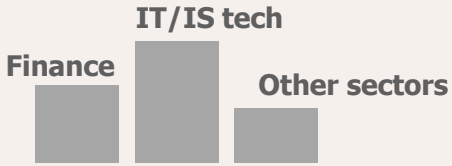
…but there are still more to do:

1. Leverage on market standards
2. Structure initiatives through programs
3. Anticipate risks of emerging technologies



International comparison

How do Dow 30 companies compare to their EU peers?

	Dow 30	CAC 40, BEL 20 & FTSE 100
Awareness of risk and impact	**100%** elaborate on cybersecurity risks and impacts	**87%** mention cybersecurity risks and impacts
Leading sectors		
Security-minded innovations	**7%** consider cybersecurity in the design of their new technologies	**26%** consider cybersecurity in the design of their new technologies
Training & awareness	**30%** mention training programs on cyber risk awareness	**58%** mention training programs on cyber risks awareness
Cyber Risk Audit	**87%** mention audit on cyber topics	**60%** mention audit on cyber 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 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)

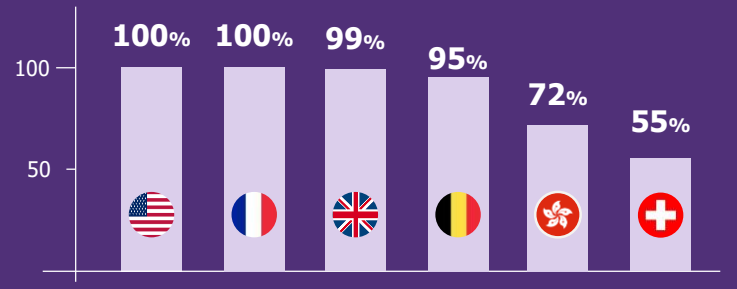
	Weighting	Level 0	Level 1	Level 2
Security of business-specific systems (Industrial control systems, anti-fraud mechanisms, payment systems, etc.)	1	0 points No mention	+1 point Mention of business-specific risks	+2 points Mention of a significant programme and investments
Privacy: GDPR, Privacy, personal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

International analysis

A great involvment at a global scale

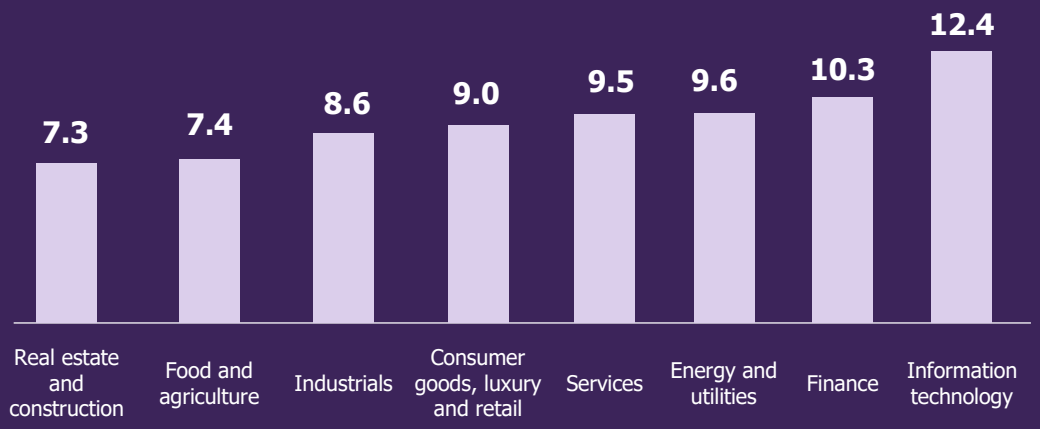
The following figures are based upon a factual analysis of the most recent financial communication, published by companies by June 1st, 2019 listed in the stock market indices where Wavestone has a point of presence: Dow Jones, CAC 40, FTSE 100, BEL20, SMI, HSI, i.e. representing a panel of 260 companies

90% **of companies act on cybersecurity**



Zoom on the leading countries

The following figures focus on the 190 companies listed in the four leading stock market indices



2019 Global Cybermaturity Index

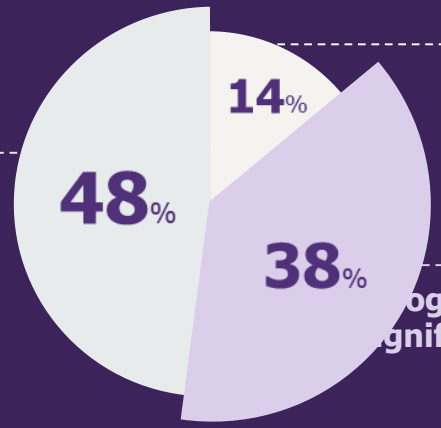
/20

The information technology sector leads the way, ahead of the financial sector

Zoom on the leading countries

61% address cybersecurity at Executive Committee level

Cybersecurity investments are fragmented overall



No mention

Standalone action plans

ogrammes involving
gnificant investments

The subject matter of the year: PRIVACY

80%

mention GDPR, privacy or personal data protection

Zoom on the leading countries

How to build a safer future? Companies are developing innovative technologies, yet cybersecurity is hardly part of the discussion, as it should be

66 mention it,
4 consider cybersecurity

38 mention it,
3 consider cybersecurity

22 mention it,
2 consider cybersecurity

17 mention it,
2 consider cybersecurity

What are leading companies doing?

- **Cyber insurance**
- **Supply chain security**
- **Cyber resilience**
- **Merger and acquisition security**

WAVESTONE

Erwan LE LAN
Partner IT & Digital Transformation

M +1 347 880 2689
erwan.lelan@wavestone.com

Baptistin BUCHET
Head of Cybersecurity & Digital Trust (AMER Region)

M +1 (917) 346-3658
baptistin.buchet@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