Cyber Security Rating – a rising challenge for EU industries

March 2025

Cyber rating has started to become as impactful as financial rating

The financial crash that occurred in the United States in 1837 prompted the need for risk assessment for investors. The power of financial rating agencies in influencing investors has grown in importance over the past decades, due to a number of significant events (the collapse of Enron in the US; the US Subprime mortgage crisis; the late 2000 financial crisis; and the Greek national debt crisis). Following an increased number of complaints and a significant impact of such agencies, this has led to the creation of the European Securities and Markets Authorities (ESMA) in Europe. Since 2010, credit rating agencies therefore need to comply with ESMA rules.

Nowadays, cyber rating is gaining prominence, paralleling the significance of financial rating. In 2015, Standard and Poor's was the first agency to announce that it was taking cyber risk into consideration when calculating its rating. Cyber rating initiatives in general have been booming over the past five years and there are now several, mostly US-based vendors that produce cybersecurity ratings, such as Security ScoreCard, BitSight, FortifyData, Panorays, VisibleRisk etc.

The momentum has further accelerated through significant investments and acquisitions. For example:

- In September 2021, business and financial services company Moody's announced a $250 million investment in cybersecurity ratings company BitSight; in turn, BitSight would acquire VisibleRisk, a cyber risk rating joint-venture created by Moody's and Team8, a global venture group. Moody's investment was intended to create an integrated cybersecurity risk platform. In April 2024, BitSight and Moody's launched a new cyber risk solution 'Implied Cyber Threat (ICT) covering the rating of more than 325 million organisations.

- In September 2024, Mastercard acquired a threat intelligence firm Recorded Future for $2.6 billion showing the increased momentum of financial institutions for cyber intelligence and rating.

These developments underscore how businesses increasingly rely on cyber ratings for decision-making. Credit Rating Agencies are looking for KPIs that assess cyber security risk coverage and companies are using these ratings more and more when considering entering into business arrangements; they can influence the decision of a company to work with another. EU governments are also beginning to integrate these cyber ratings into their risk assessments. Developing ratings in our complex and interconnected world is understandable and welcome, as long as the methodologies used are transparent, reliable, and robust, considering their huge business impact especially on EU companies.

Existing rating methodologies should be improved

Since 2020, EU businesses (industry, health, energy, etc.), which all function in the digital world, are increasingly subject to such ratings by these many agencies. But these agencies are performing controls without any mandate and based on what they view from the internet – i.e. without exchanges with the rated ("evaluated") companies. Despite their growing adoption, current rating methodologies behind cybersecurity ratings face

significant shortcomings.

Key Issues and Areas for Improvement

1. **Lack of Engagement with Evaluated Companies**

   Many rating agencies conduct evaluations without direct interaction with the companies being rated. These assessments are often based solely on publicly available internet data, resulting in incomplete or inaccurate analyses.

2. **Absence of Standardization**

   The methodologies used are developed without a standardized approach, leading to inconsistencies and potential inaccuracies in ratings. For instance, some agencies evaluate companies based on a technical scope that is neither validated nor tailored to the organization's actual cyber infrastructure. They often base their assessments on publicly available information rather than on sound, relevant, and appropriately validated data. This lack of a sound methodology causes some of the flaws observed and acknowledged by the GSMA in August 2024[1], as well as by the United States telecommunications and ISP community. The broadband association US Telecom has urged service providers to exclude companies with cybersecurity scores derived from unsound or erroneous methodologies from their assessments[2].

3. **Irrelevant or Misleading Assessments**

   Agencies frequently misidentify the public perimeter of evaluated companies. For example, in the telecommunications sector, agencies may incorrectly attribute vulnerabilities from private customers' IP addresses to the telecom operator itself. This lack of contextual understanding results in ratings that fail to reflect a company's true cybersecurity "cyberhealth".

4. **Flawed Metrics**

   Some agencies assign disproportionate weight to minor vulnerabilities, thus distorting the ratings. This is the case in the evaluation of vulnerabilities related with SSL/TLS protocols. While there is a wide consensus among experts on the little practical relevance of these vulnerabilities due to their theoretical nature, some agencies still continue to assess these vulnerabilities by assigning them the same importance as critical vulnerabilities (e.g.: remote code execution).

These issues lead to inconsistencies and biases that can severely impact industries such as telecommunications, financial services, and insurance. A flawed cyber rating can influence insurance premiums, contract negotiations, and even regulatory compliance, ultimately eroding trust and confidence in companies.

In the specific case of telecommunication network operators, Cyber Rating Agencies cannot correctly identify the public perimeter of the evaluated company and do not know if the assigned public IP ranges are used by the telecom company itself or by its clients. Every single private customer who uses an IP-address provided by the telecom operator is factored in. Security issues with private customers can be very significant, with little possibility for the operator to control and manage them. Therefore, there is no correlation, based on objective data, between the score presented by these agencies and the 'cyberhealth' of an organisation in terms of cybersecurity.

[1] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/cyber-risk-quantification-and-cyber-security-rating-what-about-mobile-telecommunications-service-providers/

[2] https://www.ustelecom.org/enhancing-cybersecurity-scoring-methodologies-a-call-for-improved-accuracy/

Very often, instead of starting by assessing the needs, basing actions on them, and determining the necessary sources of information to carry out the risk evaluation, these agencies do the opposite; they look at what information is available, and they set up a scoring scheme from there.

As a result, for the telco industry sector, critical bias has impacted the accuracy of the cyber rating produced dramatically. As an example, the rating from several agencies lacks comparability as the attack surface can differ from one to another (ex: number of IP addresses considered). Business adoption of such false or incomparable metrics is increasing and EU actors can be faced with several consequential enquiries impacting the confidence of their operations with potential business impacts. For instance, cyber rating used in the context of the insurance ecosystem can adversely impact the insurance cost or at Request-for-Proposal (RFP) phases be used as an unfair decision-making criterion.

Considering that these agencies report on ratings associated with one company to other companies, a bad decision based on an incorrect rating can lead to consequences that go beyond those associated with a decrease in the score, but of a more immediate and operational nature such as access restrictions or interruption of connectivity.

Challenges ahead

Despite these facts, we observe an increase in businesses using such metrics in their day-to-day cyber assessments of companies. Typically, the industry sectors scrutinising our companies include financial services, insurance, mechanical and industrial engineering, ITS, other Telco providers, and likely public administrations. It should be noted that the adoption by the market of such KPIs could undermine the impact and uptake of European cybersecurity certification schemes' efforts, as a makeshift way to address cybersecurity risk assessment needs.

Considering these ratings are seen as equivalent to ratings in other areas more and more (e.g.: credit ratings), they should be subject to similar obligations. Evaluated companies are confronted with situations where these ratings are incorporated into contracts and binding legal documents. This should not be allowed until cyber rating agencies comply with a set of minimum requirements.

Call for a more accurate and transparent framework

From an EU sovereignty perspective, we strongly believe that it is necessary to better monitor the work done by existing cyber rating agencies, in order to enable a more just and fairer framework for EU businesses. For that, a comprehensive debate should be launched with consultation of all relevant stakeholders with a view to **define minimum requirements** as well as those procedures to be followed to assess compliance.

To address these challenges, the EU must take quick action to ensure cybersecurity ratings are transparent and reliable.

1. Transparency and Standardisation

Rating agencies should be required to disclose their methodologies, including:

- How ratings are determined.
- The data sources used and their quality.
- The process for defining the scope of an evaluation.

2. Regulatory Oversight

The EU should establish a registry or certification scheme for cyber rating agencies. This framework would require agencies to meet minimum standards of independence, methodology, and accuracy, verified by a third party.

3. Stakeholder Collaboration

A comprehensive debate involving businesses, policymakers, and rating agencies is needed to define best practices and procedures. This collaboration should aim to create a balanced system that fosters trust and prevents the misuse of cyber ratings.

4. Creation of an EU Cyber Rating Charter

Building on the principles of the Paris Call for Trust and Security in Cyberspace, the EU could develop a charter to govern relationships between rating agencies and the companies they evaluate. Key principles might include:

- A "right to reply" for companies to dispute and correct ratings.
- Methodologies tailored to the specific characteristics of each business.
- Educational initiatives to improve understanding and use of cyber ratings.

These principles are key to building a more transparent relationship between cyber rating agencies and evaluated companies.

Conclusion: Building trust and EU sovereignty in cyber ratings

As cybersecurity ratings become increasingly influential across industries, it is vital to ensure that they accurately reflect the cyber health of organisations and do not undermine EU businesses. By implementing transparent methodologies, establishing regulatory frameworks and fostering collaboration, the EU can lead the way in creating a reliable and fair cyber rating ecosystem.

Until these measures are in place, cyber ratings should not be included in contracts or binding documents. Instead, they should be used as a tool for dialogue and improvement. The EU has an opportunity to assert its sovereignty in this area and ensure that its industries are fairly represented in an increasingly digital world.

For questions and clarifications regarding this paper, please contact **Paolo Grassia**, Senior Director of Public Policy (grassia@connecteurope.org).