

EUROPEAN COMPANIES FACING THE CYBERSECURITY CHALLENGE

ETHIFINANCE ESG DATABASE 2023-2025

EthiFinance

EXECUTIVE SUMMARY

As companies face a rapidly evolving and intensifying cyber risk landscape, assessing their ability to manage this exposure has become a key component of their non-financial performance. As part of its annual extra-financial rating campaigns, EthiFinance therefore tracks a number of indicators relating to the practices put in place to mitigate this risk.

This study quantifies the cybersecurity practices of the **2,346 listed European companies rated by EthiFinance in 20251 and tracks how those practices have evolved** since 2023. In addition to this overall analysis, we conducted a more targeted review of a sample of **646 companies** operating in sectors for which our double materiality analysis highlights particularly high cyber risk materiality (both for the company itself and for its stakeholders, including society at large).



The key takeaways are as follows:

1. **A risk now widely recognised, but with a clear execution gap**: nearly 90% of companies integrate cyber risk into their operational risk framework, yet implementation of concrete measures remains uneven, with penetration testing at around 60%, ISO 27000 certification rarely exceeding 31%, and training disclosure averaging just 20%. Among companies that do disclose, 79% report training more than 75% of their workforce; when companies commit, they tend to do so at scale.
   Pages 10-13

2. **No meaningful over-performance among high-risk companies**: within the panel of the 646 most exposed companies, the picture remains broadly aligned with that of the full sample. Cyber risk is widely recognised, but this does not systematically translate into stronger mitigation measures, with penetration testing reaching only 63% and ISO 27000 certification 39%.
   Pages 10-12

3. **Company size is not a major differentiating factor**: regardless of market capitalisation, cyber risk is well identified and the gaps observed across mitigation practices remain limited overall, not exceeding 4 to 5 points in 2025. Pages 3-5

4. **Sector gaps remain pronounced**, with some sectors showing more advanced maturity, notably Transport & Logistics, which leads on penetration testing (62%) and employee training coverage (93%), while others continue to lag, such as the Food sector (74% for integration into the operational risk framework; 17% for ISO 27000 certification).
   Pages 7-8

5. **Country analysis reveals a multi-speed Europe**: while integration of cyber risk into the operational risk framework exceeds 80% in most countries and reaches 100% in Ireland, Portugal and Lithuania, significant gaps remain in technical practices, with France peaking at nearly 72% for penetration testing versus around 30% in some Nordic countries.
   Pages 5-6

6. **Overall transparency remains uneven, particularly on employee training**: only 23% of companies disclose their training practices, even though this is a key indicator of maturity in cyber risk management.
   Pages 11-12

EthiFinance

1. Analysis by Market Capitalisation

The analysis by market capitalisation points to a high degree of consistency: whatever the indicator considered (penetration testing, ISO 27000 certification, integration into the operational risk framework, or employee training coverage), the gap between size segments does not exceed 4 to 5 points in 2025. Small Caps, often perceived as lagging behind, are narrowing the gap (+8 pts in high training coverage since 2023). Company size therefore does not appear to be a strong predictor of cybersecurity practices.

Integration into the operational risk framework: this is the most consistent indicator. Regardless of size, classifying cyber risk as an operational risk is now an established governance practice across almost the entire market.

Penetration testing: this practice remains correlated with market capitalisation. Large Caps maintain high adoption rates throughout the period, while Small Caps post the lowest rates, including a slight decline in 2025.

ISO 27000 certification: mid-cap companies post the highest certification rates, followed by large-cap companies. Smaller companies continue to lag on this international standard.

Employee training coverage: contrary to expectations, training coverage is relatively consistent across size segments: around 77% to 81% of companies train more than 75% of their workforce, regardless of market capitalisation. Mid Caps lead (81%), but Small Caps have significantly narrowed the gap (+8 pts since 2023, rising from 69% to 77%). The overall trend is one of convergence.

Figure 1: Trend in penetration test completion rates

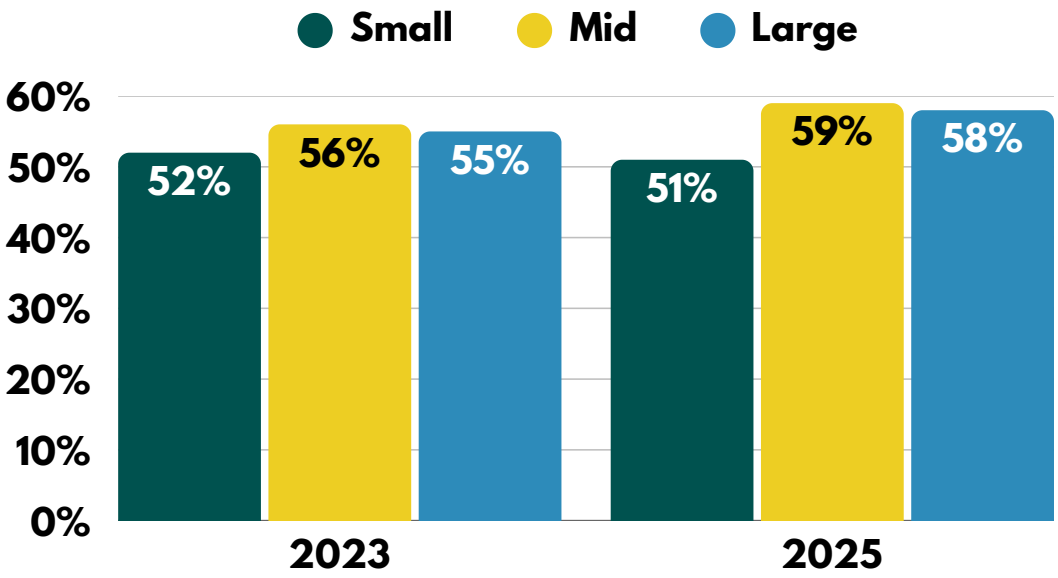


Figure 2: Evolution of adoption rates for international cybersecurity standards (ISO 27000)

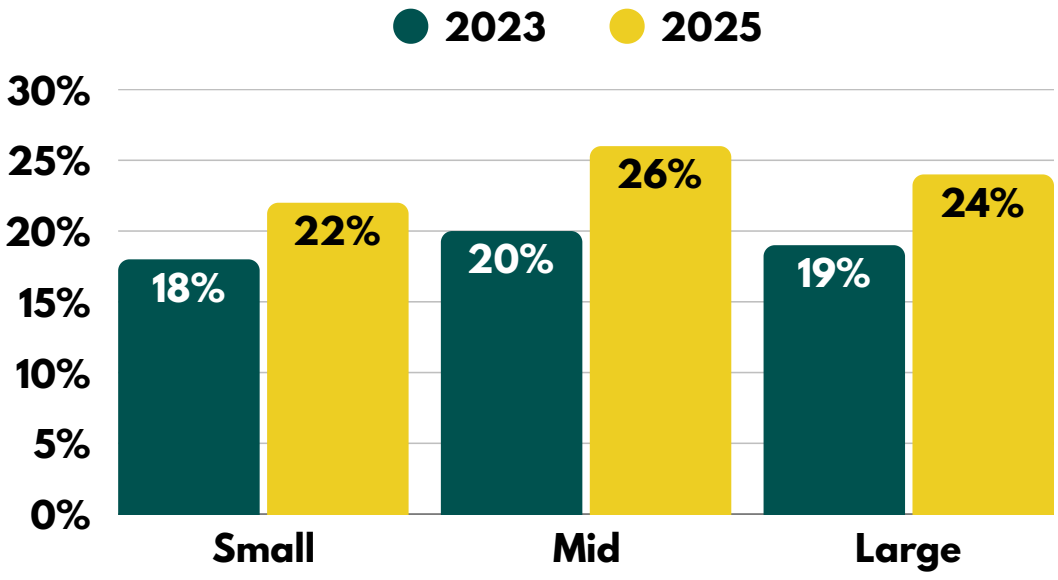
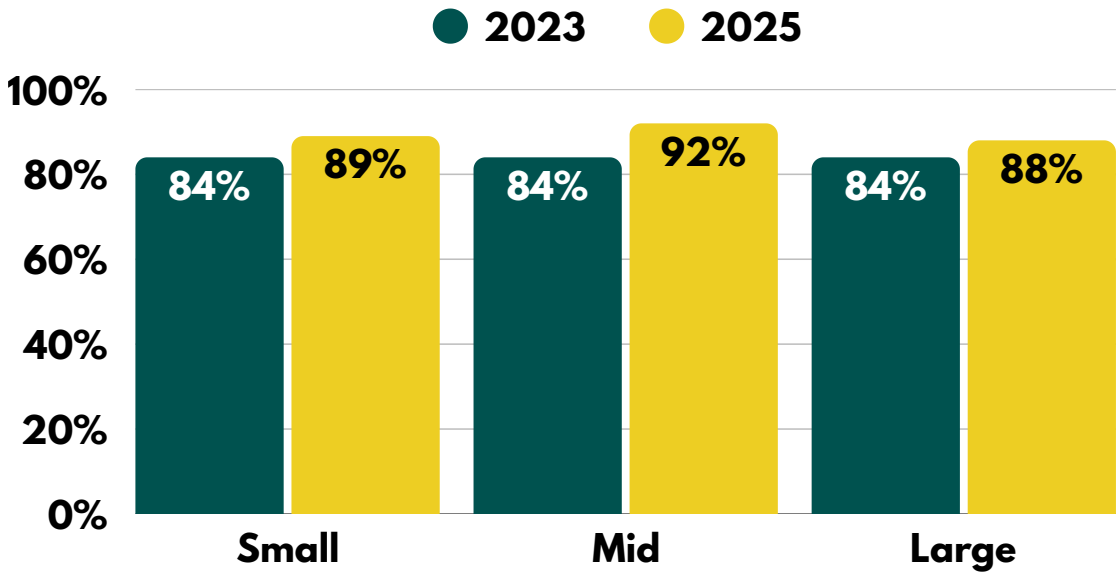


Figure 3: Evolution of cybersecurity risk integration into operational risk mapping



Share of companies that trained more than three quarters of their employees

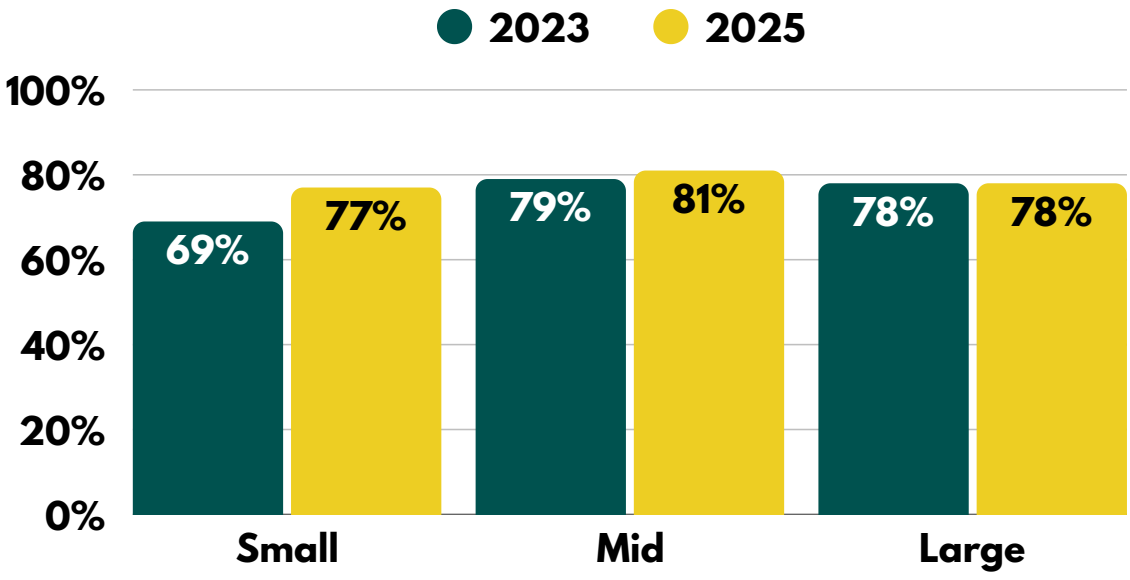
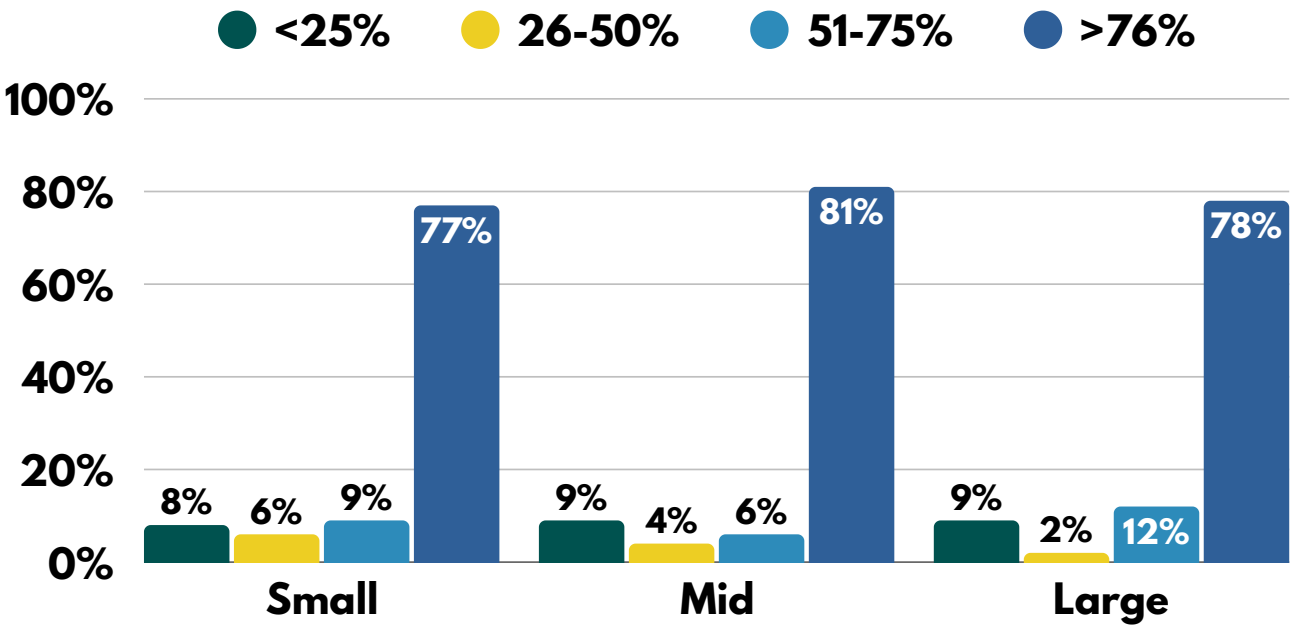


Figure 4b: Distribution of cybersecurity-trained employees by company size (2025)



2. Analysis by Country

Country analysis reveals a multi-speed Europe: while integration of cyber risk into the operational risk framework exceeds 80% in most countries and reaches 100% in Ireland, Portugal and Lithuania, significant gaps remain in operational implementation, with France peaking at nearly 72% for penetration testing versus around 30% in some Nordic countries.

Integration into the operational risk framework: in 2025, this practice is almost universally established, with most countries above 80%. Ireland, Portugal and Lithuania stand out at 100%, well ahead of Poland (73%) and Norway (77%), which rank at the bottom. Over 2023-2025, the trend is one of broad consolidation, supported by strong catch-up effects, particularly in Greece (+21 pts) and Lithuania (+17 pts).

Penetration testing: in 2025, the use of these tests shows strong contrasts: France stands out at nearly 72%, whereas Nordic countries struggle to exceed 30%. The 2023-2025 analysis underscores this divide: while a few countries such as France and Greece are on an upward trajectory, most countries ultimately recorded a decline in these practices over the period as a whole.

ISO 27000 certification: Greece stands out, closely followed by Spain and Austria, with rates approaching 50%. By contrast, Ireland and Northern Europe rank last, with rates around 12%. Over 2023-2025, the European trend is overall positive, with an average increase of +1.7 points. This overall improvement would have been stronger without the sharp decline observed in a few countries, including Austria (-5 points) and especially Lithuania (-33 points).

Employee training coverage: in 2025, transparency remains low (only 10% to 20% of companies disclose on this topic, depending on the country), except in France (36%). Among those that do disclose, employee coverage is high: in Denmark and Ireland, 100% of reporting companies train more than 75% of their workforce. Over 2023-2025, the disclosure rate remains flat, but performance is becoming more polarised. Leading countries are stepping up their efforts (the share of highly engaged companies rose from 59% to 70% in France, and from 73% to 90% in Norway), unlike Lithuania, which fell sharply (from
100% to 0%).

Criterion	Observations (2023-2025 Trends)
Over-representation	The leading trio - **France** (score of 56%), **Greece** (54%) and **Ireland** (50%) - stands out on a strong upward trajectory. These leaders are lifting the European average through strong penetration testing results (≥68%) and distinct strengths: France leads on training disclosure (36%), Greece is clearly ahead on ISO 27000 certification (50%), and Ireland reaches 100% for integration into the operational risk framework.
Under-representation	Northern Europe (**Sweden** and **Norway** at 34%, **Denmark** at 38%) records the lowest overall maturity levels. This cluster lags significantly on both technical and normative pillars, with penetration testing capped at 30% to 34% and ISO 27000 certification at 11% to 13%. In addition, Sweden and Norway show a completely flat trajectory (trend →).
Change	Major markets such as **Italy** and the **Netherlands** show a more moderate overall trajectory. While they record very strong integration of cyber risk into the operational risk framework (close to or above 90%), they also show a clear decline in penetration testing (down 11 and 8 points respectively), bringing their rates back to around 60% in 2025.

3. Sector Analysis

The sector analysis confirms persistent maturity gaps: some sectors show more advanced practices, while others remain clearly behind. Transport stands out on penetration testing (62%) and employee training coverage (93%), whereas the Food sector continues to lag on integration into the operational risk framework (74%) and ISO 27000 certification (17%).

Integration into the operational risk framework: in 2025, the *Retail* (95%) and *Real Estate* (93%) sectors lead, well ahead of the *Food* (74%) and *Leisure* (77%) sectors, which rank last. Over 2023-2025, integration levels are generally moving towards 90%, supported by strong catch-up effects, particularly in the *Media* (+11 pts) and *Construction* (+8 pts) sectors, with the exception of the *Food* sector, which continues to struggle to improve.

Penetration testing: in 2025, the *Transport* (62%) and *Materials* (62%) sectors lead, in contrast with the low rates observed in *Construction* (44%) and *Leisure* (47%). Over 2023-2025, the *Materials* sector posts strong progress (+6 pts), while the *Construction* sector deteriorates sharply (-11 pts). Although *Transport* remains the current leader, it has declined from its 2023 level (68%).

ISO 27000 certification: in 2025, adoption remains limited (rarely >30%). The *Leisure* (32%) and *Transport* (28%) sectors perform best, whereas the *Real Estate* (15%) and *Food* (17%) sectors clearly lag behind. Over 2023-2025, the trend is generally upward: the *Automotive* sector posts the strongest increase (+9.8 pts), in contrast with the stagnation of the *Food* sector.

Employee training coverage: in 2025, transparency remains low across all sectors: only 11% to 32% of companies disclose on this point (with the *Automotive* sector leading at 32%). However, among these reporting companies, the *Transport* (93%) and *Commercial Services* (93%) sectors stand out for broad training coverage (more than 75% of employees covered), well ahead of the *Consumer Goods* sector (50%). Over 2023-2025, while the disclosure rate remains flat, performance is becoming more polarised: the *Real Estate* sector is catching up (+17.7 pts in highly engaged companies), while the *Food* sector is declining sharply (-30 pts).

Criterion	Observations (2023-2025 Trends)
Over-representation	The **Transport & Logistics** sector emerges as the most mature, leading on penetration testing (62%) and employee training coverage (93%). The **Commercial Services** sector follows closely on the human factor (92%), while **Retail** stands out for integration into the operational risk framework (95%).
Under-representation	The **Food** sector lags across the board, ranking last on integration into the operational risk framework (74%) and on ISO 27000 certification (17%). From a purely technical standpoint, the **Construction** sector (44%) and the **Leisure** sector (47%) show the greatest vulnerabilities in 2025 in terms of penetration testing.
Change	Over 2023-2025, the ***Real Estate*** sector shows a strong catch-up in employee training coverage (+18 pts among companies with high coverage, reaching 87%). Conversely, the ***Food*** sector records a sharp decline on the same indicator (-30 pts), while the ***Construction*** sector declines on penetration testing (-11 pts).

EthiFinance

4. High Cyber-Risk Sectors
(646 companies)

Within this panel of high-materiality sectors (where the risk is material both for companies and for their external stakeholders*), one might expect more robust systems and more developed reporting. However, the differences observed relative to the full sample remain limited. The lack of published data also constrains investors' ability to assess the actual level of control over this type of risk.

Integration into the operational risk framework: with 90% of companies in this segment classifying cyber risk within their operational risk framework in 2025, this group does not stand out materially from the broader sector universe, where this practice is already widely established. Over 2023-2025, this standardisation strengthened further, with steady progress (+6 points from 84% in 2023), mechanically reducing the share of less engaged companies to just 9%.

Penetration testing: for this more exposed group, technical testing is a majority practice in 2025, reaching an implementation rate of 63%, only slightly above the full sample (60%). This gap remains limited: the most exposed sectors stand out only marginally on this technical measure, even though it is a central tool for preventing and detecting vulnerabilities. Over 2023-2025, use of these tests nevertheless increased by +4 points from its starting level (59% in 2023).

ISO 27000 certification: in 2025, adoption remains moderate at 39%, around 9 points above the average observed across all sectors, where certification rarely exceeds 30%. Despite the materiality of the risk, formal certification has not yet become a generalised requirement: nearly 60% of companies in this panel remain uncertified, highlighting significant room for improvement on this indicator. Over 2023-2025, however, there was an increase of +8 points (from 31% in 2023), accompanied by a decline in non-disclosure (from 61% to 56%).

Training disclosure: In 2025, transparency remains particularly low, with only 23% of companies publishing quantified data (versus 77% non-disclosure), a level only slightly above that observed across the full sample (20%). Over 2023-2025, this

** Double materiality analysis conducted by EthiFinance teams across 38 sectors*

practice has stagnated and gained little traction, posting only a marginal increase (+3 points from 20% in 2023): this type of reporting is clearly not yet viewed as essential.

Employee training coverage (reporting sample): 80% of companies in this segment that disclose their training practices report covering more than 75% of their workforce. This is aligned with the broader trend observed across the full sample (79%). Over 2023-2025, this training dynamic strengthened slightly (+2 points from 79% in 2023), while the share of companies covering less than a quarter of their workforce declined from 11% to 5%. In other words, when information is published, high-materiality sectors do not stand out for significantly greater training intensity, but rather confirm a pattern already visible across the rest of the market.

Figure 1: Evolution of IT penetration testing

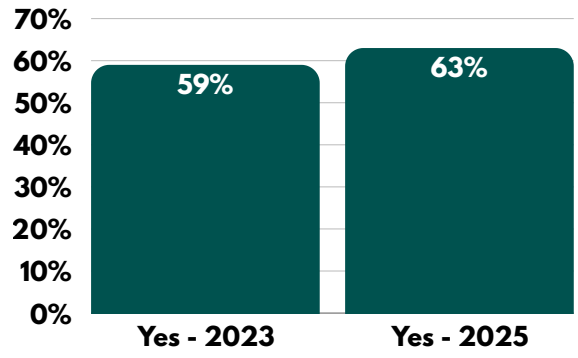


Figure 2: Cybersecurity certification rates (ISO 27000)

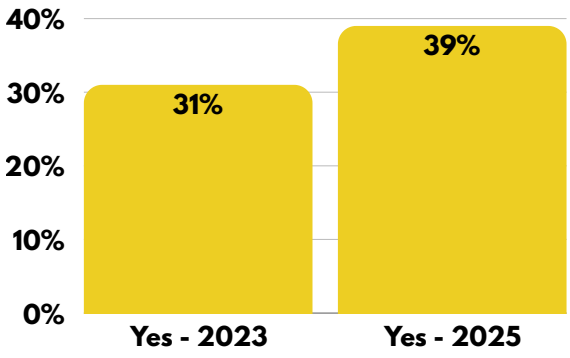


Figure 3: Evolution of IT risk integration into operational risk mapping

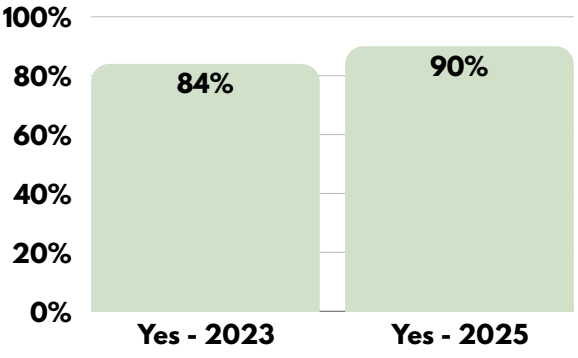


Figure 4: Reporting rate on the share of employees trained in cybersecurity

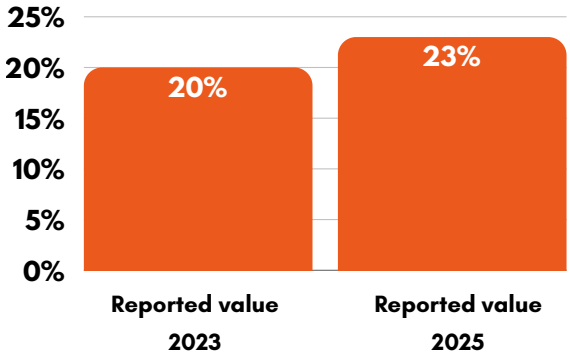
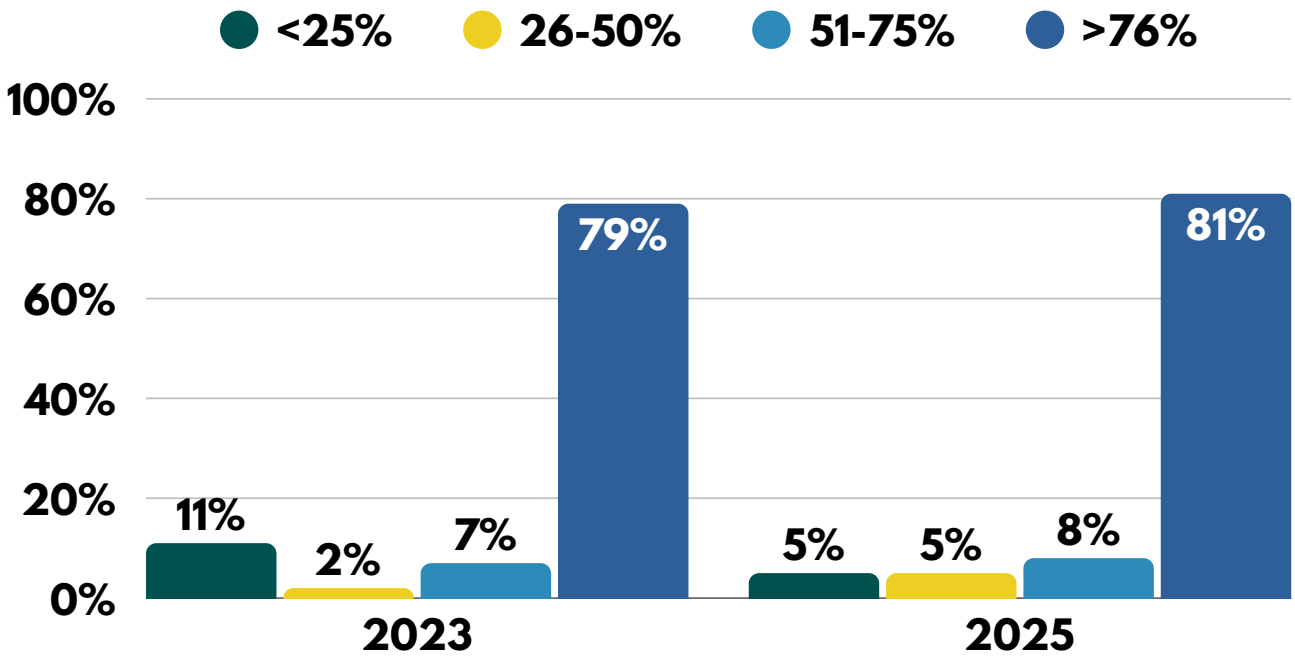


Figure 4b: Share of employees trained in cybersecurity (among companies that disclosed this data)



EthiFinance

EthiFinance is an innovative European ratings, research and advisory group dedicated to sustainable finance. The group provides solutions to investors, businesses and organisations to address financing challenges as well as environmental and societal changes.

EthiFinance ESG Database

EthiFinance conducts an annual ESG rating campaign covering more than 2,400 listed European companies. The database provides comprehensive insights across all extra-financial pillars, including governance, social and environmental factors.

It enables investors and corporates to assess ESG performance, identify risks and benchmark against peers.

Want to know more ?