September 2021

Cyber Security Rating – a rising challenge for EU industries

Cyber rating is starting 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 increased complaints and impact of such agencies, this has led to the creation in Europe of the European Securities and Markets Authorities (ESMA). Since 2010, credit rating agencies need therefore to comply with ESMA rules.

Cyber rating is now being introduced in continuity with 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 US-based agencies that produce cyber ratings, such as Security ScoreCard, BitSight, Panorays, VisibleRisk etc.[1]

Those credit rating agencies are looking for KPIs that assess cyber security risk coverage. Today, companies are more and more using these ratings when considering to enter into business arrangements; they can influence the decision of a company to work with another. It appears that EU governments are also increasingly working with cyber rating agencies. 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.

Various existing rating methodologies deserve improvement to be accurate, transparent and comparable

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 companies. Further, the methodologies used are developed without any involvement of standardisation bodies.

The ratings produced could be irrelevant due to the fact that the assessment is performed on a technical scope which is not validated, relying on a variety of assets not always relevant. These agencies cannot correctly

[1] On 13 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 ratings joint-venture created by Moody's and Team8, a global venture group. Moody's investment is intended to creating an integrated cybersecurity risk platform.

identify the public perimeter of the evaluated companies. In the case of telecommunication network operators, currently all technical assets are taken into account for a rating and agencies 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. Very often, instead of starting by assessing the needs and based on them, determining the necessary sources of information to carry out the risk evaluation, these agencies do the opposite, they look at which information is available and from there, they set up a scoring scheme. This lack of a sound methodology causes some of the flaws observed.

A good example is 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 eminently theoretical nature. However, some agencies continue to consider these vulnerabilities by assigning them the same importance as, for example, remote code execution vulnerabilities.

As a result, for the telco industry sector, critical bias have been observed impacting dramatically the accuracy of the cyber rating produced. As an example, the rating from several agencies can lack comparability as the attack surface can differ from one to another (ex: number of IP addresses taken into account). 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 RFP phases be used as an unfair decision making criteria. Considering that these agencies report on ratings associated with one company to other companies, a bad decision based on a wrong 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.

The latest Forrester report "The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021" also concludes that "the market is still immature, with several improvements required before it's ready to be considered as a mature, enterprise-ready class of security solutions " and lists some of the main issues currently at stake[2].

[2] As an example, this report mentions that: "Ratings vendors need to go further to validate that the security data points chosen for their models, the weightings of those variables, the type of analysis, and how the machine learning models are trained and tested are also most accurately representing the true risk. Ratings vendors also need to go beyond the internal review by having their models externally validated to further build confidence in what this market delivers." […] "CSR ratings firms need to improve the level of transparency they offer around their dispute resolution procedures and consider implementing an industrywide ombudsman to independently adjudicate on disputes between firms and publish publicly the outcome of these disputes."

Despite those facts, we observe an increase in businesses using such metrics in their day-to-day cyber assessments of companies. It should be noted that the adoption by the market of such KPIs could undermine the European cybersecurity certification schemes' efforts, as a makeshift way to address cybersecurity risk assessment needs.

Considering these ratings are more and more seen as equivalent to ratings in other areas (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 to ensure a more accurate and fair reflection of EU businesses

From an EU sovereignty perspective, we strongly believe that it is necessary to better conceive and control the work done by existing cyber rating agencies, in order to enable a more just and true reflection of 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:

- How? Transparency on mechanisms for setting the ratings and mechanisms to verify;
- What? Transparency on which data is used, quality of this data and how this data is collected;
- Where? Transparency on how the definition of the perimeter of the evaluated companies;
- To whom? Transparency on which data is shared to whom and under which conditions.

The European Union should aim at establishing an official registry or inventory of approved rating companies according to a scheme. In other words, we call for a certification scheme for rating companies, so that there are certain guarantees verified by a third party on the requirements of independence, methodology and solvency, among others. In this way, more control and confidence would be given to the whole ecosystem, preventing non-serious agencies from providing untrusted services.

As a first step, and taking into the account the Paris Call For Trust and Security in Cyberspace[3], notably its principles 7 on cyber hygiene and 9 on international norms, we call for an EU Charter for Cyber Rating between the agencies and the EU companies being subject to these ratings, in order to ensure transparency and trust in cyber rating.

[3] https://pariscall.international/en/

Such a Charter should be based on some fundamental principles, under the monitoring of relevant public bodies in case of litigations, such as at the very least:

- Respect the targeted company's "right to reply" and allow rating rectification and removal rights in case of dispute; If the reliability of the information/rating is not agreed, companies should have the right to have the rating publication corrected or removed.
- Be transparent regarding the methodology, which should be adapted to the specificity of the company subject to the rating, in particular concerning the definition of the scope, controls performed, and risk analysis regarding the facts and rating outcomes to be shared[4].
- Create an understanding and knowledge base between the rating agencies and the actors being assessed and develop education for the use of these indicators.

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

In the meantime, and before these agencies are subject to these minimum principles, we believe that these kinds of cyber ratings should not be incorporated in any contract or binding document. After all, all sectors of the EU industry are or will be impacted by these ratings and we need to ensure EU sovereignty and leadership in this context too. We are happy to actively contribute to further work with cyber rating agencies and policy makers in this field and to the elaboration of such an initiative for the European Union.

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

[4] For instance, a clear procedure should be defined by which these agencies associate a given asset (IP, domain) to a given company.