REPORT

# Europe’s Top 100 Companies:

# Cybersecurity Threat Report

SecurityScorecard

# Introduction

With the EU's Digital Operational Resilience Act (DORA) deadline looming on 17th January, 2025, Europe's top 100 companies face an urgent cybersecurity challenge. Despite the high stakes, many organizations lack effective ways to measure their risk, effectively leaving them exposed and 'flying blind.'

SecurityScorecard changes that. With an A-to-F rating system based on continuous threat intelligence, it gives companies an instant snapshot of their cyber resilience. This matters: companies with an F rating are 13.8x more likely to suffer a breach than those with an A. In the digital age, a poor cybersecurity score is as risky as a poor credit rating.

Financial entities such as banks, insurance companies, and investment firms will all need to ensure that the European financial sector is able to maintain resilience during severe third-party operational disruptions.

This report analyzes the cybersecurity of the top 100 companies in Europe by market capitalization.

As the saying goes, "What you can't measure, you can't improve." Several years after the ransomware attack that shut down the Colonial Pipeline, the world still lacks a standard framework to measure cyber risk. SecurityScorecard instantly calculates a precise measurement of cybersecurity risk with an "A" through "F" letter-grade rating system using continuously monitored threat intelligence data.

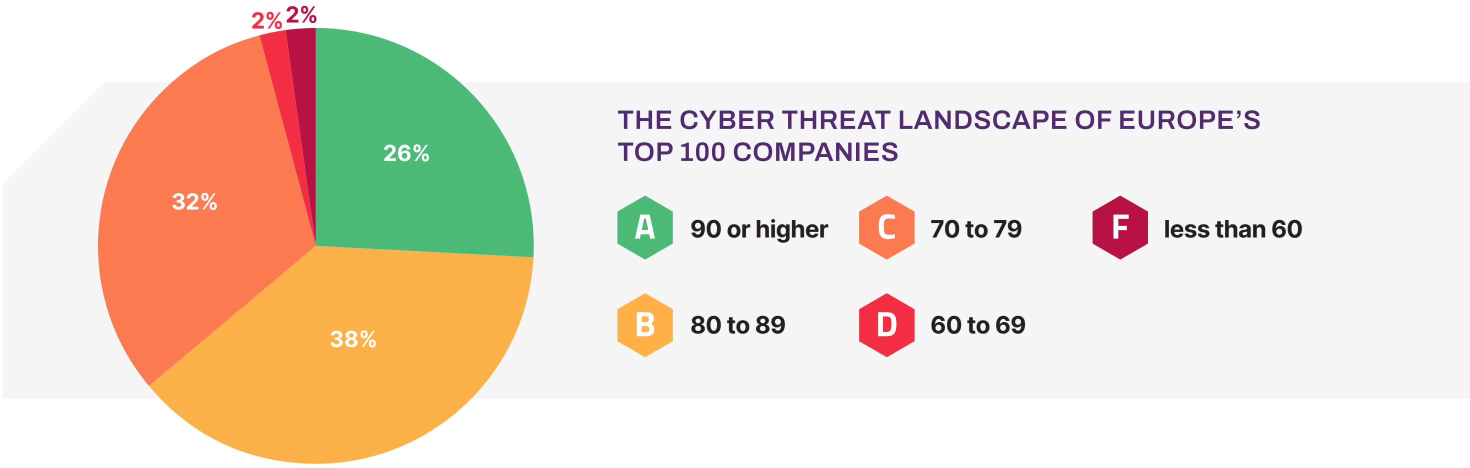
Just as a poor credit rating is associated with a greater probability of default, a poor cybersecurity rating is associated with a higher probability of sustaining a data breach or other adverse cyber event. Organizations with an F rating have a 13.8x greater likelihood of a data breach than companies with an A rating. SecurityScorecard ratings deliver a universal language for cybersecurity.

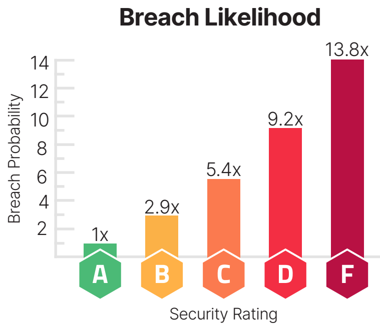
# Key Findings

SecurityScorecard evaluated Europe's top 100 companies based on critical cybersecurity factors such as network security, malware infections, endpoint security, patching cadence, application security, and DNS health. The findings reveal significant vulnerabilities:

- **98%** had a breach in their third-party ecosystem in the last year
- This is the top end of our analysis of European cybersecurity
- **98%** had a breach in their fourth-party ecosystem in the last year too
- **100%** of the European companies with an A grade have not been breached in the last year (demonstrating the importance of having an A grade)
- **36%** had a C rating or below
- The average for UK, France, Germany, Italy and Scandinavia is **31%**
- **18%** have suffered a direct breach in the last year
- Only **24%** of the top 25 companies by market cap have a rating of C or below compared to **36%** of the bottom 25 companies
- The Transport sector is the most robust with all of the companies in it scoring a B or higher compared to the Energy sector in which **75%** had a C rating or below

## Results





**13.8x**

Companies with an F rating are 7.7x more likely to suffer a data breach versus those with an A rating.

> *"The average global cost of a data breach is $4.5M"*
>
> -IBM Security,<br>Cost of a Data Breach Report 2023

# SECTOR OVERVIEW

## Supply chain cyber risk

Supply chain vulnerabilities create an all-too-easy point of entry for adversaries to make their way into organizations and networks. Organizations of all sizes are only as secure as their weakest link, which means even the ones that invest large sums into security still face risks from third- and fourth-party vulnerabilities.

Previous SecurityScorecard research found that 98% of companies have a relationship with a third party that has been breached. In this report, sectors with the lowest security ratings have the most complex attack surfaces due to the sheer number of their third, fourth, and nth party vendors.

> "The supplier ecosystem is a highly desirable target for ransomware groups. Third-party breach victims are often not aware of an incident until they receive a ransom note, allowing time for attackers to infiltrate hundreds of companies without being detected. Governments worldwide are set to enforce stricter security regulations in 2025 that place accountability on organizations and their suppliers, demanding higher security standards across the board making monitoring and understanding a company's flaws will become essential."
>
> – Ryan Sherstobitoff, Senior Vice President of Threat Research and Intelligence

## Energy

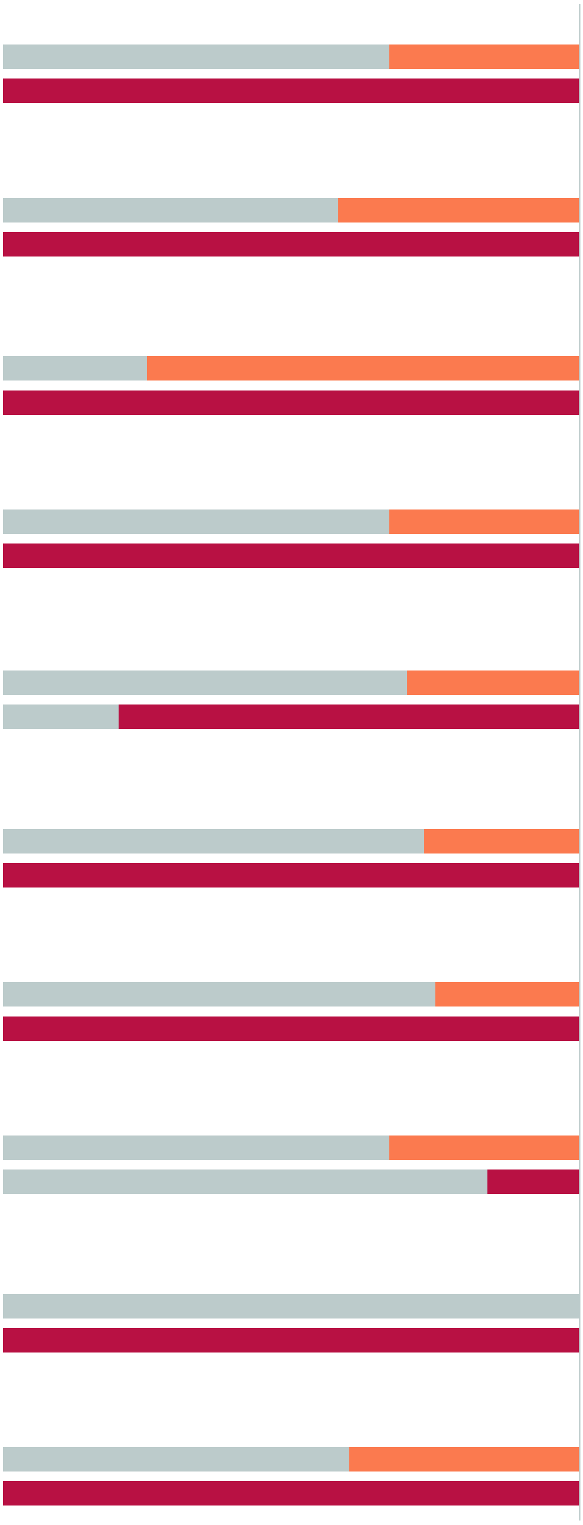
Companies in the Energy sector had the lowest overall security ratings, with an alarming 75% receiving a C rating or below. This is unsurprising, considering that both of these industries have unusually complex attack surfaces, with vast networks of third-party vendors, partners, and service providers. 25% of the energy companies also experienced direct breaches in the last year.

The Energy sector is an integral part of critical infrastructure making them a prime target for nation-state attacks and other threat actor groups. The energy sector's growing dependence on third-party vendors highlights a critical vulnerability — its security is only as strong as its weakest link. Our recent Energy research shows that this rising reliance poses significant risks. It's time for the industry to take decisive action and strengthen cybersecurity measures before a breach turns into a national emergency.

## Transport

The transport sector stands out as the most secure in Europe, with no companies scoring a C rating or lower. Following closely is the technology sector, where only 25% of companies fall into the C rating category or below.

# Scores by Sector



### Basic Materials

**33%** — C rating or below

**100%** have had a third-party breach in the last year

### Consumer Goods

**42%** — C rating or below

**100%** have had a third-party breach in the last year

### Energy

**75%** — C rating or below

**100%** have had a third-party breach in the last year

### Financial

**33%** — C rating or below

**100%** have had a third-party breach in the last year

### Healthcare

**30%** — C rating or below

**80%** have had a third-party breach in the last year

### Industrial

**27%** — C rating or below

**100%** have had a third-party breach in the last year

### Technology

**25%** — C rating or below

**100%** have had a third-party breach in the last year

### Telecommunications

**33%** — C rating or below

**16%** have had a third-party breach in the last year

### Transportation

**0%** — C rating or below

**100%** have had a third-party breach in the last year

### Utilities

**40%** — C rating or below

**75%** have had a third-party breach in the last year

## Score comparison by country

The interconnected nature of today's digital landscape means that cybersecurity issues extend far beyond national borders and individual networks, presenting a global challenge. This makes collaboration and information sharing between governments, industries, and organizations crucial for building collective cyber resilience.

This report centers on the top 100 companies in Europe, but past analyses of leading companies in Germany, Italy, France, the UK, and Scandinavia provide deeper insights. Scandinavian companies have demonstrated the strongest overall cybersecurity, with only 20% rated C or below. In comparison, the figures are higher for the UK (24%), Germany (34%), France (40%), and Italy (41%).

France, however, stands out for a different reason: it has the highest rate of third- and fourth-party vendor breaches, at 98% and 100% respectively. These rates surpass those of the UK, Germany, Italy, and Scandinavia, highlighting a significant vulnerability in managing supply chain security.

SecurityScorecard's recently released Global Third-Party Cybersecurity Breach Report underscores why these findings are so pressing. The report reveals that 75% of third-party breaches target the software and technology supply chain, a trend reinforced by recent high-profile breaches involving SolarWinds, Log4j, and MOVEit.

## Cyber risk concentration: A growing concern

According to the Global Cyber Resilience Scorecard, ten threat actor groups are responsible for 44% of global cyber incidents—with the C10p cybercrime group being the most prolific perpetrator of third-party breaches.

The fact that a few groups are behind such significant disruptions raises serious concerns about concentrated risk in the global economy.  "Redefining Resilience: Concentrated Cyber Risk in a Global Economy," with knowledge contributions from McKinsey and Company, looked at this very issue. A striking finding is that just 15 companies dominate 62% of the global technology market.

Because of their large influence, these companies have greater potential to inflict third-party harm on their customers due to their extremely large market share and vast attack surfaces. These vulnerabilities are the root of many recent, high-profile supply chain attacks that have crippled critical industries. One example of this is the cyberattack on Change Healthcare, a major medical claims processor in the United States. The February 2024 attack forced Change Healthcare to disconnect over 100 systems, pushing many providers to the brink of closure.

# Benchmarking across Europe

### Top 100 companies breached in the last year

**3%** of Scandinavian companies

**7%** of French companies

**12%** of UK companies

**8%** of German companies

**3%** of Italian companies

### Top 100 companies with an A grade that has not been breached in the last year

**100%** of Scandinavian companies

**88%** of French companies

**95%** of UK companies

**100%** of Italian companies

**100%** of German companies

### Top 100 companies with a breached entity in their third-party ecosystem

**98%** of Scandinavian companies

**98%** of French companies

**97%** of UK companies

**95%** of Italian companies

**94%** of German companies

> “The urgency for harmonization has reached a tipping point. In response to these mounting challenges, there will be a growing push for greater regulatory harmonization in 2025. Governments, international organizations, and industry bodies will unite to create consistent standards and frameworks that can be adopted globally, particularly among the United States, Canada, Australia, and across Europe.
>
> Third-party risk management is a key component of any robust cybersecurity program, and the companies represented in this report would benefit by making it a priority. The sectors and organizations in Europe (and in Europe as a whole) need to do more now if they are going to be ready for the implementation of DORA [Digital Operational Resilience Act] by January 2025 as well as the NIS2 directive.
>
> “The rise of data breaches across Europe demonstrates that European companies need to make third-party risk management (TPRM) an integral component of not only their security program but of their vendor selection process as well.
>
> SecurityScorecard can help with this effort by providing ratings to evaluate prospective vendors and monitor existing vendors to hold them accountable.”
>
> - Jeff Le VP, Global Government Affairs & Public Policy at SecurityScorecard

## Supply chain risk extends beyond third parties

While third parties typically receive most of the supply chain scrutiny, fourth-party vendors also create significant risk.

This report shows that 98% of the companies have a breached entity in their third-party ecosystem. Further analysis also shows that 98% of Europe's top companies have a breached entity in their fourth-party ecosystem. These threats underscore the importance of identifying and assessing the security posture of all Nth parties in a company's digital ecosystem.

The potential impact of these breaches is clear from recent events. The MOVEit exploit, discovered in the spring of 2023, continues to disrupt operations and cause financial strain, with projected costs exceeding $65 billion USD.

## Further market capitalization insights

Our analysis found that the top 50 companies by market capitalization (82 Billion plus USD) have higher security ratings than the 50 companies with lower market capitalization. An average of 36% of the companies with lower market capitalization have a C rating or below; while an average of 24% of the higher value companies have a C rating or below. This demonstrates that any company—regardless of size, industry, value, or revenue—can be a target for cyber criminals if it doesn't have strong cyber defenses.

Globally, however, there appears to be a correlation between a country's cyber risk exposure and its GDP. The aforementioned Cyber Resilience Scorecard found that a nation's economic prosperity is closely tied to its ability to navigate the complex landscape of cyber threats.

The Middle East, North America, the Pacific, as well as Northern, Western, and Central Europe have the highest security scores in the world. In other words, regions with higher per capita GDP tend to exhibit better cybersecurity hygiene and lower cyber risk.

Considering that Europe (and other countries in Europe) has one of the highest rankings of GDP per capita, it is presumably better equipped to invest in resilient and safe infrastructure and to implement and maintain active security programs to combat the ever-evolving nature of cyber threats. Wealthier countries like Europe may also be more likely to use licensed software that is kept up to date with security patches.

## Securing critical infrastructure is key

A significant portion of the companies in this report are part of critical sectors such as utilities, telecommunications, transportation, and finance. Public trust in the safety of these essential services is vital for society to function seamlessly. Companies in these sectors should take note of the following recommendations to strengthen their cybersecurity posture. For more comprehensive guidance and best practices, refer to SecurityScorecard's 2023 report, "Addressing the Trust Deficit in Critical Infrastructure."

# Recommendations

Improving cybersecurity hygiene is a top priority for many European companies. While most received relatively high cybersecurity ratings, nearly all have faced third- and fourth-party breaches, exposing them to significant risks. To reduce these risks and strengthen their cybersecurity stance, SecurityScorecard recommends the following actions:

**Focus on application and network security:** All companies should prioritize improving application and network security. These two aspects are fundamental to safeguarding against a wide range of cyber threats.

**High-risk companies:** The 41% of companies with cybersecurity ratings of a C or below require more urgent attention. In addition to improving application security and network security, these high-risk companies should place special emphasis on:

- DNS Health: Ensure the health and integrity of your Domain Name System (DNS) configurations. Misconfigurations in this critical component can lead to vulnerabilities.
- Endpoint Security: Strengthen the security of all endpoints, including laptops, desktops, mobile devices, and BYOD devices. Identifying and addressing vulnerabilities in these endpoints is crucial.
- Patching Cadence: Establish a consistent and timely patching cadence for your systems, software, and hardware. Frequent updates help mitigate known vulnerabilities.

All companies need to know not only their score, but the factors that influence it. Any company can obtain a detailed report on their score for free from SecurityScorecard.

# CONCLUSION

In cybersecurity, trust and transparency are essential. Yet, many organizations find it challenging to accurately assess their cybersecurity. Our analysis of Europe's top companies highlights the importance of these principles.

Assessing cybersecurity is a continuous effort. Security ratings provide cybersecurity leaders with the insights needed to make informed decisions, strengthen their defenses, and encourage collaboration in an increasingly risky environment.

In this evolving threat landscape, security ratings and third-party monitoring solutions represent a proactive commitment to cybersecurity. Every company in this analysis has the potential to achieve cybersecurity resilience and foster a safer, more collaborative environment.

## Methodology

A dynamic threat landscape requires real-time risk assessment. Cyber risk must be evaluated based on up-to-the-minute data. SecurityScorecard gathers significant amounts of non-intrusive data on the cybersecurity performance of companies around the world. Using this data, we're able to score companies' cyber defenses. We produce an overall score, graded A-F, based on ten factors that are predictive of a security breach.

The report covers the cybersecurity posture of the top 100 companies in Europe by market capitalization from 28th August 2023 to 28th August 2024.

# APPENDIX - WHAT ARE SECURITY RATINGS?

SecurityScorecard provides organizations with a comprehensive view of security posture for companies, including third- and fourth-party risk.

Security Ratings are entirely evidence-based; everything is scored on an underlying and transparent observation, based on scans of the entire IPv4 space. Correlated with incidence data, SecurityScorecard factors provide insight that can help organizations focus on areas that need the most attention to reduce their risk exposure. Here are the ten factors:

- **Network Security** checks for open ports (such as SMB and RDP), insecure or misconfigured SSL certificates, database vulnerabilities, and IoT vulnerabilities.
- **DNS Health** checks for misconfigurations, such as Open Resolvers, and checks for recommended configurations for DNSSEC, SPF, DKIM, and DMARC.
- **Patching Cadence** measures the frequency of updates for an organization’s identified services, software, and hardware.
- **Endpoint Security** measures the versions and exploitability of laptops, desktops, mobile devices, and BYOD devices that access an organization’s networks.
- **IP Reputation** signals are collected by SecurityScorecard’s sinkhole system, which ingests millions of malware signals from commandeered Command and Control (C2) infrastructures from all over the world. Identified infected IP addresses are mapped back to impacted organizations.
- **Hacker Chatter** is collected from underground and dark web locations discussing targeted organizations and IP addresses.
- **Information Leak** consists of compromised credentials that have been exposed as part of a data breach or leak, keylogger dumps, pastebin dumps, database dumps, and other information repositories.
- **Social engineering** involves measuring the use of corporate accounts in social networks, financial accounts, and marketing lists.
- **Cubit Scores** are calculated using SecurityScorecard’s proprietary threat algorithm that measures a collection of critical security and configuration issues, such as exposed administrative control panels.
- **Application Security** utilizes threat intel on exploitable conditions from white hat CVE, black hat databases, and search engine findings

**To learn more and create your free account, visit SecurityScorecard.com**

## ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

**SecurityScorecard.com**
info@securityscorecard.io