IL SOLE 24 ORE – 21 NOVEMBRE 2025

La cybersicurezza diventa un rischio d’impresa da presidiare al vertice

di Alessandro De Nicola

A inizio novembre Assonime ha pubblicato una circolare (la numero 23) che commenta l’attuazione del decreto legislativo 138/2024 di recepimento della direttiva NIS 2, ridefinendo il governo del rischio di cybersicurezza nelle imprese considerate «essenziali» o «importanti».

L’analisi evidenzia come la sicurezza informatica diventi parte integrante della strategia d’impresa, con obblighi puntuali per gli organi amministrativi e direttivi, presidi organizzativi minimi da implementare e un sistema sanzionatorio graduato. L’Agenzia per la cybersicurezza nazionale (Acn) completa il quadro con determinazioni e Faq che specificano misure, tempistiche e responsabilità.

Il decreto impone, infatti, un cambio di paradigma: il rischio cyber non è un tema tecnico delegabile in via esclusiva alle funzioni It, ma un rischio d’impresa da presidiare al vertice. L’articolo 23 affida agli organi amministrativi e direttivi tre doveri non eludibili: approvare le modalità di implementazione delle misure di gestione dei rischi, sovrintendere alla loro attuazione (incluse le notifiche di incidente) e curare la formazione. L’Acn qualifica questi doveri come obblighi di indirizzo e pianificazione strategica, dunque non delegabili: dal punto di vista del diritto societario abbiamo un’interessante commistione, giacché un’authority amministrativa incide sulle regole di governance influenzando l’interpretazione del Codice civile relativamente alle materie riservate alla competenza del consiglio di amministrazione.

Ne discende che la cybersicurezza entra a pieno titolo nei piani strategici e industriali, nella valutazione periodica dell'adeguatezza del sistema di controllo interno nonché degli adeguati assetti organizzativi all'articolo 2086 del Codice civile.

Questo riposizionamento ha conseguenze organizzative: servono processi, procedure e flussi informativi dedicati, una chiara ripartizione di compiti e poteri e un monitoraggio continuo allineato allo stato dell'arte, con un approccio proporzionale e multirischio. La discrezionalità del Cda, tipicamente ampia sulle scelte organizzative, è qui incanalata in un perimetro normativo definito, che riduce lo spazio persino della *business judgment rule*.

Ai fini informativi vanno comunicati all'Acn i nominativi di tutti i componenti del Cda mentre ai fini della responsabilità valgono i principi del diritto societario: rilievo al ruolo e ai poteri concretamente esercitati, ferma la "alta vigilanza" del plenum.

Nel modello codicistico l'articolo 2381 del Codice civile prevede la figura dell'organo delegato (amministratore o comitato esecutivo) per la gestione operativa della società laddove al Cda restano il potere-dovere di indirizzo, la valutazione dell'adeguatezza degli assetti, la vigilanza informata mediante flussi periodici, nonché l'intervento correttivo e l'eventuale avocazione. Le determinazioni Acn, pur qualificando come non delegabili gli obblighi di indirizzo e pianificazione, ammettono la delega di funzioni per l'attuazione.

È dunque coerente un assetto con delega gestoria a uno o più amministratori e, a valle, deleghe di funzioni a strutture specialistiche, mantenendo al consiglio responsabilità ultima e presidi di controllo.

Peraltro, l'Acn definisce un set minimo di misure che il Cda deve presidiare, approvare e riesaminare periodicamente tra cui la politica di gestione del rischio cyber coerente con la strategia aziendale; il piano di gestione dei rischi e il documento di valutazione; il piano di trattamento, il piano vulnerabilità e il

piano di valutazione dell'efficacia delle misure; i piani di continuità operativa e *disaster recovery*; il piano di gestione degli incidenti e di notifica al Csirt e, infine, il piano di formazione per tutti.

Diventa evidente che con questi doveri la nomina di un responsabile per la cybersicurezza che supporti il Cda nella pianificazione e nel monitoraggio è una leva cruciale di *accountability*.

In quest'ottica, la sicurezza della *supply chain* è parte integrante dell'assetto. Al Cda è richiesto di orientare processi di acquisto e *outsourcing* che incorporino requisiti di sicurezza coerenti con le misure interne, di assicurare la valutazione del rischio cyber delle forniture e l'inserimento di clausole di sicurezza nei contratti con impatto sui sistemi informativi e di rete.

Il Cda sovrintende poi agli adempimenti informativi verso l'Acn, inclusa la registrazione annuale e l'aggiornamento dei dati, e all'intero processo di notifica degli incidenti significativi al Csirt secondo le finestre temporali previste (prenotifica entro 24 ore, notifica entro 72 ore).

Il sistema sanzionatorio combina ammende agli enti e sanzioni interdittive personali in caso di inottemperanza alle diffide dell'Acn, applicabili anche agli organi amministrativi e direttivi. Sul piano civilistico, la mancata predisposizione degli assetti cyber configura una grave irregolarità gestoria; l'inadeguatezza può far emergere responsabilità per violazione dei doveri di diligenza, con attenuazione degli spazi di insindacabilità quando la norma dettaglia contenuti minimi e criteri tecnici.

La circolare chiarisce insomma che la cybersicurezza non è un adempimento settoriale, ma un elemento strutturale degli assetti e del governo dei rischi. Il Cda è chiamato a guidare la trasformazione: integrare la resilienza digitale nei piani, dotarsi di competenze informate, assicurare risorse e flussi per un controllo effettivo e continuo, orientare la filiera contrattuale e tecnologica. È una responsabilità che abbraccia strategia, organizzazione e *accountability*, in cui la qualità della governance fa la differenza tra conformità formale e capacità sostanziale di prevenire, assorbire e gestire il rischio cyber.

Tutto molto bello, se non fosse che i consigli di amministrazione sono lentamente ma inesorabilmente oberati di sempre maggiori responsabilità che rischiano di snaturarne il ruolo di gestore dell'impresa per trasformarlo in uno di *Collective Chief Complience Officer*.