



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

July 2020



Florian DROUIN
florian.drouin@wavestone.com
+1 646 407 0521



Joy HAN
joy.han@wavestone.com
+1 646 617 0443



Shweta RAI
shweta.rai@wavestone.com
+1 913 406 9228

Wavestone in a nutshell



Pure player
in consulting
since 1990

12 offices
in 8 countries

3 000+
employees

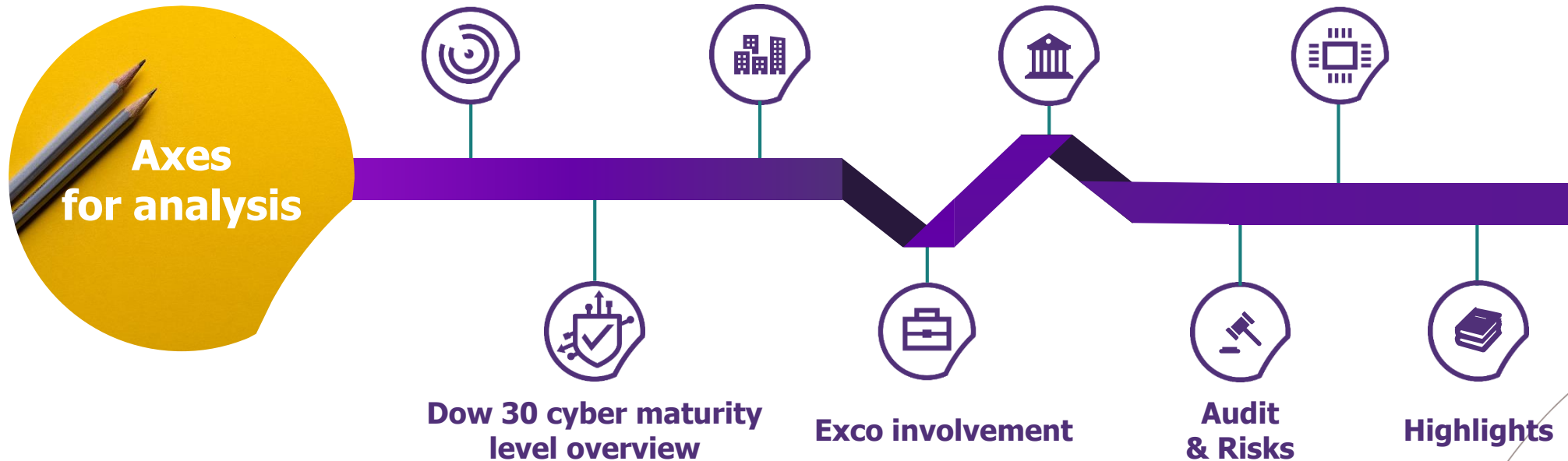
€392m
2018/19 revenue

How mature are the Dow 30 companies in cybersecurity?

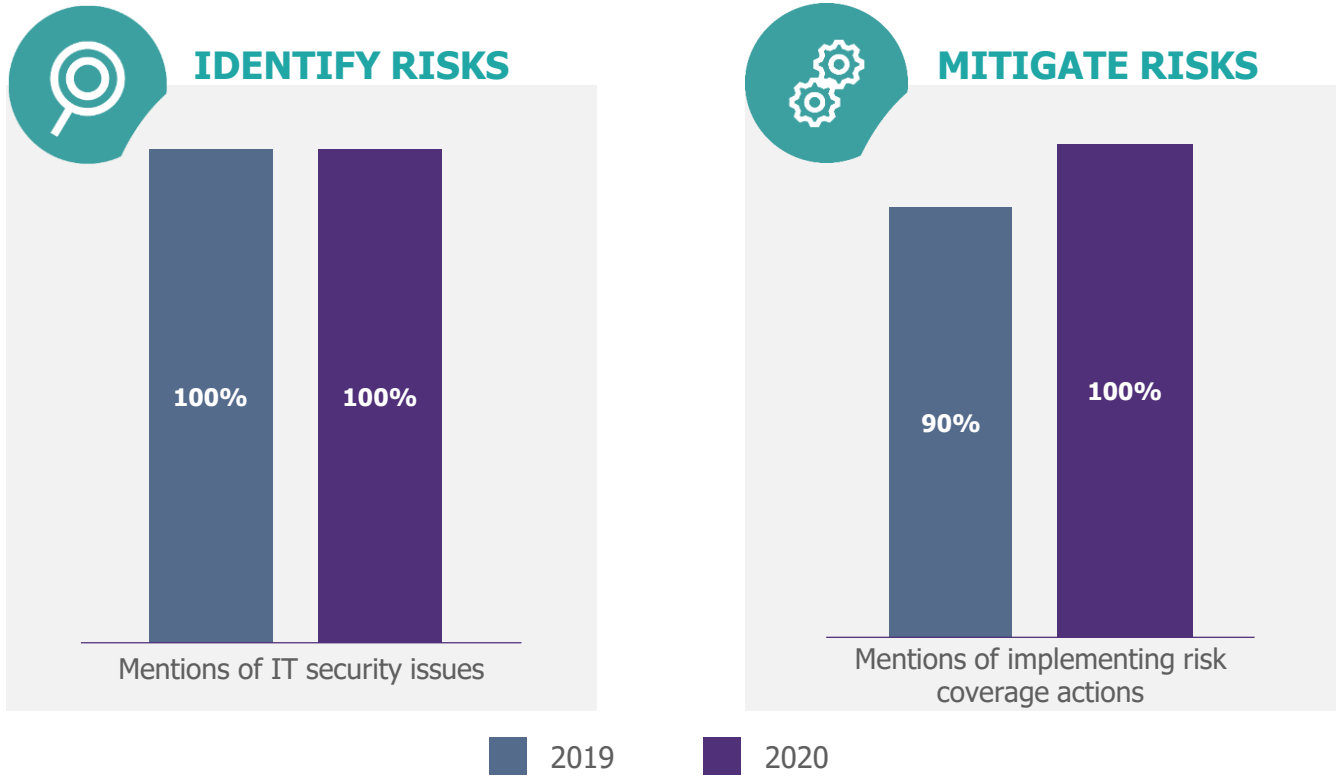


Method: This study is based on a factual analysis of the most recent annual reports and proxy statements, published by the Dow 30 companies up to 06/01/2020.

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.



100% of the Dow 30 companies now take actions to mitigate cybersecurity risks

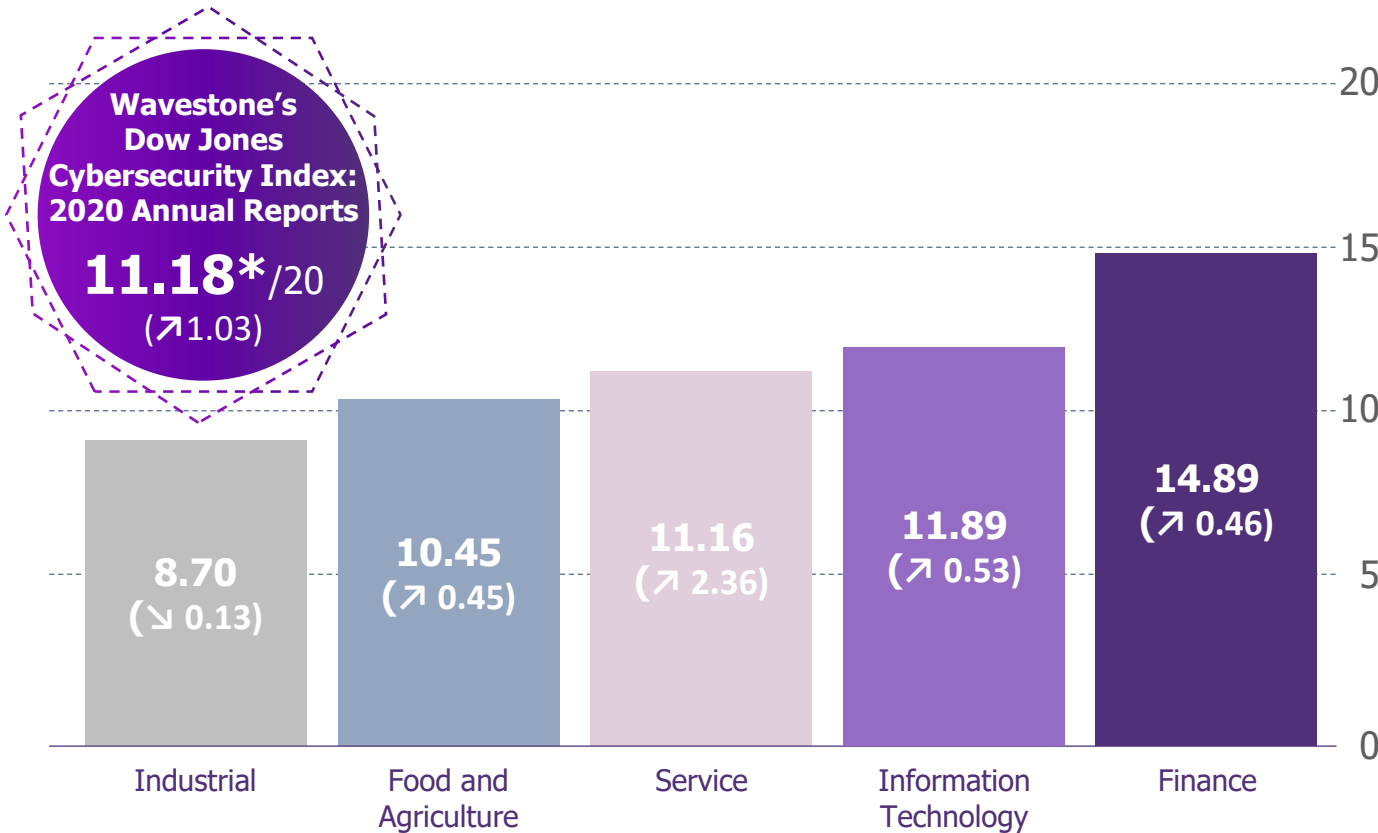


All the Dow 30 companies this year made at least some mention of cybersecurity related considerations or actions in their annual reports. This is up 10% from the 2019 analysis, showing a significant increase in cybersecurity awareness.

The service sector stands out, while others continue to grow at a steady pace

Wavestone identified increases in the score for the majority of sectors except Industrial. Especially, the Service sector jumped by approximately two points this year due to **heavy investments in cybersecurity programs, information security training & awareness and privacy compliance.**

Industrial Sector now falter behind the pack due to a lack of awareness and investment.



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 2019 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

Information security 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.

*Mean average across all companies in all sectors

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

Almost half of the Dow 30 companies are industrializing their cybersecurity strategy

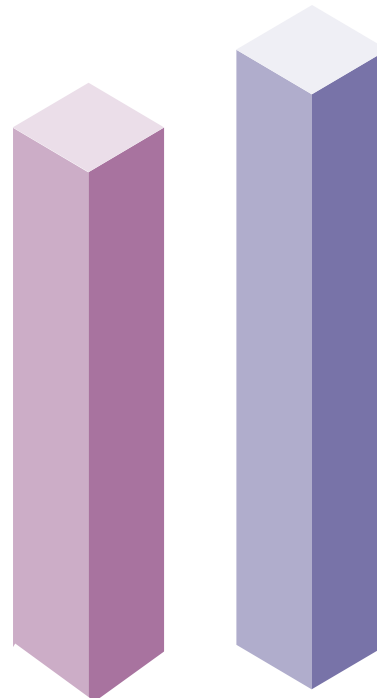
43%

Cybersecurity programs (Systematic Approach)

Security programs involving significant investments and/or comprehensive attack response plans are mentioned.

A **13% increase** this year shows that now close to half of the Dow 30 companies are heavily investing in Cybersecurity.

We are seeing large improvements as **5 companies** went from having standalone action plans to heavily invested cybersecurity programs.



57%

Standalone action plans (Opportunistic Approach)

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

A **10% increase** this year shows that now all Dow 30 companies we analysed have at least outlined a standalone action plan to invest in cybersecurity.

Since last year, the remaining **3 companies** that did not mention of investments aimed to address cybersecurity risks, have invested in standalone action plans.

Executive Committees are placing cybersecurity issues on their agenda

63%

of Dow 30 companies address issues at the executive committee level.

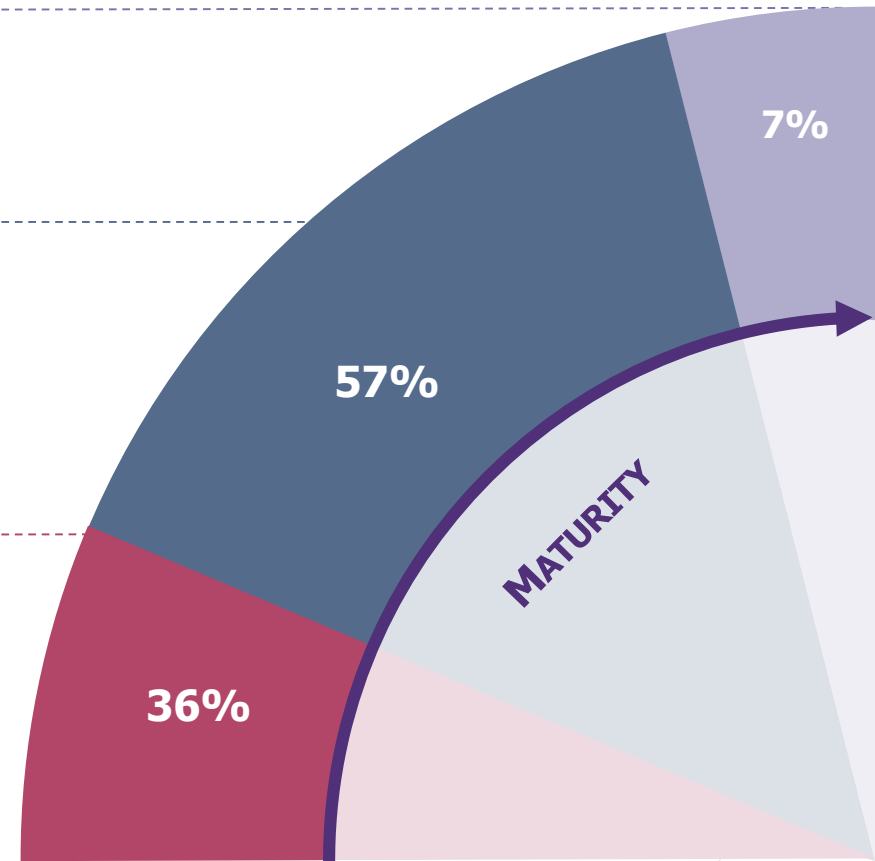
We saw a decrease in the Executive Committees' involvement, which highlights that some companies' ExCos are handing over the cybersecurity reins to different areas of the business, preferring to receive regular updates instead.

Today more than ever, chief information security officers (CISOs) need to maximize cyber impact by reporting their mission and needs, showcasing business acumen, and building C-suite relationships.

Executive Committees **play an active part**

Executive Committees **are regularly informed**

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



Personal Data Protection continues to gain corporate recognition



In compliance with GDPR* and other privacy regulations, last year, 87% of Dow 30 companies showed their maturity in the data protection domain. This year, in order to comply with more US state-level privacy regulations such as CCPA*, New York SHIELD* Act, etc., 93% of Dow 30 companies have shown an improvement in their maturity with the personal data protection. Moving forward, all of Dow 30 companies have to make sure that they have the adequate governance and framework to manage any emerging new privacy regulations in a consistent and efficient way.

37% of Dow 30 companies mention US state-level privacy regulation, compared to 10% last year



*GDPR: General Data Protection Regulation

*CCPA: California Consumer Privacy Act

*SHIELD: Stop Hacks and Improve Electronic Data Security

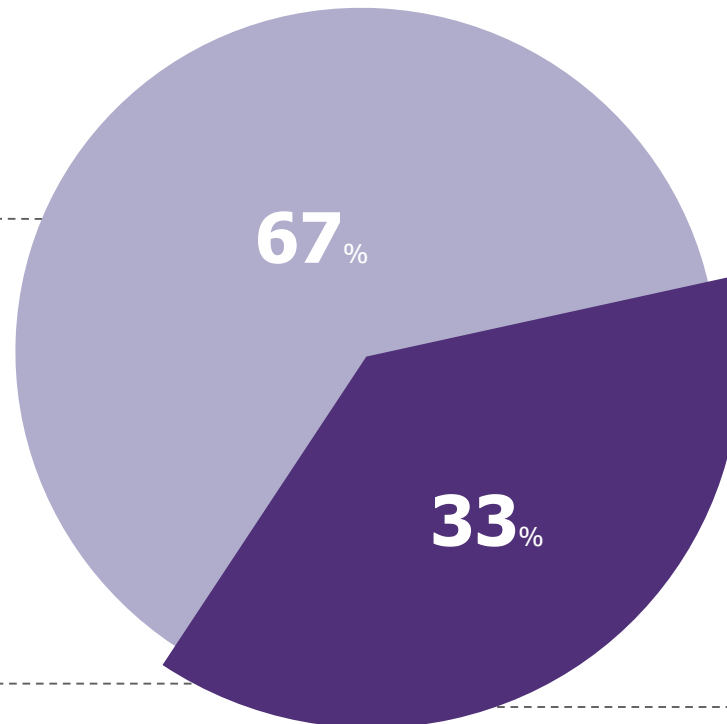
All of Dow 30 companies mention audit and cyber risk coverage for information security

+13%

100%

Of Dow 30 companies mention information security **audits & risk controls**

The rest of Dow 30 companies from **all sectors** only mention audit and cyber risk coverage measures with no details

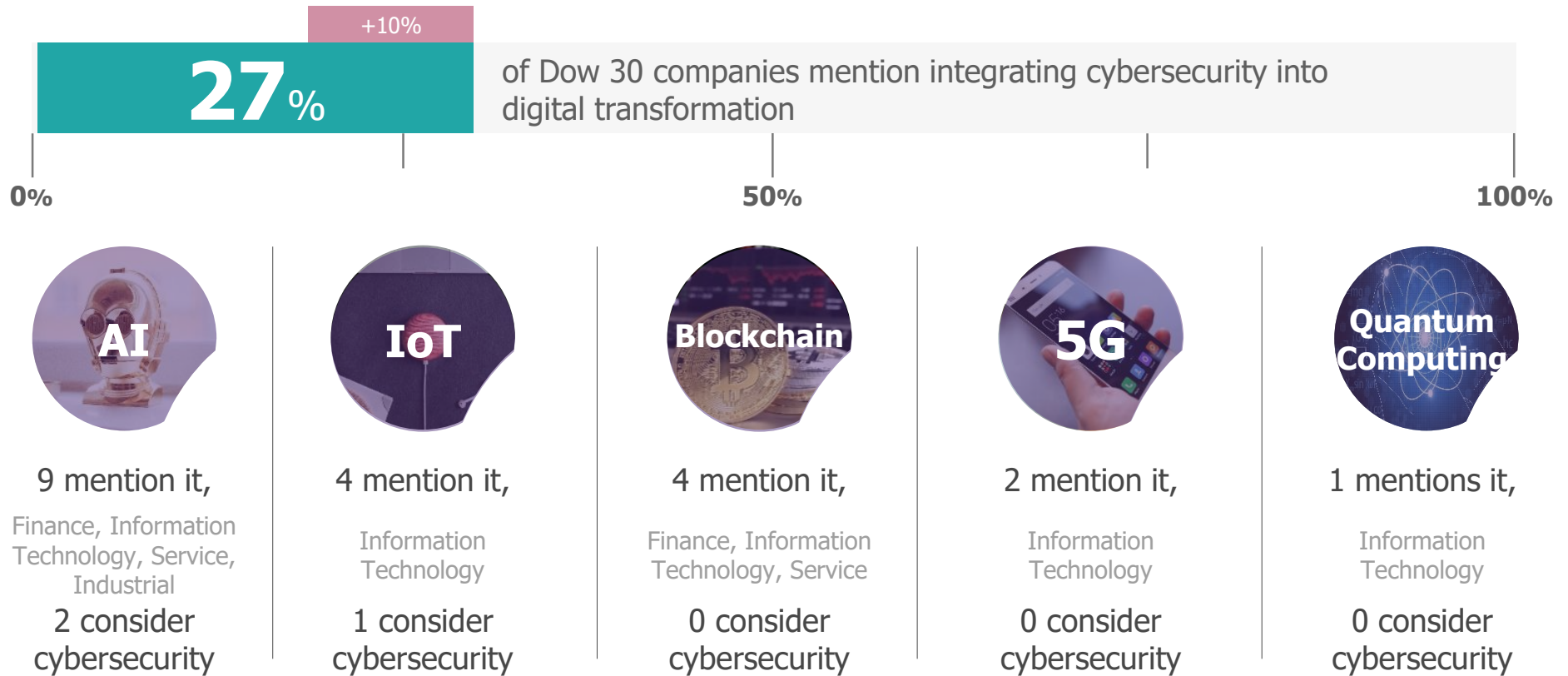


3/10 companies not only mention **broad control plans**, but also propose **specific control plans** (such as Cybersecurity and Technology Control organization, Information Security Program and Operating Model, etc.). They are from the **Finance** and **Information Technology** sectors

7/10 companies who mention **broad control plans** (such as dedicated audit committee and risk committee, etc.) are from the **Information Technology** and **Service** sectors

In order to meet audit & regulatory expectations, **33%** of Dow 30 companies leverage **standard frameworks** such as NIST, FFIEC, etc.

More companies should consider cyber aspects of digital transformation



Overall, **more but still very few** companies mention integrating cybersecurity into digital transformation. When discussing emerging technologies, companies have the tendency to focus on their **key areas of business and success**. For example, the **finance sector** focuses on **AI and Blockchain** to improve their payment systems and financial products. Among all innovative topics, **AI** is the most popular one to be discussed.

Highlights observed in the reports

BUSINESS RISKS ARE NOT FULLY REFLECTED IN CYBERSECURITY STRATEGIES

Companies **continue to consider** the cyber risks related **to their business**

However, still few companies report on **specific security means** they implement to prevent attacks on their **business systems**

100% OF THE COMPANIES TAKE ACTIONS ON CYBER SECURITY ISSUES

This year, **100%** of companies in the **Dow Jones** are taking actions to mitigate **cybersecurity risks**

It demonstrates that cybersecurity is still a topic of ever-increasing importance. As a result, companies are **more and more structuring** their cybersecurity programs with a **systematic approach**

IMPROVEMENTS ON REGULATORY STANDARDIZATION

More companies are **leveraging standard frameworks** such as NIST & FFIEC to standardize their control plans

Unfortunately, **still two thirds** of the Dow 30 companies **do not report on structuring** their audit & control plan

And to conclude



All Dow 30 companies are still well aware of cybersecurity issues and now take actions to mitigate the risks...



... and more and more are structuring their initiatives to efficiently drive their strategies (some of them leveraging recognized standards such as NIST) ...



... but some areas are still to be improved:

1. Restructure programs to better showcase the value & benefits at the Executive level
2. Better anticipate, prepare & report on regulations by having a consistent regulatory framework
3. Better include cyber risks of emerging technologies

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

Study Caveats/Limitations

- / Many constituents of the Dow Jones have differing financial years. Based on that, they release their respective annual reports at different times. As a result, observations for some of the companies analysed may be up to a year out of date.
- / This study cannot guarantee to present any given company's cyber maturity as it exists in reality. This is because scores are based only on the information that companies wish to disclose.












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

