CONSOB
COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA

PRESS RELEASE

Cybersecurity and listed companies: SEC, ESMA and CONSOB comparing mutual transparency regulations
Ciocca: assessing whether the resilience to hacker attacks should figure in the periodic reporting
U.S. Authority asks for a mandatory, non-discretionary, communication
The point today and tomorrow at the Catholic University

Publicly listed companies should be prepared to release information on *cybersecurity* in their mandatory periodic reporting to the market, due to the interest had by investors in knowing how tough or vulnerable the company in which they invest their money is, with respect to the risk of hacker attacks.

This is the position expressed by Luna Bloom of SEC (*Securities and Exchange Commission*), the U.S. regulatory and supervisory authority on the financial markets, in her intervention at the Conference "*Cybersecurity, market disclosure & industry*", underway today and tomorrow at the *Università Cattolica del Sacro Cuore*.

Cyber risks are growing with their stepping up due to the digitalization of the economy and finance, with strong operational, legal and reputational impacts on listed companies, Bloom observed. The boards of listed companies must hold robust rules and skills, added Bloom, demanding that transparency in the field of cybersecurity must be mandatory and not discretionary.

“Cyber-risk has a potential systemic impact”, observed Paolo Ciocca, CONSOB Commissioner. “The question is not whether to release information, but when and how to release it and what to convey to the market. This places a burden on the Boards”.

"A consistent, comparable and decision-oriented disclosure of information on *cybersecurity* would put investors - commented Elena Beccalli, Dean of the Faculty of Banking, Finance and Insurance at Università Cattolica - in a better position to be aware of risks and incidents".

"The pandemic, the war in Ukraine and the frequent use of outsourced suppliers have increased the threat of systemic risks", observed Alexander Harris of ESMA, emphasizing that collaboration between regulators and other market players is necessary.

For the financial markets of the European Union this would represent a radical change of perspective. Today, in fact, hacker attacks are subject to the transparency regulations of price sensitive events. As a result, they need to be disclosed only if and when the emergency occurs. Furthermore, it is the same company that evaluates whether or not the episode is of interest to the market and when, if necessary, to communicate.

If the proposals of the SEC were also implemented in the EU, the information on *cybersecurity* would no longer become voluntary but mandatory, and it would be subject to the transparency regulations according to predefined criteria valid for all.

Milan, 27 February 2023