Cyber Benchmark

Market maturity and cybersecurity trends

June 2024

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com
(+33) 6 10 99 00 60

Clément JOLLIET
Manager
clement.jolliet@wavestone.com
(+33) 6 46 14 80 12

WAVESTONE

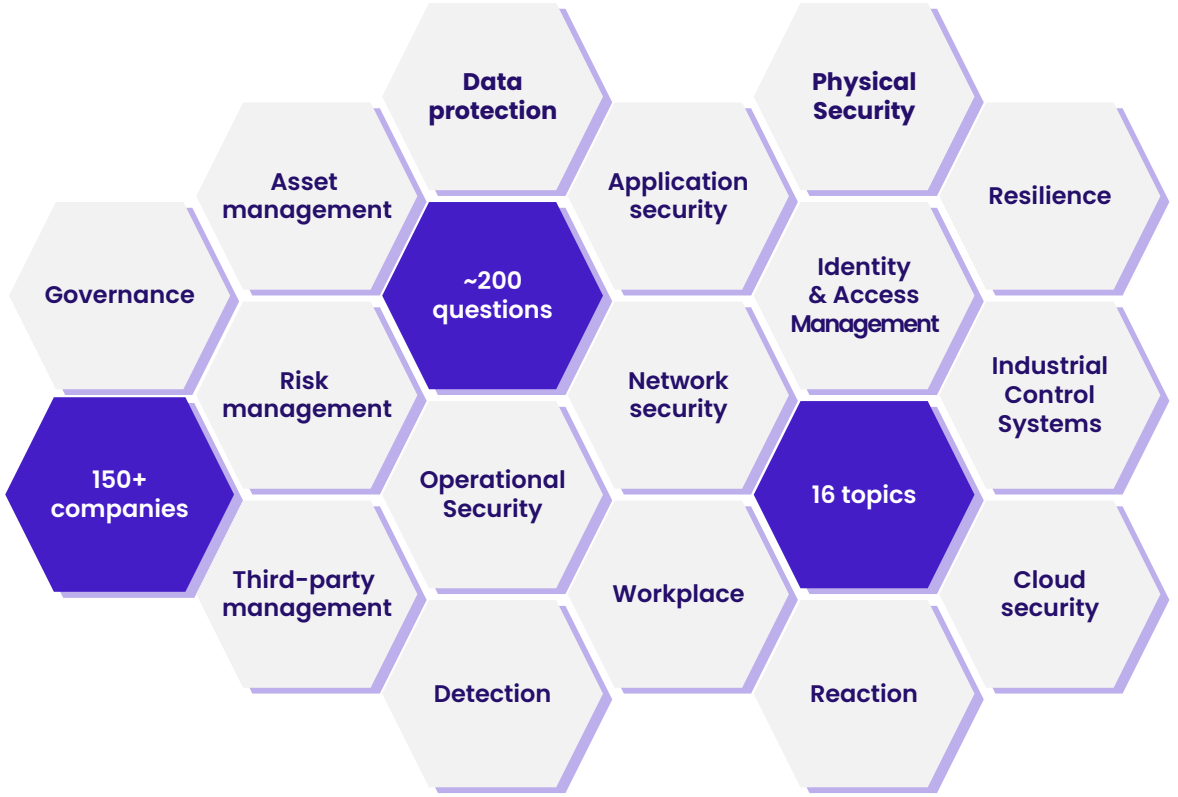
W-CyberBenchmark: A result-driven methodology for an in-depth analysis of the level of cybersecurity maturity

Based on NIST Cybersecurity framework and ISO 27001/2, the **W-CyberBenchmark,** our **360° assessment approach, goes further** and provides:

A comprehensive approach with an **organizational** and a **technology** maturity **assessment**

An assessment that takes into account the **complexity of organizations** that have different entities with different maturity levels

A benchmark vision: **150+ Wavestone customers** have already completed the assessment over the past years, presenting more than 7 millions employees .



How mature are large organizations?

Large organizations*

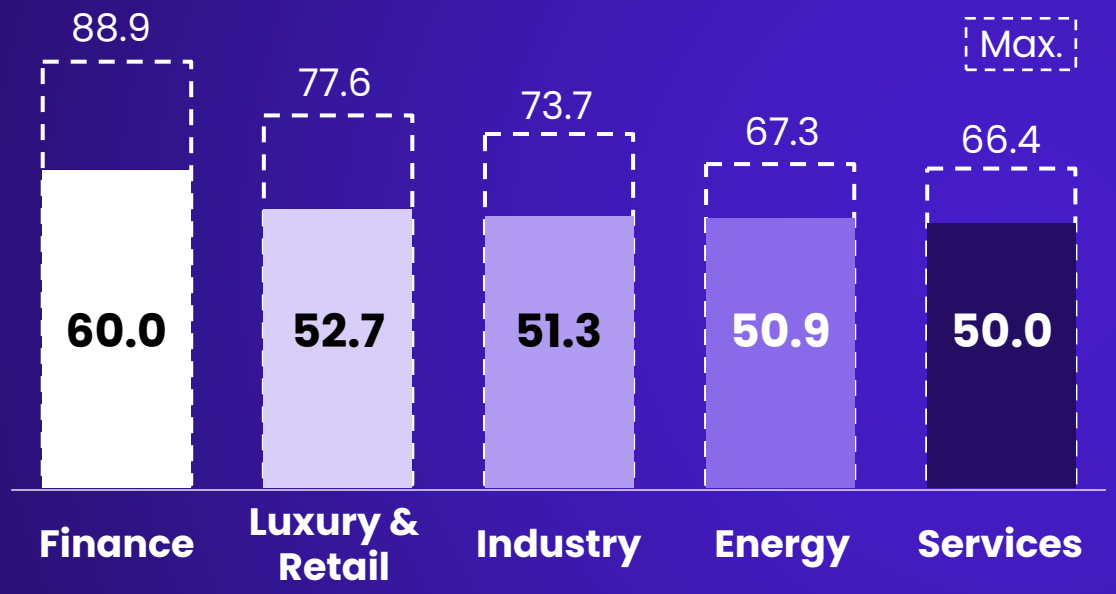
53

/100

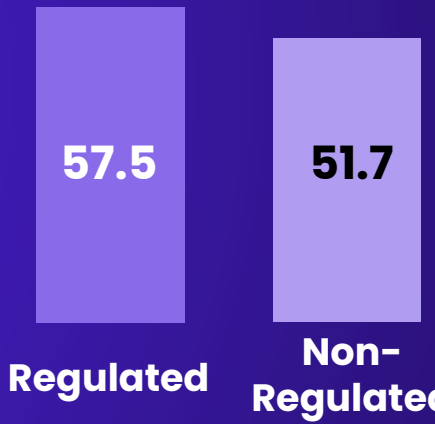
Based on **Wavestone 2024 CyberBenchmark**, overall maturity for large organizations is still increasing **(+1 point since 2023),** but the pace is slowing down

*Companies with a turnover over $1B (100+ org.)

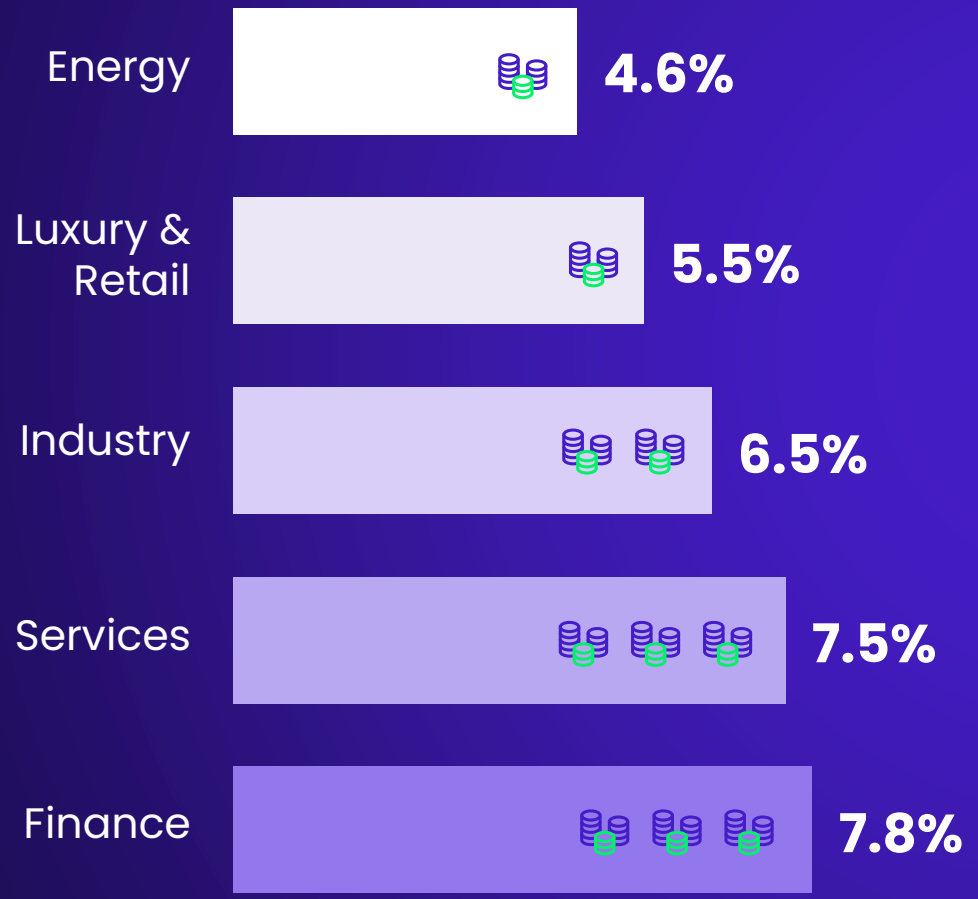
Financial sector is **well ahead** in overall maturity



Regulations have a **major impact** on maturity



Cybersecurity spending remain mostly stable in large organizations



Average IT budget percentage dedicated to cybersecurity*

6.6%

Range

First quartile	Last quartile
3.1%	**8.1%**

**Taking into account that budget percentages can vary a lot depending on previous investments and current build VS run balance*

Despite the lack of resources, cyber teams are still growing...

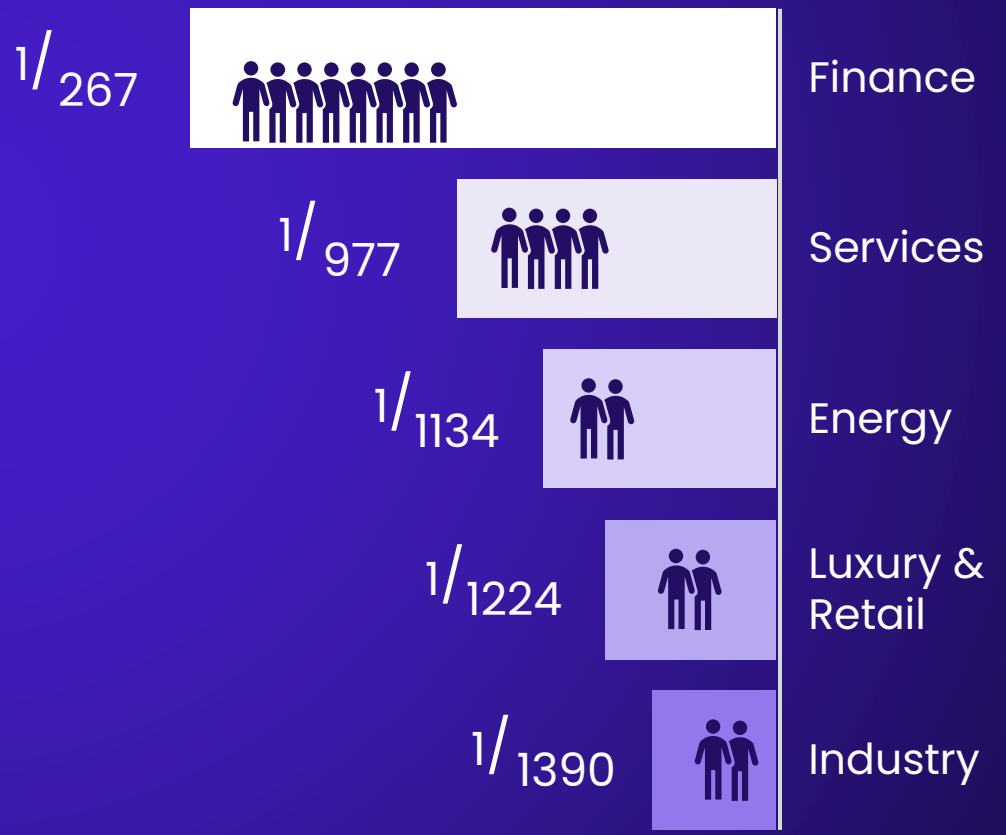
Average FTE dedicated to cybersecurity
per employee in large organizations

1/1086

Range

Best in class (top 10)	Last quartile
1/86	**1/1291**

... but differences between sectors remain significant



Talent management is a challenge that must not be overlooked

The cybersecurity workforce landscape is not without complexity…

Persistent talent shortage	Lack of diversity in profiles	Increasing skill gaps
4 million unfilled cybersecurity jobs in the world (+13% compared to 2022) *(ISC2 2023)*	Only **25% of women** working in cyber (+1% compared to 2022) *(ISC2 2023)*	**92%** of professionals reported having cybersecurity **skill gaps** within their organizations *(ISC2 2023)*

Some are starting to invest on short term and individual posture…

47% of the companies have defined a **salary policy** and monitoring gaps with HR

60% of the companies have a clear **mobility process**

…but actions taken are still lacking long term and collective view

0% of the companies have a materialized **career path** (66% are building their first)

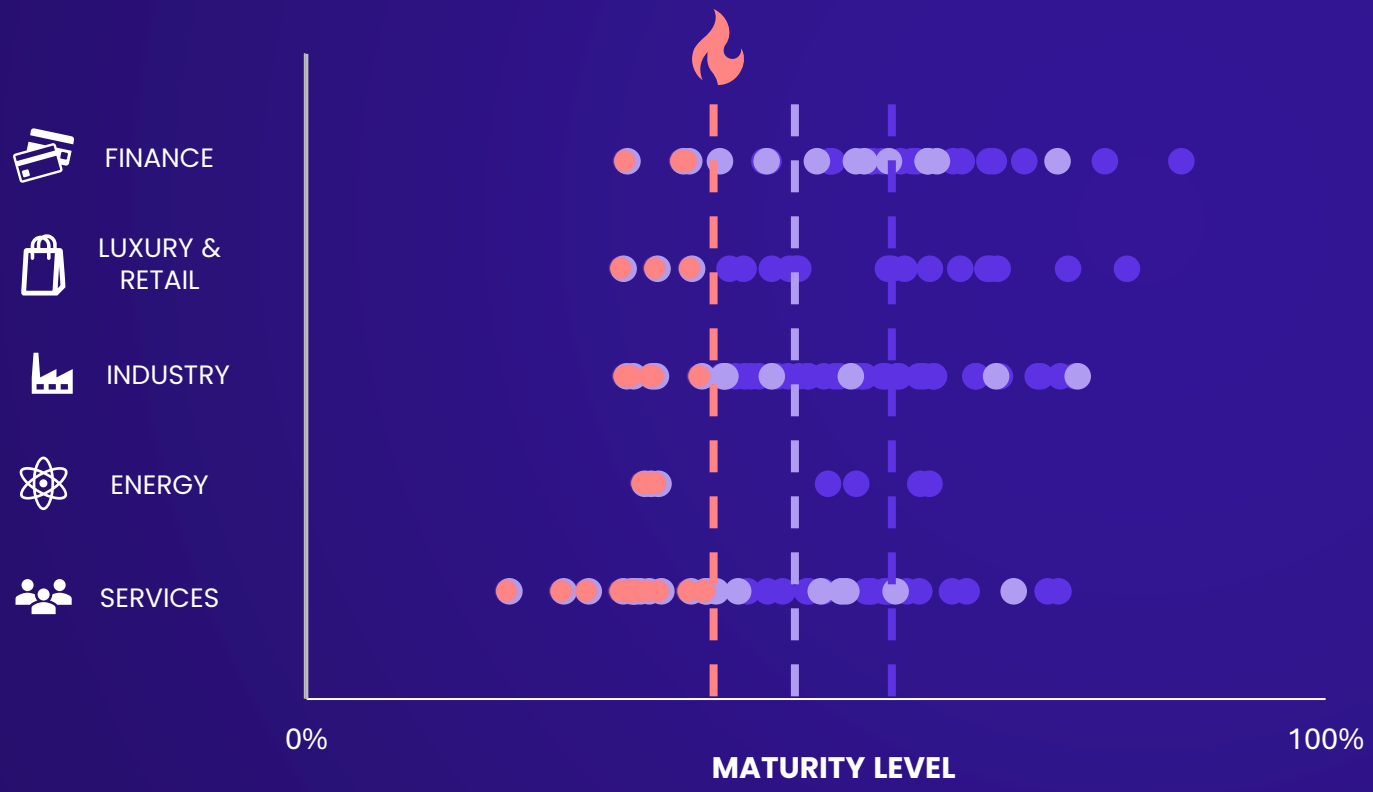
6% of the companies have initiated actions to enhance **their internal branding image** (20% for external branding)

Source: *Wavestone Cyber Talent Management Benchmark*


How does the
MARKET stand
against the latest
cyberattacks?
56.9%
Average maturity
against Ransomware
for large organizations

How does the market stand against the latest cyberattacks?

Based on the latest **cyberattacks managed by CERT-Wavestone**, we have selected 29 anti-ransomware measures and assessed our customers' maturity on each of them (concerned topics: attack entry point protection, crisis management, backups, red button…)



56.9%
ANTI-RANSOMWARE MATURITY OF **LARGE ORGANIZATIONS**

51.9%
ANTI-RANSOMWARE MATURITY OF **MEDIUM AND SMALL ORGANIZATIONS**

54%
OF **MEDIUM AND SMALL ORGANIZATIONS** CONSIDERED TO BE IN A **CRITICAL SITUATION**

0
LARGE ORGANIZATIONS IN A CRITICAL SITUATION

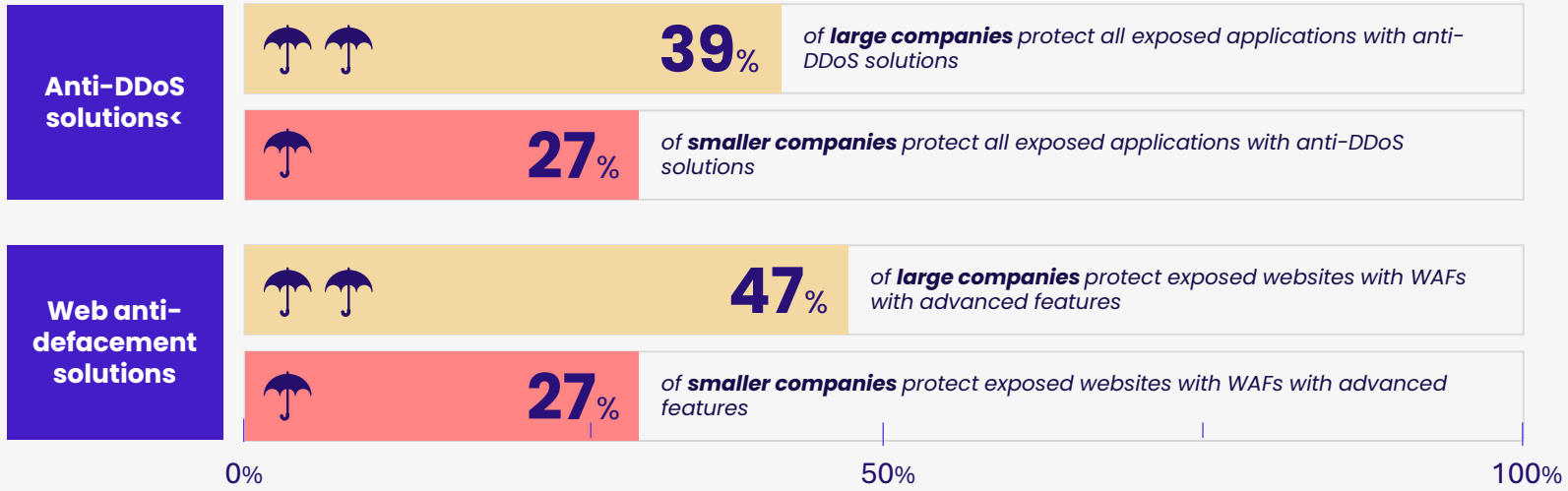
Large-scale events expose companies to a heightened cybersecurity risk

When a large-scale event takes place in a country, hacktivist groups are likely to launch **widespread DDoS (Distributed-Denial-of-Service) attacks** aimed at rendering proposed services unavailable via multiple requests and **website defacements** aimed at modifying the content shared on the affected sites against the companies within the country

Companies,
symbols of the country on the international stage and more or less involved in the event

Entities providing essential services to the event (security, transport, energy, logistics, etc.) **and official sponsors**

Official entities
(Organizing Committee, sites hosting the event, media…)



More likely to be targeted by **state threats**, **cybercriminals** and **hacktivists**

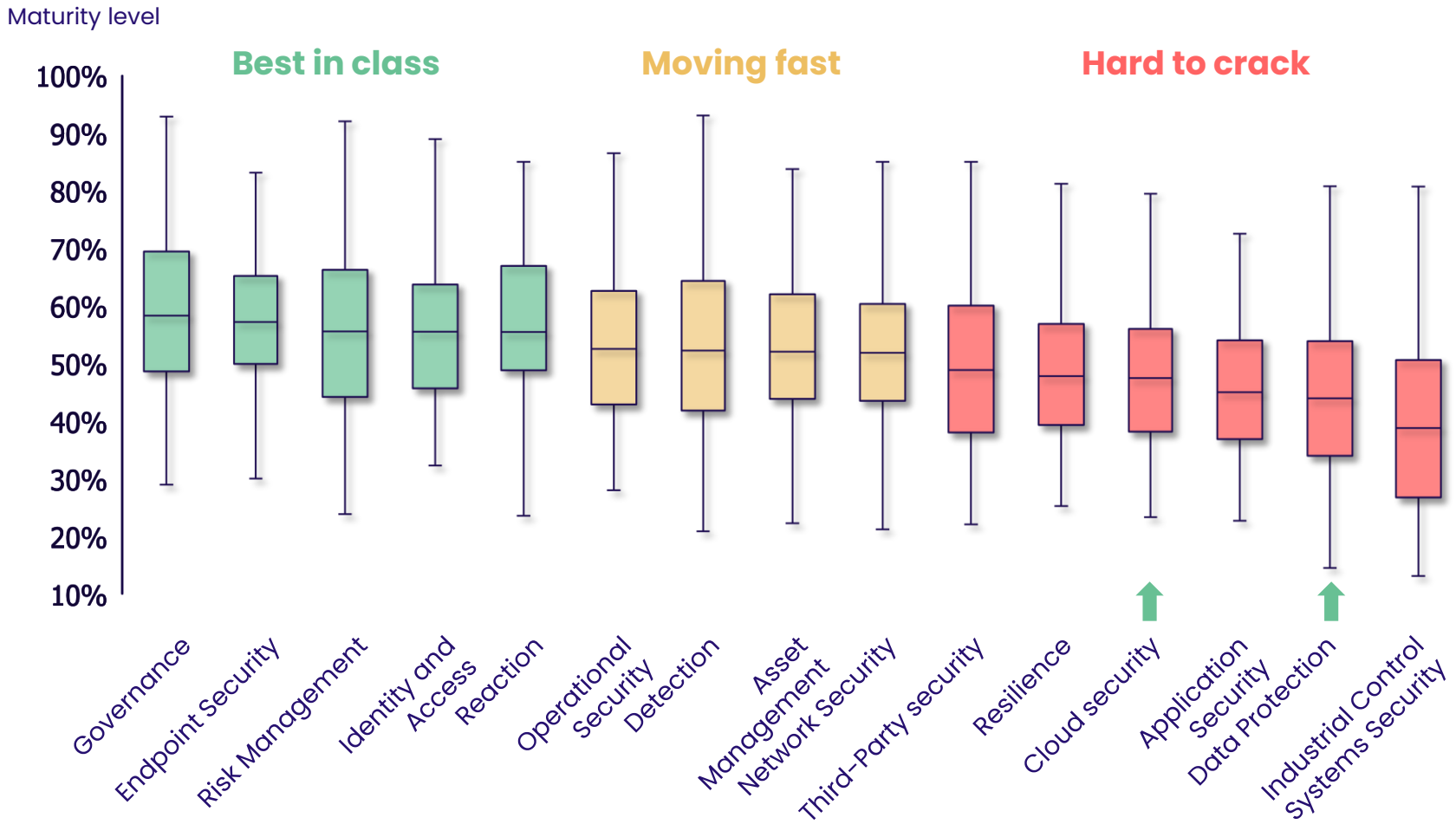
More likely to be targeted by **state threats**

A majority of these companies are **already supported by the authorities** and **have deployed advanced security measures** in response to high-level threats (state-sponsored cybercriminals, etc.)

Types of event stakeholders

Global overview on cyber topics

Large organizations' performance on key cyber topics in our 2024 CyberBenchmark



Box plot view of maturity score for every topic: Minimum / 1st quartile / Median / 3rd quartile / Maximum.

Cloud

Cloud security, which was one of the less mature topics the previous year, has experimented the **most important increase** of maturity between 2023 and 2024 (+5%).

In many cases, the will to carry out a **quick migration** to cloud resulted in an **unsatisfactory level of security** that is being enhanced over the years.

Data

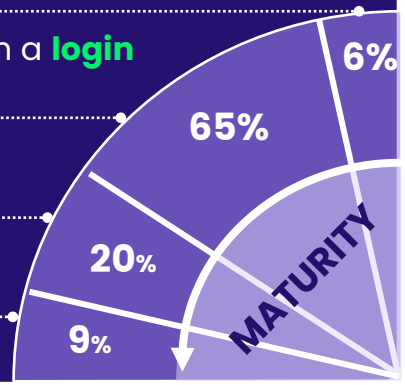
Data security has also strongly evolved since 2023 (+4%). **Non-structured data** (such as emails and documents) are better classified according to their confidentiality, which is a key prerequisite to implement **Artificial Intelligence** solutions that will facilitate access to data.

Moreover, **data leaks are better detected** than last year, thanks to manual or automated monitoring.

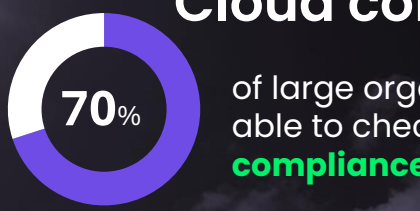
Cloud security is the biggest progress in 2024, reaching 48.3% for large companies (+5.1%)

Cloud administration

- Cloud console accessible **from anywhere** with a **login and password**
- **Multi-factor authentication** (MFA) for administration accounts
- Administrators must connect through a **bastion**
- **No admin** or **Just-in-Time** admin



Cloud compliance



of large organizations are able to check **cloud compliance**

of organizations **automatically correct** detected cloud non-conformities

New opportunities and challenges

CSPM (Cloud Security Posture Management) solutions and the challenge of **scaling up and putting the responsibility outside cyber teams**

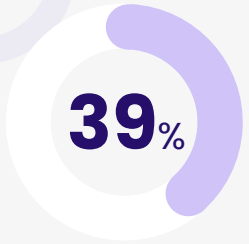
CNAPP (Cloud-Native Application Protection Platform) solutions and the challenge of **converging existing security tools**

Cloud Eraser resilience scenario and the challenge of **rebuilding a Cloud IS** from scratch

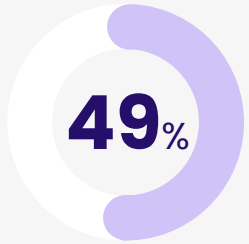
Data security is progressing, while Artificial Intelligence is aiming at disrupting Cybersecurity

Cybersecurity *for* AI

Artificial Intelligence solutions feed on enterprise data. Before implementing AI, it is essential to **secure the access to data** and to properly manage **access control**. Then, you can start thinking about securing the AI solution itself.



of large organizations are ready to **train their own AI model** in a secure way (data sanitization and classification)



of large organizations are ready to **use AI to facilitate access to data** while preserving data confidentiality (data identification, inventory and classification)

of our clients are launching or have already launched projects to secure their AI solutions

AI *for* Cybersecurity

Cybercriminals have seized AI technologies, which facilitate and accelerate their attacks. Therefore, **CISOs should** level up and also **adopt AI** for the **improvement** of their cyber capabilities. Some identified use cases are:

- **Anti-phishing** and **anti-malware** protection
- **Threat detection and response**
- **Identity and Access Management**
- **Data classification**
- **Network filtering** (review of firewall rules and verification of compliance to filtering policy)

Some entry points are being **increasingly exploited** by cybercriminals...

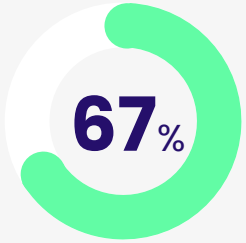
THIRD PARTIES

OPERATIONAL TECH & INDUSTRIAL SYSTEMS

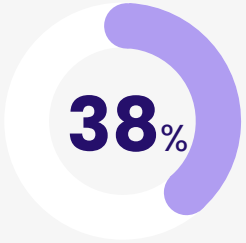
...and the path to progress on these issues **is both long and tortuous**

The implementation of a third-party security operational model remains a challenging issue for large organizations

A persistent challenge in securing their suppliers…

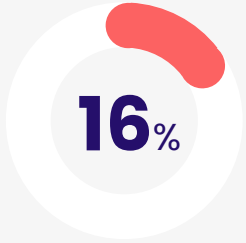


of large organizations include **security clauses in contracts** they signed



of large organizations **regularly audit** their critical suppliers*

**Among the 60% that correctly inventory their suppliers*



of large organizations test their **incident response** and **recovery plans** with their suppliers across **all critical areas**

…which slow down some clients…

Challenges that our clients often face due to the proliferation of suppliers (several thousands or even tens of thousands):

- **Lack of synergy and communication** with procurement teams
- **Lack of understanding** of third-party risks
- **Unreliable third-party inventory**, resulting from **a lack of detailed processes**

…where others succeed!

The success Story of a high-performing large group:

- **An efficient TPRM operational model** (synergy between security and purchasing)
- **30+ FTEs** dedicated to third-party monitoring
- Implementation of a **Data Warehouse**, **inventorying all third parties** continuously
- Ability **to link third parties to relevant business chains**, their level of risk, and underlying technical dependencies

A slow but constant improvement of Industrial Control Systems' security for large organizations: 39.9%

Network protection and filtering is the Industrial Control Systems topic that has progressed the most (**+4%**) since last year

Cyber Resilience is one of the current challenges for the industrial sector: only **36%** of large organizations manage safely **backups** and prioritize the most critical resources

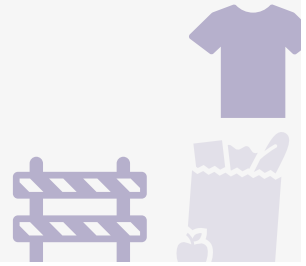
The **industry-related sectors** present significant **differences in maturity** depending on whether the sector is **regulated** or not.

50%

Of maturity for Sectors with **strong regulatory constraints**

37%

...whereas **other sectors** are noticeably less mature



NIS2

However, this is meant to change with **NIS 2 directive** in all EU countries. All sectors considered "essential" or "important" (many of which are industry-related) will need to be compliant to the directive (see dedicated focus).

What
TO EXPECT
in the years to come?

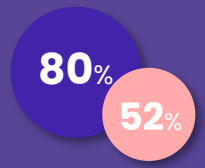
NIS 2: what should EU countries expect?

NIS 2 directive **extends the number of sectors** covered compared with NIS 1, will be applied to a lot more of organizations **(+50 employees and sales over 10M€)**. What's more, NIS 2's coverage now extends to **the entire company**, and not just to perimeters qualified **as essential**.

Are large organizations ready?

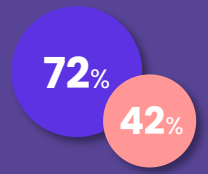
Through **the NIS 2 directive**, the European Union has set a number of **cybersecurity topics** that all EU countries must **comply with**. These topics include:

CYBERSECURITY POLICIES



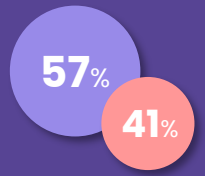
of large organizations have properly implemented **ISS Policies** and **risk analysis processes**.

RISK MANAGEMENT AUDIT PROCEDURES



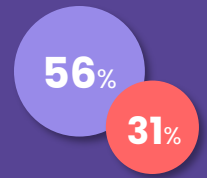
of large organizations **correctly control and audit** their IS, applications and cloud providers

INCIDENT RESPONSE



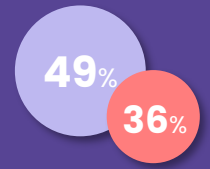
Large organizations have a 57% maturity score in the **incident reaction topics**

CYBER HYGENE & TRAINING



of large organizations **train** internal and external staff and top management **in cybersecurity topics**

BUSINESS CONTINUITY & CRISIS MANAGEMENT



Large organizations have a 49% score maturity in **resilience topics**

X% percentage of business with less than 1 billion turnover

The other *mandatory* topic areas

- HR, IAM AND ASSET MANAGEMENT
- CRYPTOGRAPHY
- SECURITY BY DESIGN AND IN RUN
- STRONG AUTHENTICATION & ACCESS
- THIRD-PARTY MANAGEMENT

Let's state the obvious, the cybersecurity landscape will constantly uncover NEW CHALLENGES

2024

Disruptive technologies
AI, encryption, quantum

Compliance Boom
CRA, DORA, NIS2, AI ACT

More aggressive attackers

Digital skills challenges

Economic uncertainties

Geopolitical tensions
Leading to decoupling

Cyber is becoming a differentiating factor for clients

2027

How do you fare? Get your own evaluation!


WAVESTONE