REPORT

United Kingdom Top 100 Companies:

Cybersecurity Threat Report

SecurityScorecard

Introduction

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

Historically, there have been very few breach reporting requirements for companies, leaving government officials, policymakers, and investors without key information on cybersecurity incidents. Just as credit scores standardized the financial world, companies have needed a universal framework to measure cybersecurity risk.

If you drive a car, you have the speedometer. At a doctor's office, you have a scale. But with cybersecurity, you're completely flying in the dark.

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. SecurityScorecard ratings deliver a universal language for cybersecurity.

Companies with an A rating are

13X LESS LIKELY

to suffer a cyber incident than those with an F

Key Findings:

The UK's top 100 companies were scored on critical cybersecurity factors, including: network security; malware infections; endpoint security; patching cadence; application security; and DNS health. Through comprehensive analysis of their attack surface and reported breaches, SecurityScorecard data scientists uncovered:

1. **97% had a breach in their third-party ecosystem**
   Compared to 94% of German companies; 98% of French companies; and 95% of Italian companies

2. **97% had a breach in their fourth-party ecosystem**
   95% of German companies; 100% of French companies; and 97% of Italian companies

3. **85% of the UK companies with an A grade have not been breached in the last year** (demonstrating the importance of having an A grade)

4. **24% of companies have a C rating or below**
   Compared to 34% of German companies; 40% of French companies; and 41% of Italian companies

5. **Only 12% experienced a direct breach in the last year**
   Compared to 8% of German companies; 7% of French companies; and 3% of Italian companies

Cybersecurity by Industry

- The Basic Materials sector (mining and raw materials) and then the Energy sectors have the strongest security posture in the UK, with no companies holding a C rating or below
- The Financial sector is the second strongest industry, with only 5% having a C rating or below
- The Communications sectors had the lowest overall ratings, with 70% having a C rating or below
- The Top 25 companies have the best cyber rating, with only 12% holding a C or below, while of the other 75 companies, 28% have a C rating or below.

Results

Overall scores

1. **39%** received an A
2. **37%** received a B
3. **18%** received a C
4. **2%** received a D
5. **4%** received an F

Grade	Breach Likelihood
A	1x
B	2.9x
C	5.4x
D	9.2x
F	13.8x

The average global cost of a data breach is $4.5M.

IBM Security, Cost of Data Breach Report 2023

Sector Overview

Supply chain cyber risk

Supply chain vulnerabilities create an all-too-easy entry point for adversaries to enter 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 ransomware note, allowing time for attackers to infiltrate hundreds of companies without being detected."

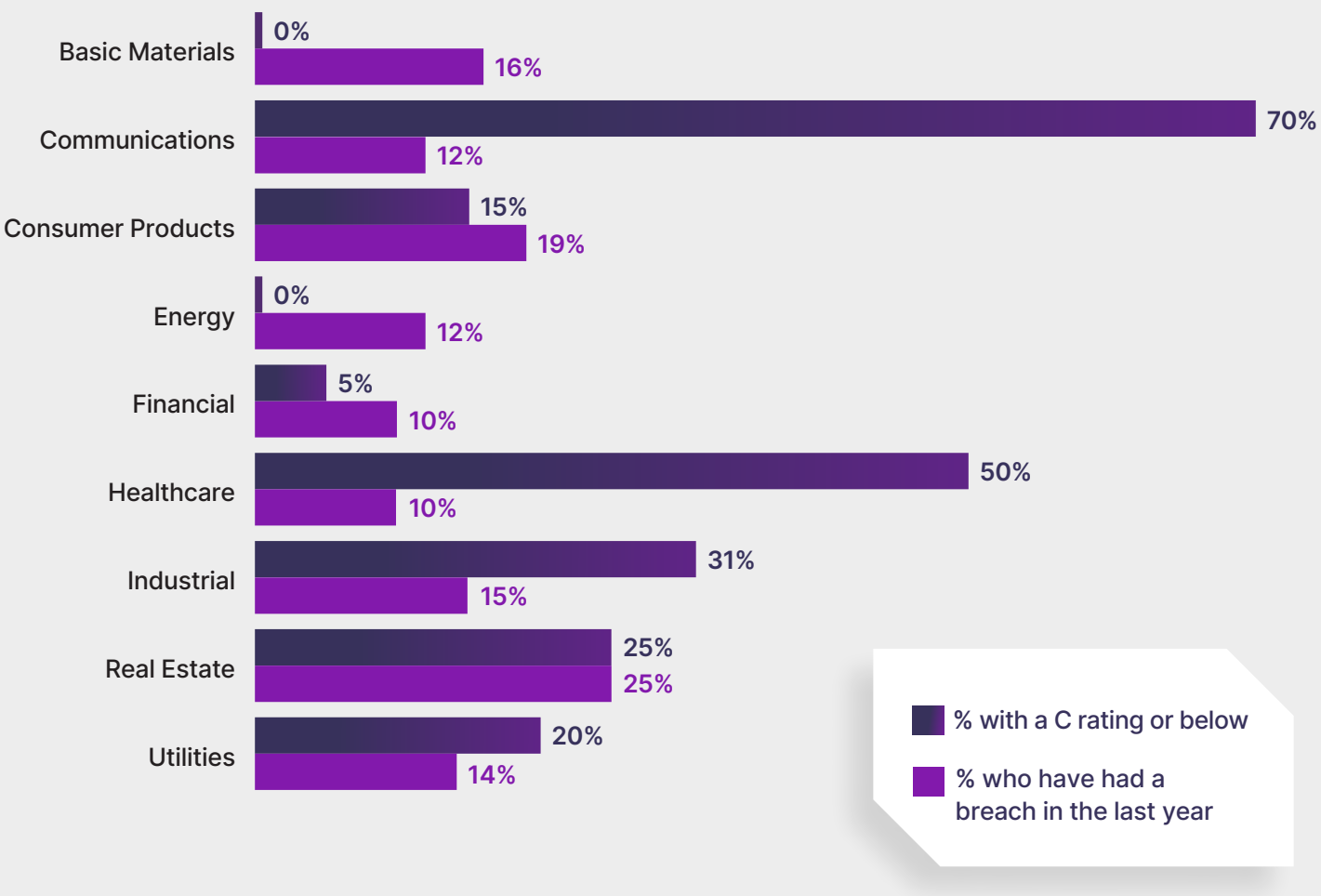
– Ryan Sherstobitoff, S
enior Vice President of Threat Research and Intelligence

Basic Materials

The Basic Materials and Energy sectors (mining and raw materials) have the strongest security posture in the UK, with zero companies receiving a C rating or below. Meanwhile, the Financial sector is the second strongest in the UK, with only 5% of companies receiving a C rating or below.

The Communications sector had the lowest overall security posture, with 70% having a C rating or below. The healthcare sector also has a low cybersecurity posture, with 50% of companies receiving a C rating or below.

Scores by sector



Score comparison by country

The interconnectedness of the digital world means that cybersecurity transcends national borders and a company's own network, posing a global challenge. Therefore, information sharing and collaboration between governments, sectors, and organizations is key to ensuring our collective cyber resilience.

Though this analysis is focused primarily on organizations in the UK, it also examined comparable data from top companies in nearby Germany, France, and Italy. The data shows that companies in the UK have the strongest overall cybersecurity (24% with a C or below) compared to their French, Italian, and German counterparts, with 40%, 41%, and 34% having a C or below, respectively.

Additionally, France has the highest rate of third- and fourth-party vendor breaches (at 98% and 100%, respectively) compared to the UK, Germany, and Italy .

SecurityScorecard recently released the Global Third-Party Cybersecurity Breach Report, which comes at a time when supply chain breaches dominate the news. One key finding from this report is that 75% of third-party breaches targeted the software and technology supply chain. This has been underscored in the last few years, with several high-profile data breaches attributed to 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.

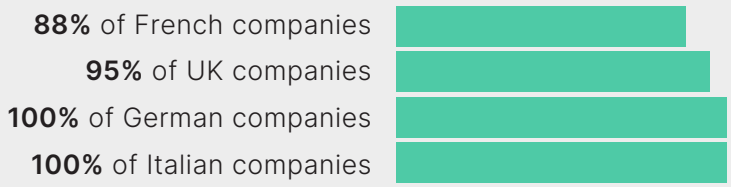
The prevalence of just a few groups being responsible for such large-scale supply disruptions points to much larger concerns about the concentration of risk in the global economy. SecurityScorecard's report, "Redefining Resilience: Concentrated Cyber Risk in a Global Economy," with knowledge contributions from McKinsey and Company, looked at this very issue. The most notable finding to emerge is that just 15 companies control 62% of technology products and services worldwide.

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 devastated 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 the company to disconnect over 100 systems and brought many providers to the brink of closure.

Benchmarking

Companies breached in the last year

Companies with an A grade that have not been breached in the last year



Companies with a breached entity in their third-party ecosystem

"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 the UK (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 UK 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."

- Will Gray, Director of Northern Europe

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 97% of the companies have a breached entity in their third-party ecosystem. Further analysis also shows that 97% of the UK'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.

A vendor experiencing a third- or fourth-party compromise could affect a large number of its customers, or even customers of its customers, in one fell swoop. The MOVEit exploit was discovered in the spring of 2023, and organizations are still dealing with the fallout of the breach, which is projected to cost at least $65B USD.

Further market capitalization insights

Our analysis found that the 25 companies in the UK with the highest market capitalization (over 29 Billion USD) have a stronger cybersecurity posture than the 75 companies with lower market capitalization (5 Billion – 28 Billion USD). Of the bottom 75 companies, 28% have a C rating or below, compared to 12% of the top 25 companies. While more capital does not always translate into better cybersecurity programs, it does provide companies with the resources necessary to invest in robust measures. Any company—regardless of size, industry, value, or revenue—can be a target for cybercriminals if it doesn't have strong cyber defenses.

Globally, 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 the UK (and other nearby economies) 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 the UK may also be more likely to use licensed software that is kept up to date with security patches.

Securing critical infrastructure is key

Roughly forty percent of companies in this report represent critical sectors: utilities, telecommunications, healthcare, and communications. As noted above, 70% of companies in the UK's communications sector and 50% in the healthcare sector received a C rating or below. For society to function smoothly, the public needs to trust that these services and institutions are safe. Companies in these sectors would benefit from the recommendations below. For further guidance and best practices, please read SecurityScorecard's 2023 report, "Addressing the Trust Deficit in Critical Infrastructure."

Recommendations

For many companies in the UK, improving cybersecurity hygiene should be a top priority. Though the majority received relatively high cybersecurity ratings, nearly all companies have experienced third- and fourth-party breaches. To mitigate risk and enhance overall cybersecurity posture, SecurityScorecard recommends taking 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 24% 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 their score and the factors that influence it. SecurityScorecard offers a detailed report on any company's score for free.

Conclusion

Trust and transparency are paramount in cybersecurity. Nevertheless, many organizations struggle to assess their cybersecurity precisely. Our analysis of the top companies in the UK underscores the critical significance of these principles.

Cybersecurity assessment is an ongoing process. Security ratings empower cybersecurity leaders with the insights they need to make well-informed decisions, fortify their security posture, and foster collaboration in the face of an escalating risk.

Amidst the evolving threat landscape, security ratings and third-party monitoring solutions stand as a proactive commitment to cybersecurity. We firmly believe that every company in this analysis has the potential to attain cybersecurity resilience and contribute to a safer, more collaborative world.

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 worldwide. 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.

Analysis Period:
The report covers the cybersecurity posture of the top 100 companies in the UK by market capitalization from 13th March 2023 to 13th March 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.

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