WAVESTONE

PRESS RELASE *Paris, April 19, 2023*

Cyber maturity: significant progress in large organizations impacting cyberattacks effectiveness

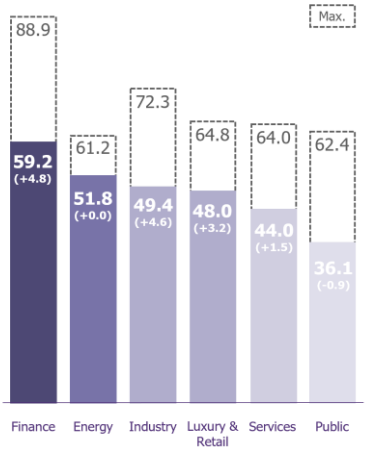
- Large organizations' **level of maturity is still low (49%)** but **has improved (+3 points)**.
- **23%** of large organizations evaluated remain very **vulnerable to potential ransomware attacks**, compared to 30% last year.
- Cyber budgets represent **5.6% of the IT budget** across all sectors, at the bottom of the recommended range (between 5 and 10%).
- **1 expert is dedicated to cybersecurity for every 1,300 employees** on average, which is an 11% improvement over last year despite recruitment challenges.
- The ability to **rebuild following an attack** remains the most complex topic to address (**43% maturity**).
- Some **key areas of cybersecurity remain unresolved**, in particular the security of **third parties** (partners, suppliers... increasingly interconnected) at 46.9% maturity, **cloud security** at 44.0% and **industrial systems** at 37.6%.

While cyber attacks are on the rise (crime, hacktivism, countries) in a troubled geopolitical context, companies are challenged to accelerate their digital transformation. But are they really equipped to face these threats? **What are the most mature sectors when it comes to cybersecurity? What assets do large organizations have at their disposal, and what pitfalls should they beware of?**

To answer these questions, the consulting firm Wavestone consolidated and analyzed data from over **100 organizations**, representing almost **5 million users**, based on a field assessment of almost **200 security measures**. Scores are based on **NIST Cybersecurity Framework and ISO 27001/2 international standards**.

Results confirm that companies are experiencing the benefits of their recent cyber investments, with an **overall maturity score of 49%**, increasing on 3 points since 2022.

Cyber maturity in progress (+3 points), yet strong sectoral disparities



The overall security score of 49% disguises significant gaps between sectors. **Finance is strong with a score of 59.2% (+4.8 points from 2022)**. This is the result of historically high investments in the industry, encouraged by regulations (DORA, NIS2, CRA). **Industry is also improving (+4.6 points)**, in an effort to catch up. **Services (44%) and Public Sector (36.1%) have the lowest score.** Although aware of the risks, this sector struggles to secure the necessary funding.

Ransomware vs. new cyber strategies: companies are gaining momentum (+7 points)

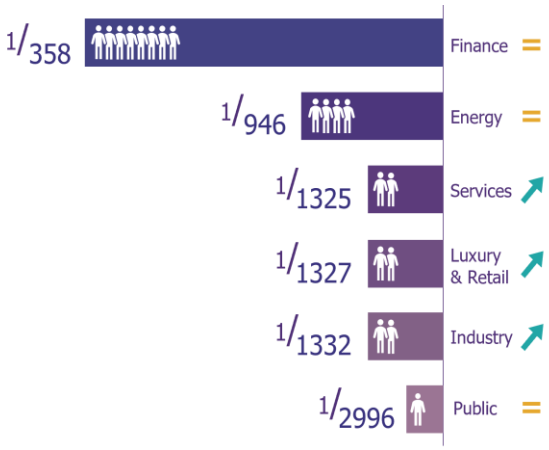
In 2022, when faced with the risk of ransomware attacks, 30% of organizations were in a **critical situation**; compared to only **23% in 2023**. This reflects significant efforts on killchain topics: attack entry point (+3 points), infrastructure (+4 points), detection (+6 points) and crisis management (+3 points).

This improvement is visible in the field, where large structures are less affected by visible incidents. In reality, **attacks are still being attempted**, but are **detected and stopped** before causing too much damage.

Workforce: the trump card of cyber strategies

Within benchmarked organizations, security teams continue to grow: there is approximately **1 person dedicated to cybersecurity for every 1,300 employees**, **an increase of 11% compared to last year**. However, this number is still too low in respect to upcoming challenges. Some players attempt to deal with the subject head-on, in particular through "talent management programs".

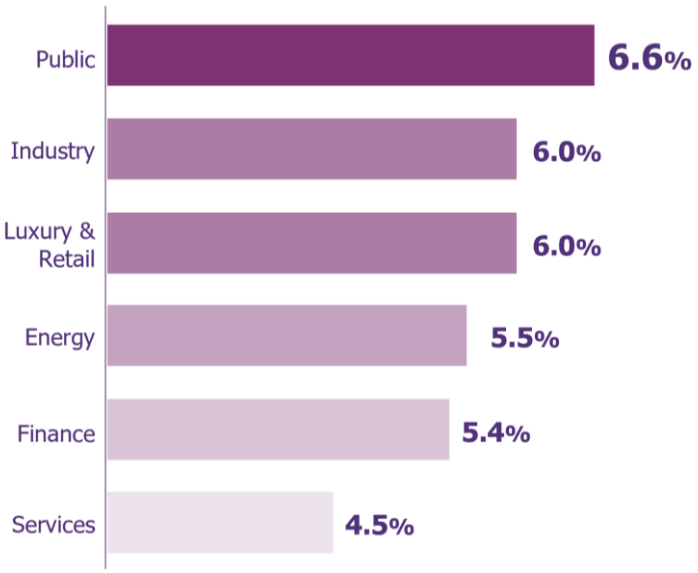
Looking at the specifics of each sector, we believe that **a plateau has been reached in Finance**.



Investments: the end of a cycle

In audited companies, 5.6% of the overall IT budget is dedicated to digital security. Rather steady, this figure points towards the end of a period of strong funding.

From a sectoral point of view, the **highest spending** is in **Public Services (6.6%), Industry (6%) and Luxury & Retail (6%)**. This may be explained by a longer delay in catching up, coupled with increased awareness that is now bearing fruit.



Looking ahead: cyber trends to monitor

Cyber-resilience: a two-speed market

When it comes to resilience, **a clear line stands between the financial sector and the rest of the industries**. Yet, risks do exist and all companies are impacted.

- While 70% of financial players regularly review their **residual risks** in their Risk Treatment Plan (RTP), only 28% of companies in other sectors do the same.
- 60% of Finance companies continuously improve their **processes for managing security incidents** and have distinct cyber response plans for different scenarios. **That's only 40% in the rest of the business sectors.**
- When it comes to **third-party security**, 60% of Finance companies have a process in place to regularly audit their suppliers, based on their criticality – compared to only 32% for the rest of the organizations.
- Most notably, 55% of Finance organizations test all **Business Continuity Plan (BCP) scenarios** at least every two years (DORA regulations require this to be done annually). Only 9% of other organizations perform these tests.

Zero Trust, a strategic deployment

Zero Trust is one of the major challenges of the next few years in cybersecurity. Some figures illustrate its **current application**.

- 24% of companies have implemented **automatic micro-segmentation** (e.g. Illumino) based on exposure, sensitivity, environment, etc. – deployed at an average of 32%.
- 14% have integrated **identity-based Zero Trust Network Access** into their cloud environments – deployed 46% on average.
- 28% take into account resource sensitivity and login context and apply **multi-factor authentication (MFA**) with conditional access – deployed 73% on average.
- 13% have begun deploying **Security Orchestration, Automation and Response (SOAR)** to isolate resources upon detection of an alert – deployed 48% on average.

Cyber Benchmark methodology

Maturity levels were measured against international standards (NIST Cybersecurity Framework and ISO 27001/2). The assessment was carried out during the course of audits conducted by Wavestone consultants, mainly through interviews with security leaders of the company under review. The sample, dated April 1, 2023, includes more than 100 organizations (including a majority with more than 10,000 employees and 30 Tier 1 groups: CAC40 organizations, FTSE100 organizations, or organizations with more than 100,000 employees), i.e. nearly 5 million employees. The data from these individual assessments was then consolidated and analyzed by Wavestone's teams

Our contacts

Belgium: Noémie HONORE – noemie.honore@wavestone.com
France: Gérôme BILLOIS – gerome.billois@wavestone.com
Luxembourg: Jérôme De Lisle - jerome.delisle@wavestone.com
Honk Kong: Chadi HANTOUCHE - chadi.hantouche@wavestone.com
Switzerland : Valery PIALAT – valery.pialat@wavestone.com & Rémi PACTAT - remi.pactat@wavestone.com
United-Kingdom: Florian POUCHET – florian.pouchet@wavestone.com
USA: Baptistin BUCHET - baptistin.buchet@wavestone.com
& Keith WORKFOLK - keith.worfolk@wavestone.com

About Wavestone

In a world where knowing how to drive transformation is key to success, Wavestone's mission is to inform and guide large organizations in their most critical transformations, with the aim of a positive outcome for all stakeholders. This is anchored in the firm's DNA and embodied in our overarching values, known as "The Positive Way."

Wavestone draws on 4,000 employees across Europe, Asia, and the United States, and is a leading global consultancy.

Wavestone is listed on Euronext Paris, is recognized as a Great Place to Work®, and ranked in Forbes's World Best Management Consulting Firms 2022 List.

More information www.wavestone.com // @wavestoneFR

Wavestone – Press Contact

Mélodie LAUQUE

press@wavestone.com