

SALONE DELLA SICUREZZA 2026 · TAVOLA ROTONDA

IL VALORE DELLE INFORMAZIONI

AI e strumenti di analisi per una sicurezza data-driven

Governare il rischio di sicurezza fisica di un Gruppo bancario significant
secondo un modello data-driven

Stefano Piroddi

Responsabile Ufficio Corporate Security

Direzione Information Technology e Security · Servizio Security e Resilience

IL PUNTO DI PARTENZA: UN PROBLEMA DI SCALA

Una struttura di dimensioni contenute presidia un perimetro nazionale, in una fase storica di forte crescita degli attacchi agli asset bancari.

4

staff
Corporate Security

65

banche affiliate
del Gruppo

~1.500

filiali
sul territorio nazionale

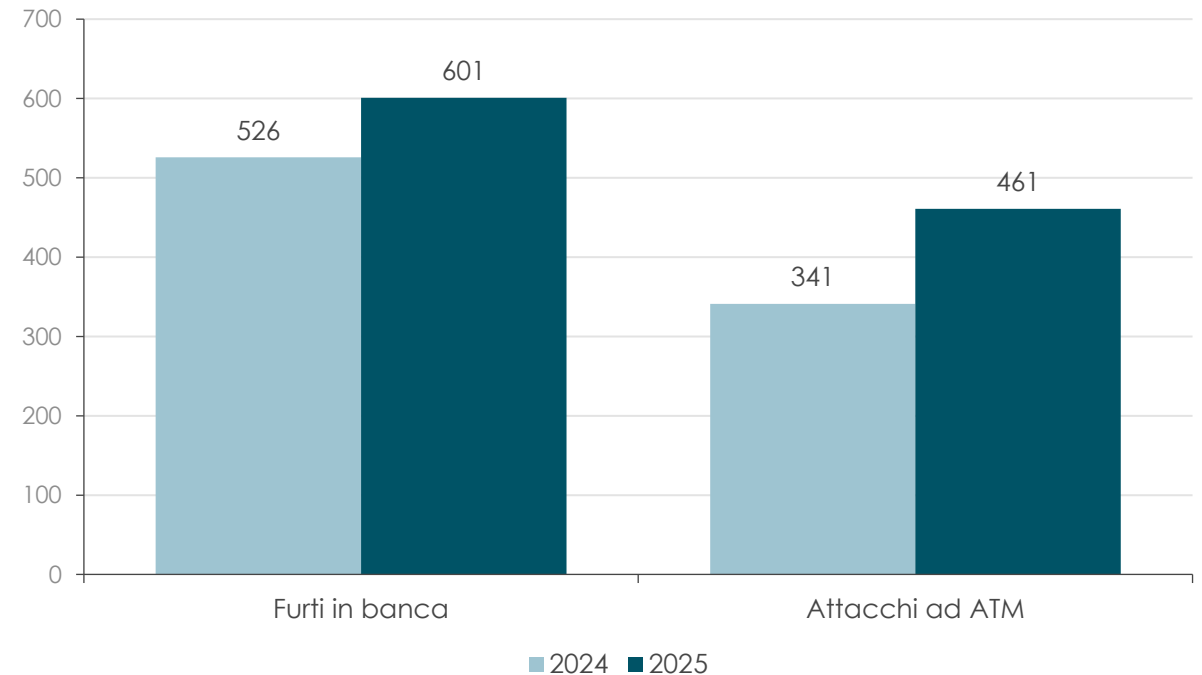
~2.000

ATM, oltre a sedi
principali e secondarie

Un presidio ogni ~900 asset.

A questa scala il controllo diretto perde efficacia: servono metodi comuni e una raccolta dati strutturata per garantire un governo efficace.

Italia — episodi criminosi ai danni delle banche



+14% furti · +35% attacchi ad ATM in un anno. Fonte: OSSIF, Rapporto sui furti ai danni delle banche nel 2025.



IL MODELLO: DUE PIATTAFORME, UN UNICO CICLO DEL DATO

@CSR (Corporate Security Risk) governa il rischio prima dell'evento; la SCR (Security Control Room) governa l'evento mentre accade. Le due si alimentano a vicenda.



L'evento gestito dalla SCR rientra nel calcolo del rischio di @CSR: ogni allarme, ogni intervento e ogni anomalia tecnica diventano evidenza che aggiorna la valutazione dell'asset. È il ciclo che rende il sistema più preciso col passare del tempo, senza aggiungere persone.



@CSR: DAL DATO PUBBLICO AL RISCHIO DEL SINGOLO ASSET

Il tasso di delittuosità in Italia esiste solo a livello provinciale, il modello normalizza su base comunale per ottenere un dato più fruibile per un calcolo su base comunale.

◆ 1 · FONTI

Dati aperti e ufficiali: ISTAT (censimento permanente — densità, struttura demografica, istruzione, occupazione) e MEF (redditi IRPEF comunali, indice di Gini). Nessun dato personale, nessun fornitore proprietario.

◆ 2 · MODELLO

Regressione regolarizzata ElasticNet, addestrata su 106 province (2018-2024) e validata con procedura geografica.

◆ 3 · SCALA

Predizione diretta sul singolo comune, riancorata al tasso provinciale reale. Output: score Minaccia.

◆ 4 · ASSET

Minaccia e Probabilità si incrociano con vulnerabilità (check-list per locale) e impatto (persone, valore dello stabile, valore custodito). Principio dell'anello debole → rischio complessivo e DVR generato dalla piattaforma.

Nella valutazione del rischio di sicurezza fisica, l'esigenza non è solo ottenere una stima affidabile, ma anche poterla motivare e documentare in modo trasparente. Gli esiti dell'analisi confluiscono nel DVR, alimentano i flussi verso l'Organismo di Vigilanza e, in determinate circostanze, possono essere oggetto di approfondimento in sede ispettiva o giudiziaria. Per questo motivo, ogni parametro del modello deve essere comprensibile, verificabile e spiegabile da parte di RSPP, auditor e altri soggetti deputati al controllo. In questo contesto, l'interpretabilità rappresenta un requisito operativo e di governance, oltre che una scelta metodologica.



SECURITY CONTROL ROOM: IL DATO IN TEMPO REALE

Il sistema supporta l'ordinamento e la prioritizzazione delle segnalazioni, ma la decisione finale resta in capo all'operatore. L'obiettivo non è sostituire il giudizio professionale, bensì indirizzarne l'applicazione verso i casi che richiedono maggiore attenzione, contribuendo a rendere più efficace e coerente il processo di analisi e gestione degli eventi.

◆ PRIORITIZZAZIONE AUTOMATICA DELLE SEGNALAZIONI

Il **sistema ordina gli eventi** in base alla tipologia, all'asset coinvolto, all'area geografica e alla concomitanza di più allarmi (macro-evento). **L'operatore** e il Capo Turno **integrano la valutazione** con la criticità dell'asset: sedi principali e filiali con cassette di sicurezza precedono gli ATM remoti, che precedono le sedi secondarie.

◆ LIVELLI DI SERVIZIO MISURATI

Presa in carico immediata dell'evento in PSIM, secondo i requisiti temporali della UNI EN 50518. Pattuglia sul posto entro **tempistiche garantite**. Ripristino dei servizi SCR entro 24 ore. Report giornaliero, settimanale, mensile, annuale.

◆ TRACCIABILITÀ COME PRESIDIO

Profili di accesso differenziati, segregazione delle funzioni, privilegio minimo. Ogni inserimento e disinserimento remoto è registrato in PSIM e nei log dei sistemi della banca. Soglie sugli allarmi ripetitivi determinano trattamenti differenziati delle segnalazioni di allarme.

◆ DAL RUMORE AL SEGNALE

Il valore della control room non è vedere tutto: è **scartare in modo documentato ciò che non richiede una decisione**, e portare all'attenzione umana il residuo. Su un perimetro di migliaia di asset, la pre-analisi con AI è l'unica leva che rende superabile un problema di scala



L'EFFETTO SULLA GOVERNANCE DI GRUPPO DELLA CORPORATE SECURITY

MODELLO TRADIZIONALE

- Valutazione dei rischi redatta sito per sito, con tempi e qualità **disomogenei**
- Controlli di conformità su base campionaria
- Deroghe alle misure di sicurezza negoziate caso per caso
- Nuove filiali progettate su **standard fissi**, indipendenti dal territorio
- Copertura del perimetro proporzionale all'organico

MODELLO DATA-DRIVEN

- DVR generato dalla piattaforma su **metodologia unica, senza incremento di FTE**
- Misure di sicurezza valutate **in funzione del rischio** misurato dell'asset
- Nuove sedi e filiali progettate **con approccio risk-based**
- Copertura dell'intero perimetro, con l'organico impiegato sulle eccezioni;
- Analisi vulnerabilità con **AI** a supporto del decisore.



La piattaforma è messa a disposizione dalla Capogruppo alle banche e società del Gruppo e diventa lo strumento di lavoro standard per la gestione della sicurezza.



QUATTRO LEZIONI DA PORTARE A CASA

Cosa abbiamo imparato mettendo l'analisi dei dati al centro del governo della sicurezza fisica del Gruppo.

1

Il dato senza norma è rumore.

Ogni indicatore che produciamo risponde a un obbligo preciso — D.Lgs. 81/2008, D.Lgs. 231/2001, Circolare ABI 45/2010, DORA. È la norma a dirci quale domanda porre al dato: senza quella, si costruiscono cruscotti che nessuno usa.

2

La scalabilità è governance, non organico.

Un presidio centrale definisce metodologie comuni, ne rende obbligatoria l'adozione, mette a disposizione strumenti operativi uniformi e monitorarne l'applicazione in modo sistematico. In questo quadro, l'automazione e le soluzioni di AI consentono di estendere la capacità di controllo, favorendo verifiche continue e una maggiore coerenza nell'attuazione del modello.

3

L'interpretabilità viene prima dell'accuratezza marginale.

A parità di utilizzo, un beneficio marginale in termini di accuratezza può risultare meno rilevante della capacità di interpretare, documentare e difendere le evidenze generate dal modello.

4

L'AI sposta il collo di bottiglia dall'analisi alla decisione che rimane sempre umana.

Quando il rischio è calcolato per tutti gli asset, il vincolo non è più la disponibilità dell'informazione, ma la capacità dell'organizzazione di assumere decisioni e sostenere le relative responsabilità.



Grazie per l'attenzione

Sede legale e Direzione Generale

Via Segantini, 5 - 38122 Trento

Tel. 0461.313111

gruppocassacentrale.it