EthiFinance

Cybersecurity Management in ESG Ratings

European Survey 2023 by EthiFinance

Content

Executive Summary

Our study finds that European firms tend to take cyber threats seriously and increasingly try to protect themselves from them through certification and training. Nevertheless, data breaches and cyberattacks remain major concerns. Our key findings are the following:

- The **average cybersecurity score** across European companies has **steadily and strongly increased** over the past three years, underlining the improvement in their overall maturity in managing cyber risk.
- **Austrian companies receive the highest average cybersecurity score**, followed closely by the Dutch, Irish and French firms. Countries with the lowest average scores are Norway, and Sweden.
- **Cyberattacks and data breaches** are more often happening to companies from **Industrials, Consumer Discretionary and Financials** and to firms in **Spain, Portugal, Ireland, Austria, and France**.
- European companies are **increasingly including cyber risks into their operational risk management**. This is the case above all for large firms and to a lesser extent for smaller companies.
- **The ISO 27000 certification is widely used** in most European countries, except for **France**, where only one third of companies were certified in 2023. **Real Estate** companies show a **particularly low certification rate** as opposed to organisations from other sectors.
- While **cybersecurity training for employees** is key for protection organisations from IT system intrusion, is not a topic that many companies report on and the proportion of companies with fully trained staff is only half of those providing the information.
- **Intrusion tests are a widely used tool** in cyber risk management. Half of the companies within our sample report on the topic and almost all of them carry out intrusion tests on a regular basis.

Introduction: Cybersecurity, the Newcomer in ESG Analysis

Over the last decade, cybersecurity has become a huge challenge for the global economy in all parts of society. According to The World Economic Forum Global Risk Report 2024, cyberattacks rank fifth in likelihood to cause a global crisis in 2024 and fourth in potential severity over two years. The private sector has been increasingly challenged to ensure robust security for IT systems and privacy requirements, and cybersecurity has made its way up to the top league of most threatening risks for corporates and their clients and stakeholders.

European Regulators are increasingly putting companies under pressure to establish robust governance structures to oversee privacy and cybersecurity risk management. The European Union has implemented comprehensive regulatory measures to enhance cybersecurity resilience, notably GDPR, DORA and NIS2 (see Box 1).

Given the significant risks associated with cybersecurity, the topic has now found its way into sustainability risk assessments and ESG reporting. Major reporting standards such as SASB and GRI incorporate cyber risk as a material sustainability factor and providing guidance on how companies should disclose their management of cybersecurity and data privacy issues.

Box 1: EU Regulation reinforcing cybersecurity

- The General Data Protection Regulation (GDPR): Implemented in 2018, this regulation mandates companies within the European Union to implement security measures for data protection, ensuring the safeguarding of individuals' personal data.
- The Digital Operational Resilience Act (DORA). This regulation is expected to be enforced in the coming years (potentially around 2025), which aims to ensure the operational resilience of the EU financial sector against cyber threats and incidents. It requires financial institutions to develop and maintain robust cyber resilience strategies and incident response plans, as well as establish reporting obligations for significant cyber incidents.
- The revised Network and Information Systems Directive (NIS2): Adopted in 2022, this Directive introduces risk management and incident reporting obligations for covered entities, along with requiring member states to establish competent authorities responsible for overseeing compliance and coordinating incident response efforts.

Cybersecurity Analysis in EthiFinance's ESG Ratings

Through our ESG Ratings, we assess the extent to which companies manage the ESG risks and issues that are material to them from a double materiality perspective, i.e. both from a financial perspective, and from an impact and stakeholder perspective. Our ratings are based on more than 140 ESG indicators spread across four pillars: Environment, Social, Governance, and External Stakeholders. In addition to data collection from publicly available sources and company disclosure, our analysts systematically reach out to companies, inviting them to supply additional information.

The topic of cybersecurity is covered in the "External Stakeholder" Pillar of EthiFinance's ESG Ratings framework. It is weighted between 3.5% and 4.6% in the overall ESG score, depending on the sector. The topic is analysed through four distinctive indicators:

- Incorporation of IT/cyber risks in the company's operational risks
- ISO 27000 Certification
- Cybersecurity training for employees
- Intrusion tests of IT systems

The data availability (public information and information provided via company dialogue) varies from one topic to the next, as shown in Table 1.

Table 1: Data Availability per Cybersecurity Topic in 2023

Cybersecurity Topic	Data Availability 2023
Incorporation in Operational Risk	100%
Intrusion Tests on IT Systems	55%
ISO 27000 Certification	25%
Cybersecurity Training for Employees	16%

In addition to our analysis of the management of cybersecurity risks by companies, we also track IT- and cyber risk related incidents within our controversy research. We follow incidents in different areas:

- Data leaks
- Cyber-attacks
- Violation of data protection regulation

The analysis presented in this report covers 2321 European companies, 6% of which are large corporations, 55% midsized firms and 39% small companies. The data has been collected during our 2023 ESG Ratings update, covering mostly data reporting on the 2022 fiscal year.

Cybersecurity management within European Companies: Our Findings

Cybersecurity Incidents Widespread Across Sectors

Cybersecurity is a concern that affects virtually every sector without exception – all types of organisations can be victims of cybercrime, intrusions, and data leaks. According to our controversy database, every sector in our Rating Universe except Real Estate has faced at least one cybersecurity-related incident over the past three years. However, certain sectors seem more prone to cyberattacks or data breaches, notably Industrials, Consumer Discretionary and Financials (Chart 1).

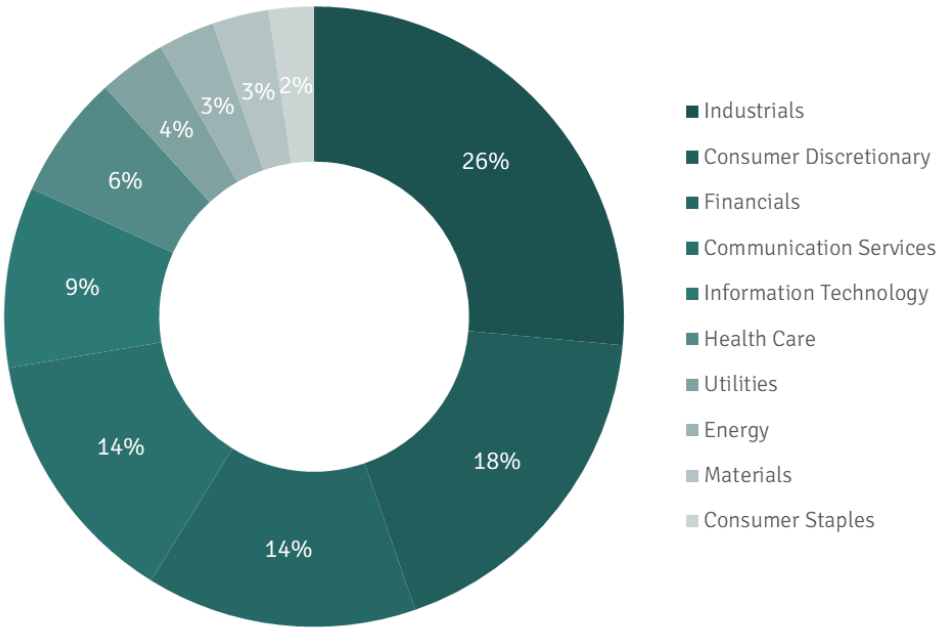

Chart 1: Breakdown of Cybersecurity Incidents per Sector

From a regional perspective within Europe, we also see differences. Chart 2 shows how companies within some countries have been more affected by cybersecurity-related incidents over the past three years. Spain, Portugal, Ireland, Austria, and France are the countries with the highest proportion of companies suffering cyberattacks and data beaches.

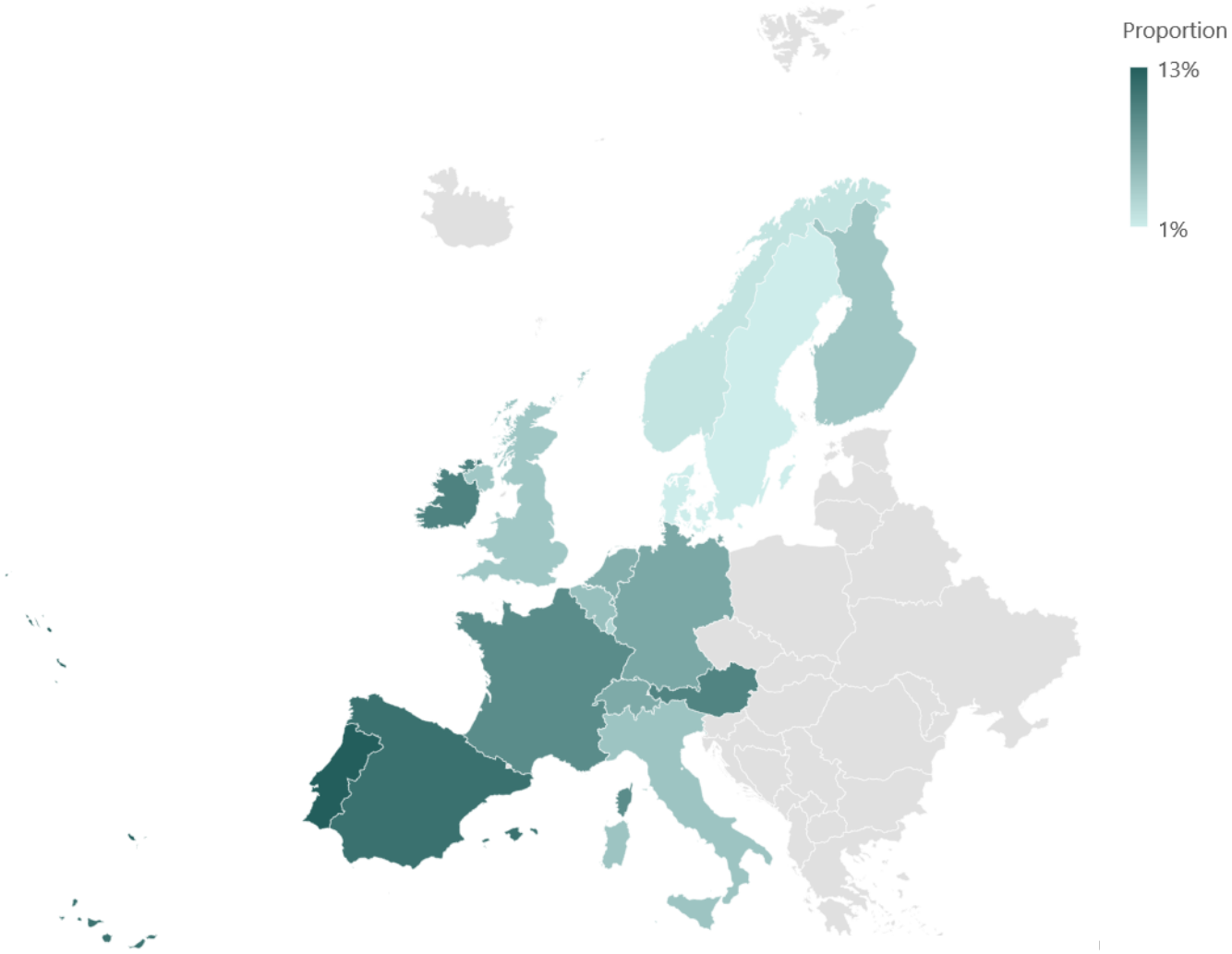

Chart 2: Proportion of cybersecurity-related controversies by country

Our controversy data is obviously only the tip of the iceberg, since it merely shows those incidents that have received a certain media coverage. The number of cyberattacks and data privacy violations throughout Europe is much higher and on the rise. However, it underlines the importance of risk management measures to protect companies and their clients from cyberattacks and data breaches.

Cyber Risk in Corporate Risk Management: Smaller Firms Lagging Behind

In our analysis of how companies manage cyber risk, we look at the analysed companies' operational risk management and see if they have included IT and cybersecurity risks. This provides insight into a proactive and systematic way of mitigating potential cyberthreats and protecting digital assets effectively. We have seen a notable increase in the proportion of companies addressing IT risks within their risk management strategies over the last three years – rising from 73% in 2021 to 85% in 2023 (Chart 3).

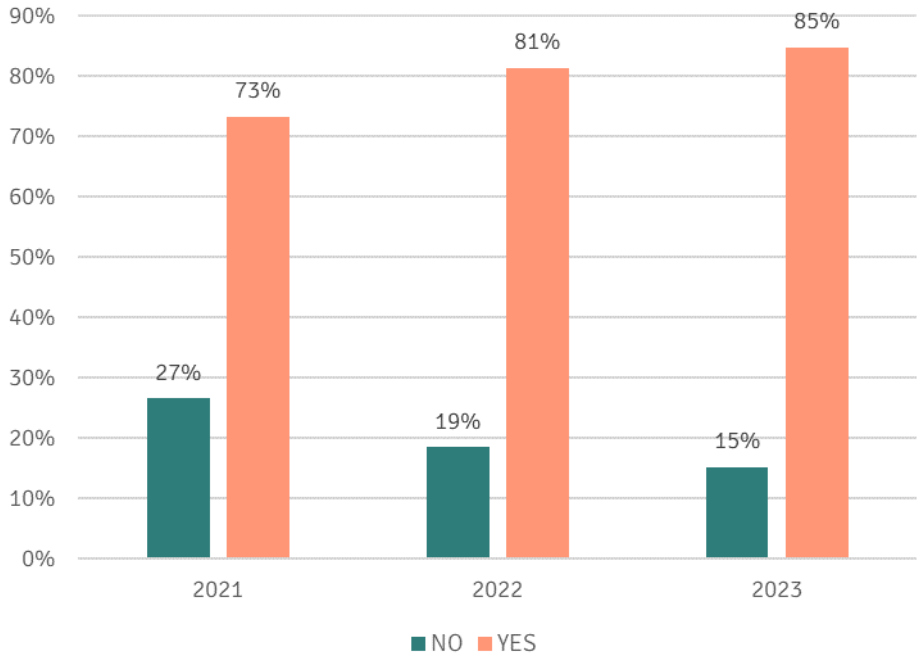

Chart 3: Percentage of Companies including Cyber Risk in Operational Risks

However, our analysis shows that smaller companies trail behind large corporations significantly. While over 90% of large firms have incorporated cyber risks into their operational risk management, this is the case for only 67% of smaller companies. Nevertheless, the 3-year trend shows that the latter are catching up (from 50% in 2021 to 67% in 2023), and cybersecurity management is taken more seriously every year.

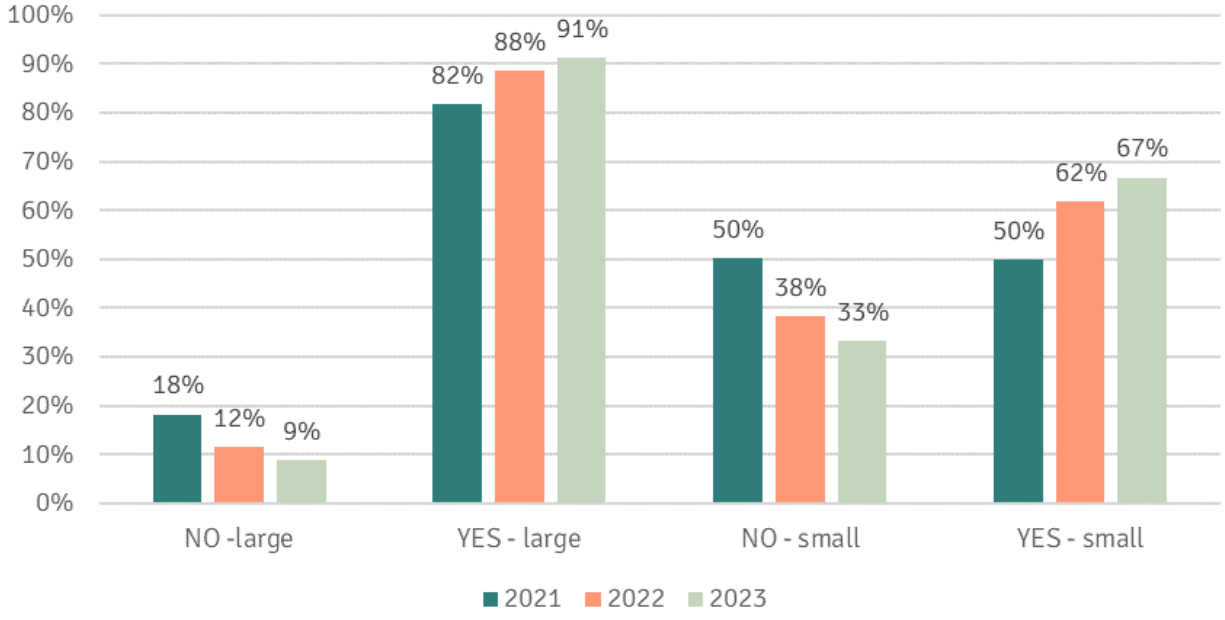

Chart 4: Percentage of Companies Including Cyber Risk in Operational Risks – By Company Size

ISO 27000 Certification: French and Real Estate Companies Late to the Game

The International Organization for Standardization (ISO) has developed the ISO 27000 certifications as part of a solution to improve companies' information security management system (ISMS). These certifications evaluate a company's ability to implement, operate, monitor, review, maintain and improve its ISMS through a process-based approach. To qualify for one of the certifications, the ISO standards must comprise several elements such as an effective assessment of information security risks completed with a risk mitigation process. In addition, the company must showcase the existence of a security controls framework and a plan to foster continuous improvement to refine security measures through regular reviews and audits.

Based on our data, we observe that most of those companies providing the information (25% of all companies analysed), have obtained the ISO 27000 certification in most European countries. The notable exception is France, where only 33% of companies were certified in 2023.

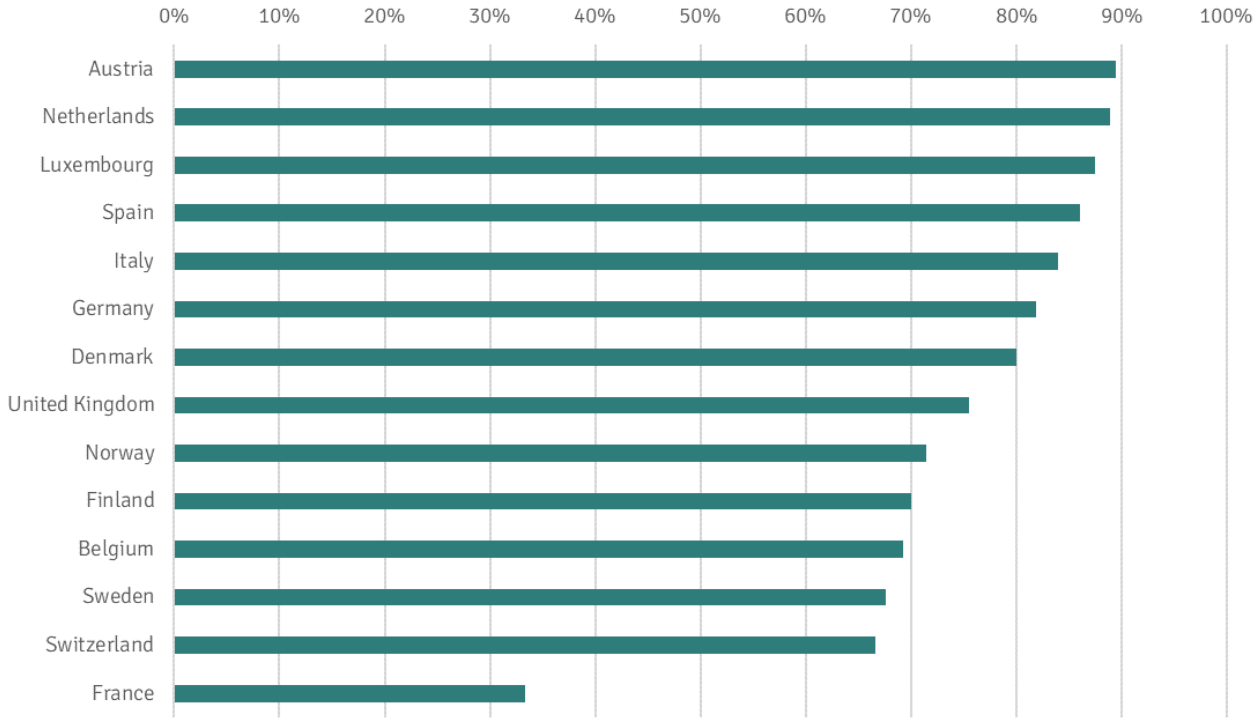

Chart 5: Proportion of Companies Certified ISO 27000 in 2023

From a sector perspective, we see even stronger disparities (Chart 6). While Utilities, IT, and Industrial companies and financial institutions show the highest proportion of ISO 27000 certification, the Real Estate sector stands apart with a particularly low certification rate.

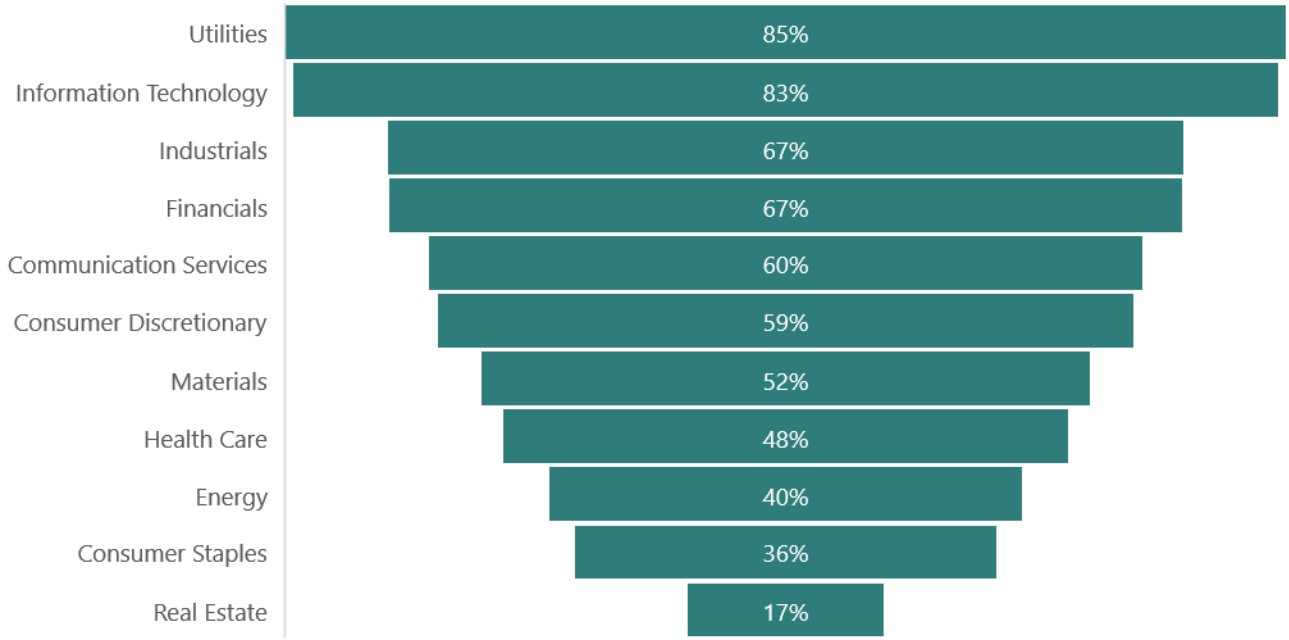

Chart 6: Proportion of ISO 27000 Certified Companies by Sector

Employees Cybersecurity Training: Modest Reporting and Low Employee Coverage

Providing cybersecurity training to employees is one of the fundamental ways in which companies can prevent cyber risks, as intruders often use phishing emails or similar ways to obtain system entry by human error. We have thus included this question in our analysis. However, obtaining this data has shown to be challenging as companies do not systematically report the percentage of their employees trained on cybersecurity. In 2023, only 16% of the companies in our ESG Rating universe provided this information, which is still a slight increase compared to 2020 (up from 6%).

Among the companies who did provide the information, we also see a slight improvement (Chart 7). In 2023, almost half of the companies reporting on the topic, have provided training to all of their employees and over one quarter have a high training coverage.

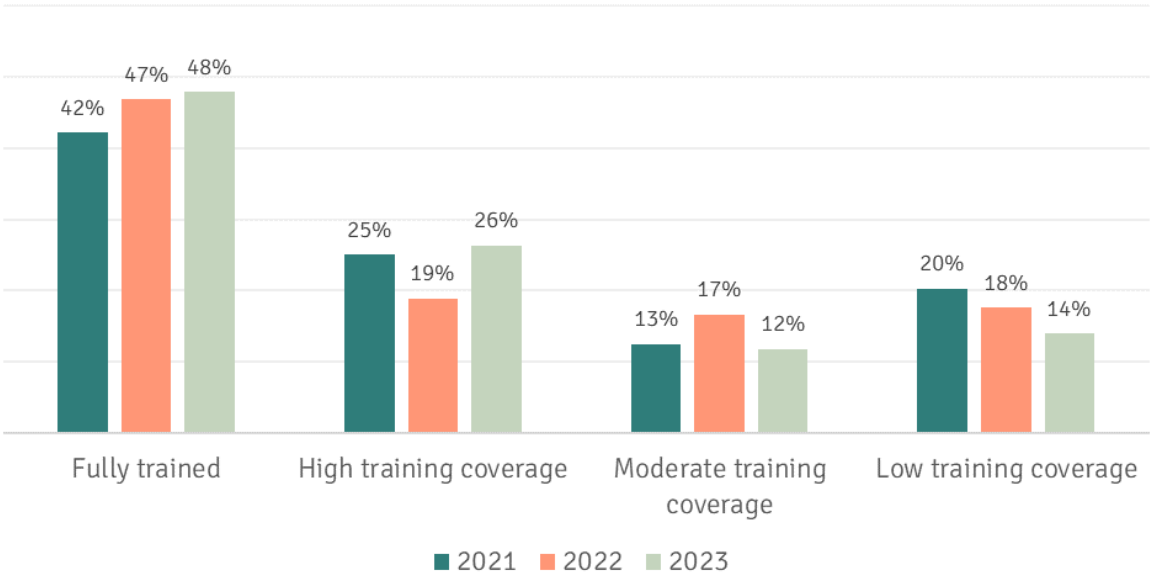

Chart 7: Proportion of Employees Trained on Cybersecurity

Intrusion Tests: A Widely Used Tool

Another fundamental tool for ensuring cybersecurity within an organisation are intrusion tests. These are simulated cyberattacks, allowing for a real-life assessment of the solidity of cybersecurity systems the organisation has put in place. Among the 55% of companies within our rating universe that report on the use of these tools, 97% have carried out intrusion tests in 2022 (Chart 8). This percentage has only slightly increased over the last three years, with an already very high percentage (95%) in 2020.

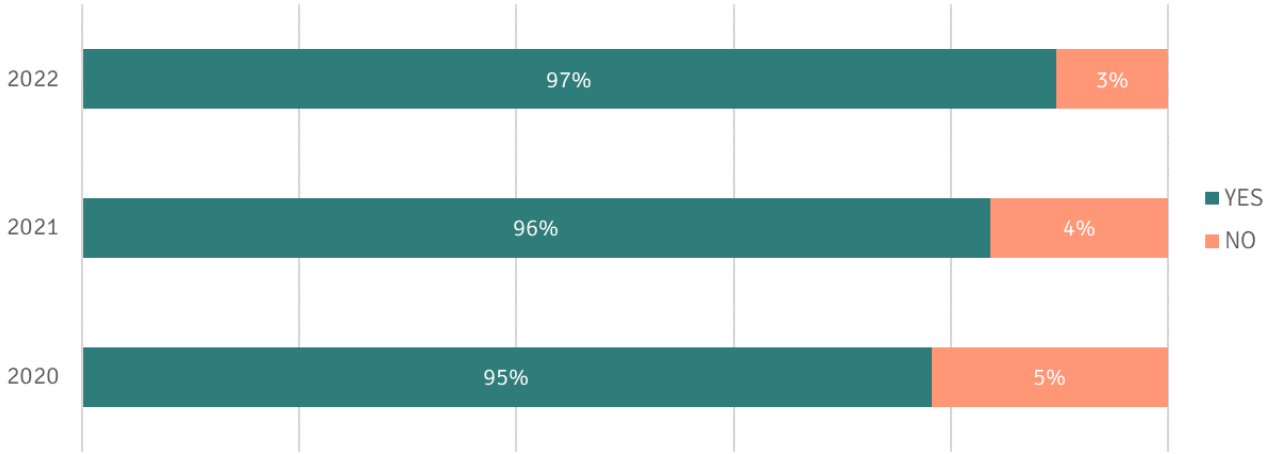

Chart 8: Proportion of Companies Undertaking Intrusion Tests

Overall Cybersecurity Scores on the Rise

When combining the different parts of our cybersecurity analysis – the four single indicators as well as the controversy analysis, we obtain an overall score expressed on a scale from 0 to 100, indicating how an organisation manages its cyber risks. Chart 9 shows how the average cybersecurity score has increased over the past three years from 57/100 to 70/100, underlining the improvement of the overall maturity of companies in managing cyber risks.

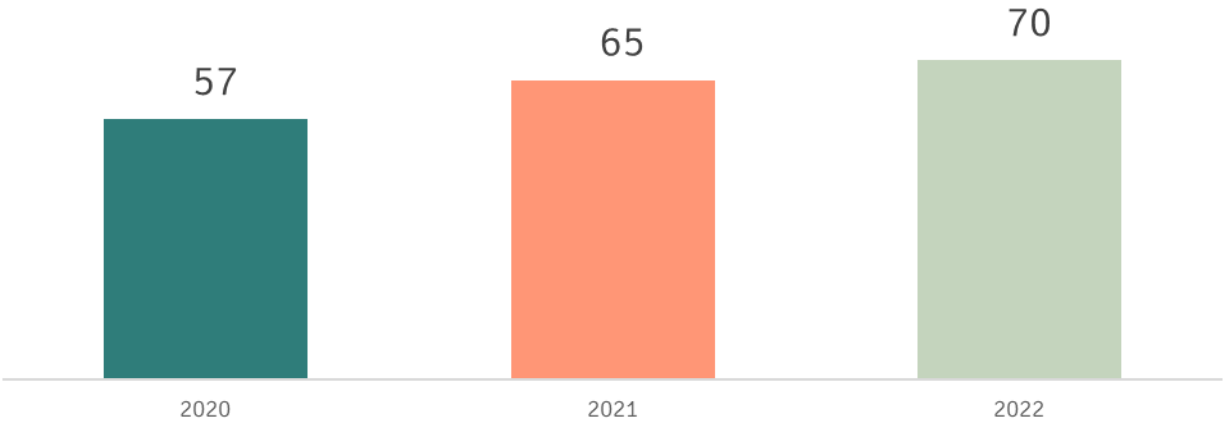

Chart 9: Average Cybersecurity Scores Across European Companies

The comparison of average scores across Europe shows a varying situation (Chart 10). Austria is the country with the highest average score of companies, followed closely by the Netherlands, Ireland, and France. Countries with the lowest average scores are Switzerland, Sweden, and Norway.

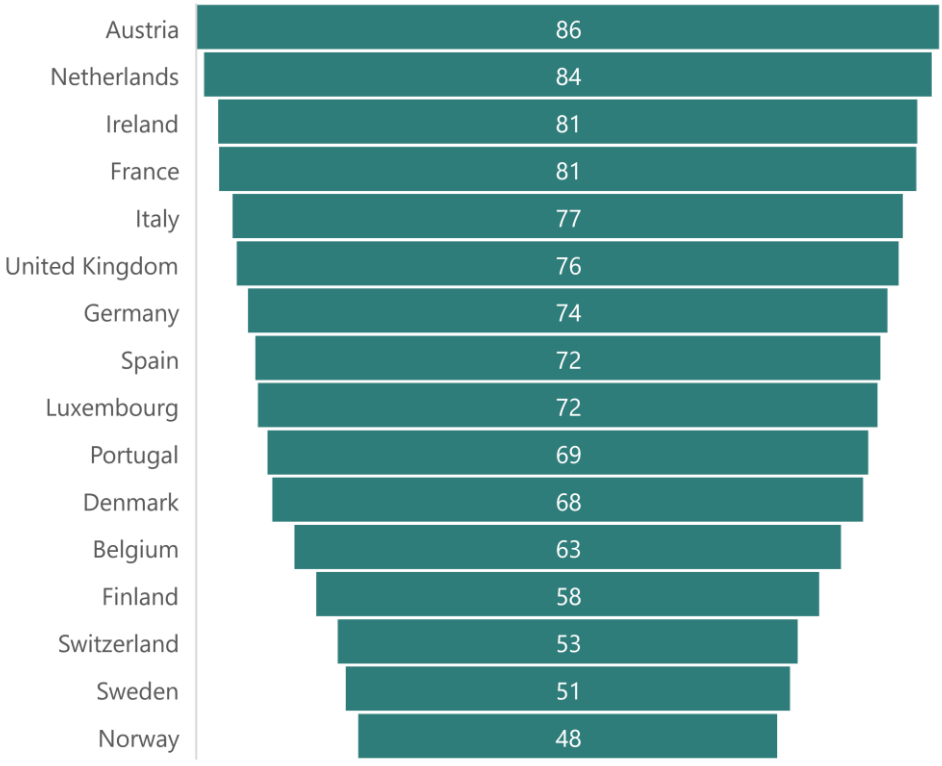

Chart 10: Average 2023 Cybersecurity Scores by Country

Conclusion

Overall, our analysis shows that cybersecurity, a most threatening risk for organisations, is being taken increasingly seriously by European companies. While cyberattacks and data breaches continue to happen, firms tend to equip themselves with adequate tools for preventing future intrusions and leaks. However, while the topic is clearly on the rise, we still see a lack of reported data by companies across Europe, which does not allow for a complete analysis in all areas. Nevertheless, it is worth noting that the enforcement of new regulations in the coming years will force companies to be better equipped in relation to cybersecurity threats sparking increased transparency in their reporting practices. As an ESG Rating agency, we are also looking to adapt our cybersecurity assessment methodology over time to reflect these new developments.