WHITE PAPER

Cybersecurity e compliance:
il rischio informatico nei sistemi di controllo d'impresa



Adamo Brunetti



Martina Salvi



Francesco Maria Froldi



Virginia Todini

Elaborazione a cura di Adamo Brunetti, Martina Salvi, Francesco Maria Froldi, Virginia Todini

White Paper tratto dal webinar del 29 luglio 2026

LUGLIO 2026

Indice

Introduzione **3**

01 **Adamo Brunetti** **4**
Dal rischio predittivo al protocollo cyber: architettura operativa del Modello 231

02 **Martina Salvi** **6**
Compliance integrata e governance dell'innovazione tecnologica

03 **Francesco Maria Froldi** **8**
Cyber risk come rischio trasversale di business e unità di crisi

04 **Virginia Todini** **10**
Cyber incident tra diritto penale e colpa di organizzazione

Introduzione

Il rischio informatico ha smesso di essere una questione esclusivamente tecnica per divenire una variabile della governance d'impresa. Un incidente non colpisce soltanto i sistemi: attraversa i processi decisionali, le operations e la continuità del servizio, e chiama in causa piani normativi distinti ma convergenti, dal D.Lgs. 231/2001 alla NIS2, dal GDPR all'AI Act. I contributi raccolti approdano a una conclusione comune: **la qualità dell'organizzazione, e non la sofisticazione dell'attacco, misura la tenuta dell'impresa. Ne discende che il presidio del rischio cyber si costruisce sul processo reale e si dimostra con evidenze oggettive**.

LE QUATTRO LENTI DELLA MATRICE DI INTERFERENZA

Modello 231 + **NIS2** + **GDPR e AI Act** → **Lettura unitaria dell'evento**

IN SINTESI

Rischio
Dalla valutazione retrospettiva alla capacità prognostica

Organizzazione
Il cyber risk esce dall'IT e diventa materia di governance

Prova
Il Modello si dimostra con evidenze, non con la quantità di carte



Adamo Brunetti

CEO DI CO.DE · COMPLIANCE, ETHIC AND SUSTAINABILITY ADVISOR

01

Dalla valutazione predittiva al protocollo cyber: architettura operativa del Modello 231

> *"L'imprevedibilità della tecnica utilizzata dall'attaccante non elimina la prevedibilità del rischio organizzativo"*

LA DIGITALIZZAZIONE PERVASIVA dei processi decisionali impone un ripensamento del concetto stesso di rischio. L'approccio tradizionale, ancorato alla matrice probabilità per impatto e fondato sull'esperienza passata, valuta ciò che è già accaduto ma non offre strumenti per anticipare scenari inediti. L'intelligenza artificiale sollecita un cambio di rotta verso una valutazione predittiva, in cui **il risk assessment non si limita a fotografare il presente, ma diventa un processo dinamico e continuativo**. La cybersecurity esce così dall'ambito strettamente tecnico per divenire una variabile trasversale della governance aziendale, pur restando intrinsecamente umana: è questa consapevolezza a fondare l'esigenza di un human in the loop che preservi il giudizio professionale.

DUE PIANI CHE SI INTERSECANO MA NON COINCIDONO

RISCHIO INFORMATICO	→	RISCHIO DI RESPONSABILITÀ DELL'ENTE
L'ente subisce l'attacco: rilevano NIS2 e GDPR		**Il digitale è mezzo del reato-presupposto**

Occorre allora distinguere il rischio informatico dell'impresa dal rischio di responsabilità dell'ente. Un attacco esterno può determinare un incidente significativo ai fini NIS2 o una violazione GDPR anche quando l'organizzazione è soltanto vittima; **il D.Lgs. 231/2001 entra in gioco quando un apicale o un sottoposto utilizza, altera, danneggia o sfrutta un sistema, un dato, un algoritmo o un accesso digitale per commettere un reato-presupposto nell'interesse o a vantaggio dell'ente**, rendendo visibile un deficit di organizzazione. Se ne individuano tre forme: **cyber-native**, quando la condotta integra uno dei delitti informatici dell'art. 24-bis del D.Lgs. 231/2001, che comprende anche la falsa od omessa comunicazione di dati rilevanti per il perimetro di sicurezza nazionale cibernetica (D.L. 105/2019); **cyber-enabled**, quando la tecnologia è il mezzo che rende possibile o più efficace un altro illecito del catalogo; **digitale esteso,** quando AI, cloud e fornitori diventano strumenti o moltiplicatori della condotta.

La rilevanza penale si accerta attraverso quattro domande: qual è la condotta digitale concreta; chi agisce e con quale potere organizzativo, deleghe e privilegi applicativi; quale reato-presupposto e quale vantaggio vengono in rilievo per l'ente; quale carenza organizzativa ha consentito o non ha intercettato la condotta. Da qui emerge il metodo di costruzione del protocollo: **una misura tecnica si trasforma in presidio 231 soltanto quando è collegata a un processo sensibile, formalizzata nel Modello, attribuita a un responsabile, verificabile mediante evidenze oggettive, sottoposta a flussi informativi, testata e sanzionabile in via disciplinare**. Il percorso muove dal processo reale e dallo scenario cyber concreto, valuta l'interferenza con NIS2 e GDPR, definisce controlli preventivi, di rilevazione e reattivi con titolare, frequenza, soglie ed escalation, e stabilisce evidenze minime e flussi verso Organismo di Vigilanza, CISO, DPO e vertice.

Le medesime evidenze alimentano valutazioni distinte ma convergenti: attraverso una **matrice di interferenza** l'evento viene letto con le lenti del 231, della NIS2, del GDPR e dell'AI, evitando i due errori opposti: qualificare automaticamente ogni incidente come caso 231 e, all'inverso, ridurre la cybersecurity a un problema meramente tecnico. Tre casi di studio illustrano la traduzione operativa del metodo: l'appaltatore che, con credenziali privilegiate, altera ticket e indicatori SLA per evitare penali; il dirigente che impiega l'AI generativa per produrre reportistica falsa a supporto di finanza agevolata; il fornitore IT che subisce un incidente di filiera mentre un apicale omette la comunicazione all'ACN. I presidi corrispondenti sono, nell'ordine: utenze nominative con MFA e privilegi minimi, segregazione tra chi esegue e chi valida e log inalterabili; inventario dei casi d'uso di AI autorizzati con logging di prompt e output; classificazione dei fornitori per criticità, con clausole su standard minimi e diritto di audit.

Resta la dimensione forward-looking: un sistema fondato esclusivamente sulla frequenza storica è strutturalmente debole, poiché la sua adeguatezza si misura sulla capacità prognostica di intercettare segnali anticipatori e preparare l'organizzazione a eventi ragionevolmente prevedibili. **L'Organismo di Vigilanza non deve diventare un SOC (Security Operations Center) né il gestore della crisi: deve vigilare sull'attuazione del Modello, sui rischi emergenti, sui flussi informativi e sulla remediation, mantenendo indipendenza e capacità critica**.

IN SINTESI

Cyber-native	**Cyber-enabled**	**Digitale esteso**	**Prevedibilità**
Delitti informatici dell'art. 24-bis	La tecnologia come mezzo di un altro reato del catalogo	AI, cloud e fornitori come moltiplicatori della condotta	Non la tecnica esatta dell'attacco, ma il rischio prevedibile



Martina Salvi

COMPLIANCE OFFICER · DATA & DIGITALISATION · AI GOVERNANCE SPECIALIST

02

Compliance integrata e governance dell'innovazione tecnologica

> *"La compliance non deve irrigidire l'organizzazione aggiungendo controlli meramente formali, ma creare l'equilibrio tra innovazione, responsabilità e fiducia"*

LA FUNZIONE COMPLIANCE ha attraversato una metamorfosi profonda: da verifica a posteriori del rispetto delle regole è divenuta un fattore strutturale di governance che accompagna l'innovazione sin dalla progettazione dei processi. In un contesto normativo europeo segnato da provvedimenti quali il GDPR, il DORA, la NIS2 e l'AI Act, l'errore più frequente consiste nel leggere tali normative come compartimenti stagni. Al contrario, **esse costituiscono tasselli di un unico modello di governance finalizzato a costruire fiducia nell'economia digitale**. La fiducia di clienti, autorità e investitori non deriva dalla tecnologia in sé, ma dalla capacità dell'impresa di dimostrare trasparenza, accountability, controlli efficaci e processi affidabili.

LA COMPLIANCE CAMBIA POSIZIONE

VERIFICA A POSTERIORI	→	COMPLIANCE BY DESIGN
Controllo delle regole a valle		**Presente dalla progettazione delle soluzioni**

L'intelligenza artificiale, in particolare, introduce una svolta epistemologica: influenza le decisioni, apprende dai dati e si evolve di continuo, generando rischi diversi rispetto ai software tradizionali. L'esperienza del settore bancario insegna che **le domande cruciali non riguardano il corretto funzionamento dell'algoritmo, ma l'affidabilità dei dati in ingresso, la spiegabilità del risultato all'esterno, l'effettività della supervisione umana e l'imputazione della responsabilità in caso di errore indotto dal sistema.**

Da qui emerge la necessità di una compliance by design che intrecci competenze di business, IT, legal, privacy e risk management fin dalle prime fasi di sviluppo delle soluzioni tecnologiche: adeguare o modificare un sistema già progettato senza aver considerato i requisiti regolamentari risulta complesso, costoso e spesso impraticabile.

La compliance non deve irrigidire l'organizzazione aggiungendo controlli meramente formali, ma **creare un equilibrio tra innovazione, responsabilità e fiducia**. Una governance efficace rende possibile un'innovazione responsabile, ne aumenta la resilienza e rafforza la credibilità verso tutti gli stakeholder, **trasformando la regolamentazione da barriera in opportunità strategica.**

IN SINTESI

Compliance by design
Business, IT, legal, privacy e risk insieme dalle prime fasi

Dati e spiegabilità
Affidabilità degli input e risultato spiegabile all'esterno

Supervisione umana
Controllo umano effettivo e imputazione dell'errore



Francesco Maria Froldi

HEAD OF LEGAL, CORPORATE & COMPLIANCE PRESSO ELIOR

03

Cyber risk come rischio trasversale di business e unità di crisi

> *"Il focus della governance si sposta dalla sala server al Consiglio di amministrazione"*

IL RISCHIO INFORMATICO non può più essere devoluto esclusivamente alla funzione IT, come se un cyber attack riguardasse unicamente i server o i laptop aziendali. Un ransomware o una violazione di dati non bloccano solo l'infrastruttura tecnologica, ma **paralizzano le operations, il commerciale e la continuità del servizio, minando l'essenza stessa del business**. La normativa NIS2 nasce proprio dalla consapevolezza che attacchi a infrastrutture critiche possono determinare conseguenze sistemiche su scala europea, e impone alle imprese di dotarsi di una mappatura dei rischi che trascenda i confini tecnici.

DOVE SI GOVERNA IL CYBER RISK

SALA SERVER **Il rischio devoluto alla sola funzione IT**	→	CONSIGLIO DI AMMINISTRAZIONE **Rischio di business governato dal vertice**

In questa prospettiva il compliance manager non è tenuto a possedere competenze di penetration testing o di ingegneria informatica, ma deve avere piena contezza di ciò che accade in azienda e dialogare costantemente con l'IT per costruire risposte condivise e coerenti. Fondamentale è la **Business Impact Analysis**, ovvero la conoscenza dell'impatto concreto che un cyber risk può avere sui singoli processi aziendali: cosa si bloccherebbe, per quanto tempo, con quali ricadute operative e finanziarie.

La compliance si inserisce come stakeholder trasversale, capace di veicolare il rischio alla governance societaria e di mediare tra esigenze tecnologiche e obblighi normativi. La creazione di un'unità di crisi dedicata agli attacchi informatici rappresenta un presidio irrinunciabile: **essa deve essere dotata di un action plan semplice e immediato, con poteri decisionali chiari e manager responsabili della gestione dell'emergenza**. La documentazione di riferimento deve essere snella ma inequivocabile, indicando chi deve essere informato, cosa comunicare e cosa fare.

Il focus della governance si sposta così dalla sala server al Consiglio di amministrazione: non è più possibile fondare la gestione del rischio sull'assenza di eventi avversi, che è ontologicamente irrealizzabile, bensì **sulla qualità delle decisioni prese e sui presidi attivati per governare un rischio che, per sua natura, rimane sempre superiore a zero**.

IN SINTESI

Business Impact Analysis	Unità di crisi	Qualità delle decisioni
Cosa si blocca, per quanto tempo, con quali ricadute	Action plan semplice, poteri chiari, manager responsabili	Il rischio, per sua natura, resta sempre superiore a zero



Virginia Todini

SENIOR ASSOCIATE AT STUDIO LEGALE AVV. GIUSEPPE IANNACCONE E ASSOCIATI · COMPLIANCE & CORPORATE RISK

04

Cyber incident tra diritto penale e colpa di organizzazione

> *"Il penalista non analizza il malware, ma ricostruisce ciò che hanno fatto le persone: le decisioni, i controlli e i flussi informativi che hanno preceduto l'evento"*

LA PROSPETTIVA PENALISTICA impone un cambio di ottica radicale: quando il cyber incident si è già verificato, l'attenzione non si concentra sulla natura tecnica dell'attacco, ma sulla qualità dell'organizzazione che lo ha subito. **Il penalista non analizza il malware, ma ricostruisce ciò che hanno fatto le persone: le decisioni, i controlli e i flussi informativi che hanno preceduto l'evento**. Il D.Lgs. 231/2001 non rileva soltanto per i reati informatici — accesso abusivo, danneggiamento di dati e sistemi: l'incidente attraversa quasi tutti i processi aziendali e può fungere da acceleratore di altri reati del catalogo.

IL MODELLO 231 DOPO L'INCIDENTE

STRUMENTO DI PREVENZIONE	→	STRUMENTO DI PROVA
Protocolli e policy adottati prima dell'evento		**Evidenze, tracciabilità e controlli periodici**

Si pensi al ransomware che colpisce poco prima dell'approvazione del bilancio, costringendo il Consiglio di amministrazione a scegliere tra il rinvio e l'utilizzo di dati parziali o stimati, con il rischio concreto di false comunicazioni sociali; oppure alla gara pubblica in cui l'indisponibilità della documentazione attestante i requisiti di partecipazione, causata da un attacco, può indurre l'impresa a ricostruzioni documentali fraudolente o a false dichiarazioni alla pubblica amministrazione.

Il diritto penale non pretende l'infallibilità o la capacità divinatoria, ma esige organizzazione: **la cosiddetta colpa di organizzazione non è altro che il giudizio retrospettivo sulla qualità delle decisioni assunte prima dell'evento**. Se un responsabile IT aveva segnalato una vulnerabilità critica e il Consiglio di amministrazione aveva rinviato l'investimento per altre priorità aziendali, il problema diventa inevitabilmente organizzativo, non meramente tecnico.

In sede processuale il Modello 231 si trasforma da strumento di prevenzione a strumento di prova: **non conta la quantità di protocolli e policy, ma la capacità di dimostrare che il Modello vive attraverso evidenze concrete, tracciabilità delle decisioni e controlli periodici**. Le prime ore successive all'attacco sono decisive per la difesa penale dell'ente, poiché è in quel lasso di tempo che si decide se preservare o perdere irrimediabilmente le tracce dei processi decisionali. **Un Modello snello, sostanziale e calato sulla realtà operativa offre una difesa assai più solida di un cumulo di carte mai attuate**, che rischia di fornire al pubblico ministero elementi a carico anziché di esimente.

IN SINTESI

Colpa di organizzazione
Giudizio retrospettivo sulle decisioni assunte prima dell'evento

Le prime ore
In quel lasso di tempo si preservano o si perdono le tracce

Modello snello
Difesa più solida di un cumulo di carte mai attuate

WHITE PAPER

Cybersecurity e compliance: il rischio informatico nei sistemi di controllo d'impresa

COMPLIANCE & DEVELOPMENT

White Paper tratto dal webinar del 29 luglio 2026

LUGLIO 2026

Tutti i diritti riservati