CONSOB

Workshop Università Cattolica del Sacro Cuore and Consob

"Cyber Security, Market Disclosure & Industry"

Speech by Consob Commissioner Paolo Ciocca

27 February 2023

EU and cybersecurity in the financial system: how to move from compliance to market levers

- The SEC's proposed new rules mark the turning point toward a new era of cybersecurity: if approved, they will transform market reporting on cyber incidents and preparedness from *voluntary* to **mandatory**, from inconsistent and incomplete to **standardized, consistent, and "decision-useful".**

-The SEC is proposing - in particular with the draft rules directed at public companies that Luna Bloom will explain soon after– to integrate several corporate filings, including annual and quarterly filings and current reports[1] with information regarding, among others:

- material cybersecurity incidents and their impact on the registrant's operations and financial condition (with periodic updates about previously reported cybersecurity incidents);
- policies and procedures adopted to identify and manage cyber risk;
- management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures and strategies;
- the board of directors' oversight of cybersecurity risk and board member cybersecurity expertise

- And SEC is considering applying these new rules to all listed companies, in **a cross sector approach**

- What is the premise of such a push for transparency? What are the risks and opportunities associated with such disclosure? When is it time to inform the market about a cyber attack or preparedness of listed companies and how much should be said? Is it useful for the investor to have this level of detail?

- With this conference we are not giving answers to all the questions, we are not defining a metric, but we can identify a direction and share some general principles.

- The direction the SEC is charting certainly starts from assumptions common to Europe: markets are integrated, infrastructure is often shared, and critical services are provided by the same providers

[1] The proposed rules on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" propose changes to the following current documents: Form 8-K (event-driven disclosure) required of all listed companies when they experience a "material" event that may affect investor decisions regarding the company; Form 10-K (annual financial disclosure) summarizes, annually, the quarterly data that SEC requires companies to file, but does not replace the annual report to shareholders, although some companies have unified the two documents; Form 10-Q (quarterly financial disclosure): three Form 10-Qs are filed each year, one for each quarter except the final quarter which is represented with the 10-K. Through Form 10-Q, therefore, there is a continuous update of the company's accounts.

(e.g. cloud service provider). We are witnessing an increasing reliance of finance on the technological element, almost a tipping of the balance (think decentralized finance, DLT, etc.) with clear predominance of technology players over financial players

- Cyber risk is in today's business models a "structural" risk, of potential systemic impact, no longer relatable to the sphere of operational ones. Not only it has changed in nature, but its assessment (probability and impact) cannot disregard the full awareness of its new "dimension" that is directly related to the infinite amount of data exchanged/archived every day and the relative value associated with it (just think in recent times we speak of *cybecrime as-a service* to indicate the economy based on the sale of stolen data)

- In Europe, this awarness was reflected in the DORA Act, which raised common cybersecurity standards for the entire financial sector and centralized oversight of critical ICT third-party service providers. But DORA does not address the issue of market disclosure

- Here comes, then, the opportunity to discuss cybersecurity and market disclosure; **public disclosure is a market lever**

- Investors and more broadly stakeholders want to understand how much they can trust companies' ability to manage growing cyber threats and how much those threats impact the company's accounts and, therefore, the return on their investments

- This puts an onus on the boards themselves, who need to understand their companies' actual exposure to cyber risk because they will be accountable to the market, CEOs will have to make appropriate proposals and CFOs will have to quantify that risk in terms of cost/profit to the company

- The question, then, **is not whether** to give the information that in the context of an attack is already out, **but when** to give it, **how** to give it, and **what** to tell the market.

- **cyber incidents**: the concept of materiality, which is essentially similar in the American and European frameworks[2], is the benchmark. Information, if assessed by the issuer as price-sensitive, must be made public *as soon as possible* under European rules (Art. 17 reg.to MAR) unless the conditions for delaying such information are met [3].

  SEC is now establishing a maximum public disclosure timeframe (*within 4 business days of cyber incident being determined to be material*), which beyond issues of compatibility with the investigation timeframe of a cyber attack, imposes quick decisions (escalation procedures) on what to say, with consequences in terms of fairness and completeness of the information to be given to the market:

  - which internal and external systems are impacted?

[2] The Information is material if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision

[3] EX Art. 17(4) MAR: An issuer or an emission allowance market participant, may, on its own responsibility, delay disclosure to the public of inside information provided that all of the following conditions are met: (a) immediate disclosure is likely to prejudice the legitimate interests of the issuer or emission allowance market participant; (b) delay of disclosure is not likely to mislead the public; (c) the issuer or emission allowance market participant is able to ensure the confidentiality of that information.

- what are the current and potential material impacts?

- who are the actors involved besides me?

- what are the estimated impacts in economic terms (e.g., loss of profits due to unavailability of data and/or software or theft of intellectual property; potential penalties for theft of sensitive data; costs associated with ransom payment, etc.) as well as reputational (loss of customer trust/long-term financial impact)?

- **Preparedness:** in this case ***what to say*** and ***how to say*** it becomes crucially important because of the strategic and sensitive content of cybersecurity risk management policies and procedures:

  - how much can I disclose about my cyber risk governance strategies or remediation actions, without giving an advantage to hostile actors?

  - how extensive is the business area that I can cover with my cybersecurity risk-strategy? Does this result meet overall investor's expectations?

  - how will I compare to my competitors in terms of cybersec preparedness?

  - how do I give the information about my preparedness without breaching, for example, sensitive data related to my clients' business?

As I said at the beginning, with this conference we do not give answers but can identify general principles.

In the SEC proposals I identify some of them:

- the **timeliness/urgency of sharing information publicly** once it is identified as material, because the interest to be protected is too high and the impact to be managed is too large

- the importance of providing the market with information that is **standardized** so that it is comparable[4] across different parties (the cyber space is cross sector), but also over time (periodic information to the market)

- the importance of **quantifying the cyber risk financially** because it is material to the company's accounts (and the economic system as a whole) and investors' returns.

But I see a wider issue emerging, which is relevant to regulators, both financial and prudential.

In our connected world, and in particular in a financial system which is increasingly relying on tech&data, providing (cyber)secure systems is a part of a more general systemic challenge: how to build a new trust concept.

Trust is, inter-alia, the essence of financial systems and markets. Trust is both integrity of contents and reliability of systems.

[4] The proposal would require registrants to report and disclose cybersecurity information in Inline XBRL format.

That is why compliance, as fundamental as it is, is no longer enough.

Investors are demanding effective reliability of their data, their investments.

And market has to consider this.

Therefore market levers are now needed.