CONSOB

Workshop Università Cattolica del Sacro Cuore e Consob
"Cyber Security, Market Disclosure & Industry"
Intervento del Commissario Consob Paolo Ciocca
27 febbraio 2023

UE e sicurezza informatica nel sistema finanziario: come passare dalla conformità alle leve di mercato

Le nuove regole proposte dalla SEC segnano il punto di svolta verso una nuova era della *cybersecurity:* se approvate, trasformeranno l'informativa al mercato sugli incidenti informatici e sulle *policies* di presidio del rischio *cyber* da volontaria a obbligatoria, da incoerente e incompleta a standardizzata, costante e "utile per le decisioni".

La SEC sta proponendo - in particolare con le *proposed rules* dirette alle *public companies* che Luna Bloom ci illustrerà subito dopo - di integrare l'informativa finanziaria periodica annuale e trimestrale, nonché ad evento[1] con informazioni riguardanti:

- *material cybersecurity incidents* e relativi impatti sui dati finanziari (con aggiornamenti periodici sulle precedenti informative fornite);
- *policies* e procedure adottate per identificare e gestire il rischio *cyber*;
- ruolo e attività concreta del *management* nell'implementare le *policies* e le procedure di *cybersecurity*;
- l'*expertise* specifica in materia di *cybersecurity* dei membri del consiglio di amministrazione e le concrete modalità di supervisione del *cybersecurity risk* da parte degli stessi.

Quale il presupposto di tale spinta alla trasparenza? Quali i rischi e le opportunità connesse a tale informativa? Quando è il momento di informare il mercato su un attacco cyber o sulla *preparedness* delle società quotate e quanto bisogna dire? È utile per l'investitore avere tale livello di dettaglio?

Con questo convegno non diamo riposte a tutte le domande, non definiamo una metrica, ma possiamo individuare una direzione, condividere dei principi di carattere generale.

La direzione che sta tracciando la SEC parte certamente da presupposti comuni all'Europa: i mercati sono integrati, le infrastrutture sono spesso in comune e i servizi critici sono forniti dagli stessi *provider* (es. *cloud*). Stiamo assistendo a un crescente affidamento della finanza sull'elemento tecnologico, quasi a un ribaltamento degli equilibri (si pensi alla finanza decentralizzata, alla DLT, *etc.*) con netta prevalenza degli operatori tecnologici su quelli finanziari.

[1] Le *proposed rules* on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" propongono modifiche ai seguenti documenti in vigore: Form 8-K (informativa ad evento) richiesto a tutte le società quotate quando subiscono un evento "materiale" che può influenzare le decisioni degli investitori riguardanti la società; Form 10-K (informativa finanziaria annuale) riepiloga, annualmente, i dati trimestrali che SEC chiede alle aziende di depositare, ma non sostituisce l'*annual report to shareholders* sebbene alcune società hanno unificato i due documenti; Form 10-Q (informativa finanziaria trimestrale) vengono depositati 3 form 10-Q ogni anno, uno per ogni trimestre eccetto il trimestre finale che è rappresentato con il 10-K. Attraverso il form 10-Q, quindi, c'è un aggiornamento continuo durante l'esercizio sull'andamento dei conti aziendali.

Il rischio *cyber* è negli attuali modelli di *business* un rischio "strutturale", di potenziale impatto sistemico, non più rilegabile alla sfera di quelli operativi. Non solo ha cambiato natura ma la sua valutazione (probabilità e impatto) non può prescindere dalla piena consapevolezza della sua nuova "dimensione" che è direttamente correlata alla infinita mole di dati scambiati/archiviati ogni giorno e al relativo valore ad essi associato (basti pensare che negli ultimi tempi si parla di *cybecrime as-a service* per indicare l'economia basata sulla vendita dei dati rubati).

In Europa questa consapevolezza si è tradotta nel DORA *Act* che ha innalzato gli standard comuni di sicurezza informatica per tutto il settore finanziario, accentrando la vigilanza dei fornitori terzi di servizi critici ICT. Ma il DORA non affronta il tema della *market disclosure.*

Ecco allora l'opportunità di ragionare sull'informazione al mercato in materia di *cybersecurity*; l'informativa al pubblico è una leva di mercato!

Gli investitori e più diffusamente gli *stakeholders* vogliono capire quanto possono fidarsi della capacità delle aziende di gestire le crescenti minacce informatiche e quanto tali minacce impattano sui conti dell'azienda e, quindi, sul rendimento dei loro investimenti.

Questo pone un onere a carico degli stessi consigli di amministrazione che hanno bisogno di comprendere l'effettiva esposizione al rischio informatico delle loro aziende, perché ne dovranno rispondere al mercato, i CEOs dovranno fornire proposte appropriate e i CFOs dovranno quantificare quel rischio in termini di costo/profitto per l'azienda.

La questione, dunque, non è *se* dare l'informazione che, in caso di attacco è già fuori, ma *quando* darla, *come* darla e *cosa* dire al mercato.

Cyber incidents: il concetto di **materialità,** che è sostanzialmente simile nel *framework* americano ed Europeo[2], rappresenta il *benchmarck*. L'informazione, se valutata dall'emittente come significativa ovvero *price sensitive*, deve essere resa pubblica il prima possibile secondo le regole Europee (art. 17 reg.to MAR) a meno che non ricorrano le condizioni per ritardare tale informazione[3].
La SEC sta stabilendo adesso un tempo massimo di informativa pubblica (entro 4 giorni lavorativi dal momento in cui il *cyber* incidente è stato determinato come materiale) che al di là delle questioni di compatibilità con i tempi di indagine di un attacco cyber, impone decisioni rapide (procedure di *escalation*), sul *cosa* dire, con conseguenze in termini di correttezza e completezza dell'informazione da dare al mercato:

- quali i sistemi interni ed esterni impattati?
- quali gli impatti materiali attuali e potenziali?
- chi sono gli attori coinvolti oltre me?

[2] L'Informazione "*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, paragrafo 4, MAR: *L'emittente o il partecipante al mercato delle quote di emissioni può ritardare, sotto la sua responsabilità, la comunicazione al pubblico di informazioni privilegiate, a condizione che siano soddisfatte tutte le condizioni seguenti: a) la comunicazione immediata pregiudicherebbe probabilmente i legittimi interessi dell'emittente o del partecipante al mercato delle quote di emissioni; b) il ritardo nella comunicazione probabilmente non avrebbe l'effetto di fuorviare il pubblico; c) l'emittente o il partecipante al mercato delle quote di emissioni è in grado di garantire la riservatezza di tali informazioni.*

- quali sono gli impatti stimati in termini economici (es. perdita di profitti per indisponibilità di dati e/o *software* o per furto di proprietà intellettuale; potenziali sanzioni per furto di dati sensibili; costi connessi al pagamento del riscatto, etc.) oltre che reputazionali (perdita di fiducia dei clienti/impatto finanziario di lungo termine)?

Preparedness: in questo caso il *cosa* dire *e come* dirlo diventa di cruciale importanza in ragione dei contenuti strategici e sensibili delle *policies* e procedure interne di gestione del rischio *cyber*:

- quanto posso rivelare delle mie strategie di *governance* del rischio *cyber* o delle azioni di *remediation*, senza dare un vantaggio agli attori ostili?
- quanto è estesa l'area di *business* che riesco a presidiare con la mia *cybersecurity risk-strategy*? Questo risultato soddisfa le aspettative complessive degli investitori?
- come dare l'informazione sulla mia *preparedness* senza violare dati sensibili correlati, ad esesmpio, al *business* dei miei clienti?
- come farò a confrontarmi con i miei concorrenti in termini di cybersec *preparedness*?
- come posso fornire informazioni sulla mia *preparedness* senza violare, ad esempio, i dati sensibili relativi all'attività dei miei clienti?

Come ho detto all'inizio, con questo convegno non diamo delle risposte ma possiamo individuare dei principi di carattere generale.

Nelle proposte di SEC ne individuo alcuni:

- la tempestività/urgenza di condividere l'informazione pubblicamente una volta identificata come materiale, perché è troppo alto l'interesse da tutelare ed è troppo ampio l'impatto da gestire;
- l'importanza di fornire al mercato una informazione che sia standardizzata affinché sia comparabile[4] tra soggetti diversi (il *cyber* spazio è *cross sector*), ma anche nel tempo (informazione periodica al mercato);
- l'importanza di quantificare finanziariamente il *cyber risk* perché è materiale per i conti dell'azienda (e del sistema economico tutto) e per il rendimento degli investitori.

Ma vedo emergere una questione più ampia, che riguarda le autorità di regolamentazione, sia finanziarie che prudenziali.

Nel nostro mondo connesso, e in particolare in un sistema finanziario che si affida sempre più alla tecnologia e ai dati, fornire sistemi (*cyber*) sicuri fa parte di una sfida sistemica più generale: come costruire un nuovo concetto di fiducia.

La fiducia è, tra l'altro, l'essenza dei sistemi e dei mercati finanziari. La fiducia è sia integrità dei contenuti che affidabilità dei sistemi.

Ecco perché la *compliance*, per quanto fondamentale, non è più sufficiente. Gli investitori chiedono affidabilità effettiva dei loro dati, dei loro investimenti.

E il mercato deve considerare questo.

Sono quindi necessarie leve di mercato!

[4] L'informazione deve essere in formato XBRL. La proposta richiederebbe ai dichiaranti di segnalare e divulgare informazioni sulla cybersecurity in formato Inline XBRL.