Marco di cosa vuoi che parli?

Pier parla delle soluzioni di sicurezza del ….FUTURO….

Cyber Vs. Physical SECURITY

Record per il mercato italiano della cybersecurity nel 2023: 2,15 miliardi di euro, +16% rispetto al 2022;
La cybersecurity si conferma principale priorità di investimento nel digitale in Italia;
Il rapporto tra spesa in cybersecurity e PIL in Italia si attesta allo 0,12%, in crescita rispetto al 2022 (era pari allo 0,10%) etc. etc..

Ecco i principali concetti che si possono trovare sul web e di cui si parlerà in questi due giorni a banche e sicurezza

ma….

Questo grafico e queste definizioni sarebbero andate benissimo anche per rappresentare la crescita esponenziale delle spese di sicurezza fisica fino ai primi anni 2000.

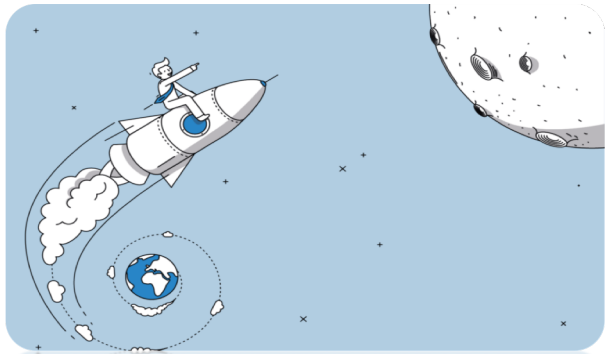
Dal 2010 è iniziato il travaso… ma anche in questo caso arriverà un calo e le grandi società che hanno approfittato, grazie alla acquisizione delle nuove competenze richieste dal mercato, di questa situazione si chiederanno cosa possano offrire ai loro clienti per compensare la contrazione di utili derivanti dal calo degli investimenti.

All'inizio del boom cyber …i manager e i fornitori della sicurezza fisica si dividevano in…

Conservatori

- Legati al vecchio concetto di allarme/reazione
- Uomo con la pistola
- Scarsa integrazione con il mondo IT
- «…si è sempre fatto così»
- Scarso o nullo concetto di trasversalità

Innovatori



- Approccio risk based
- Voglia di esplorare il mondo e le soluzioni IT senza temere di perdere la leadership del processo comprendendo in anticipo che la divisione tra sicurezza fisica e logica non sarebbe più esistita
- Provare a rinunciare al concetto o almeno ad anticipare il momento allarme/reazione

…e adesso?

01 Budget ridotto e quel budget che era destinato in gran parte all'uomo con la pistola va verso soluzioni IT che lo sostituiscano.

02 Approccio sempre più risk based e cambio del partner (prima era tipicamente un istituto di vigilanza adesso diventa un system integrator).

03 Cambio del modello di sicurezza tradizionale per il quale alla fine per capire bene un evento si affidava alla ispezione ed al pronto intervento…(sarebbe spesso sempre la soluzione migliore… ma ormai sovente i servizi vengono bucati e quindi ci si deve cominciare ad organizzare senza farci affidamento).

04 Diventa importantissima la capacità di analizzare e studiare quanto accade all'esterno dell'organizzazione (trend analysis, sharing information, dati statistici e modalità degli attacchi etc.) per ricavarne specifici alert; altrettanto fondamentale la capacità di analizzare ed individuare le aree di vulnerabilità residue che le attività di follow up sugli allarmi e sugli incidenti subiti fanno emergere… il concetto di «percettori sensibili»

BNL Methodology on Risks and Accidents

To manage its physical security effectively, **BNL Security moved from operations only to a governance approach risk-based.** To this end, a **specific methodology focused on Risks and Accidents**, structured into two phases: Ex Ante and Ex Post.

Ex Ante
Identify
Protect
Detect

Observatory

- Alerts or reports from the police
- Scenario evolution (geopolitical aspects, threats and incidents, change in context)
- Geocrime data analysis and benchmark with other competitors

Risk Analysis

Analysis and evaluation of physical security risks and potential impacts for the organization

Security Alert

Description of the risk and triggering event + prevention measures to be adopted (organisational, operational, behavioural)

Bank structures

Application of the defined measures

Monitoring

RISKS - ACCIDENTS

Ex Post
Respond
Recover

Accident

Security incident

Management

Management: classification, containment actions, relations with FFOO

Security Executive Summary

Description of the event, analysis and insights, remediation plan and follow up

Bank structures

- Information reception
- Implementation of remediation activities

Monitoring

Il supporto di una Video Assistenza avanzata ed interattiva con la vita di agenzia per il rischio rapina

Prevenzione	*Misura*	*Strumenti*	*Procedura*
Anti Comitato di Accoglienza	Video Bonifica	•Disp. Richiesta Ispezione •Segnali di allarme h24 •Immagini registrate h24	Prima dell'ingresso dei dipendenti l'operatore verifica l'assenza di segnalazioni d'allarme e di immagini pervenute nel corso della notte, procede alla video-ronda e, se non ravvisa condizioni di rischio, autorizza l'ingresso dei dipendenti
Anti Accodamento	Monitoraggio ingressi	•Gestione stato bussole •Vista bussola	L'operatore dopo aver autorizzato l'ingresso controlla che i primi dipendenti accedano singolarmente e non soggetti a minaccia o presa di ostaggi
Anti Effrazione	Monitoraggio U.E. Monitoraggio h24	•Allarmi perimetrali h24 •Vista su Varchi e U.E.	L'apertura di accessi secondari o U.E se non preavvisata determina una segnalazione di allarme
Anti Rapina (lunga durata)	Monitoraggio stato Mezzi Forti	•Ritardatore di Apertura •Segnalazione accesso al MF •Vista su MF	In condizioni di operatività "normale", verificata l'assenza di condizioni di rischio, l'operatore assiste l'apertura del affiancando il collega nelle operazioni critiche. in caso di rapina l'operatore segue l'andamento della stessa valutando le opportune azioni in base all'analisi della dinamica
Anti Rapina (ag. Con LTS)	Monitoraggio stato Mezzi Forti Accesso LTS	•Logiche di accesso LTS •Ritardatore di Apertura •Segnalazione accesso al MF •Vista interna LTS	In condizioni di operatività "normale", verificato l'assenza di condizioni di rischio, l'operatore assiste l'apertura del MF riducendo i tempi di esposizione del collega nelle operazioni critiche. in caso di rapina l'operatore segue l'andamento della stessa valutando le opportune azioni in base all'analisi della dinamica
Anti Rapina (con armi da fuoco)	Monitoraggio Accesso clientela	•Rilevazione stato MD •Intervento MD •Attivazione Manuale Bussole	L'operatore è in grado di rilevare lo stato di attività dei MD e l'eventuale disattivazione. In condizioni di scarsa affluenza il sistema riattiva il MD e ne informa l'operatore
Anti Rapina	Monitoraggio Accesso clientela	•Rilevazione stato Bussole •Attivazi. Manuale Bussole	In condizioni di rischio l'operatore può attivare la gestione manuale delle bussole

Le nuove agenzie bancarie cominciano ad assomigliare a dei punti vendita - Caratteristiche

- Cash management esternalizzato;
- Divisione fisica tra le cash machine ed il personale;
- Spariscono le bussole si passa alle sliding doors;
- Aumenta la tecnologia in campo con telecamere fornite di video analisi;
- Aumenta la tecnologia a disposizione del cliente che in molti casi può interagire con il personale banca grazie ad un monitor multimediale interattivo connesso ad una control room di servizi bancari.

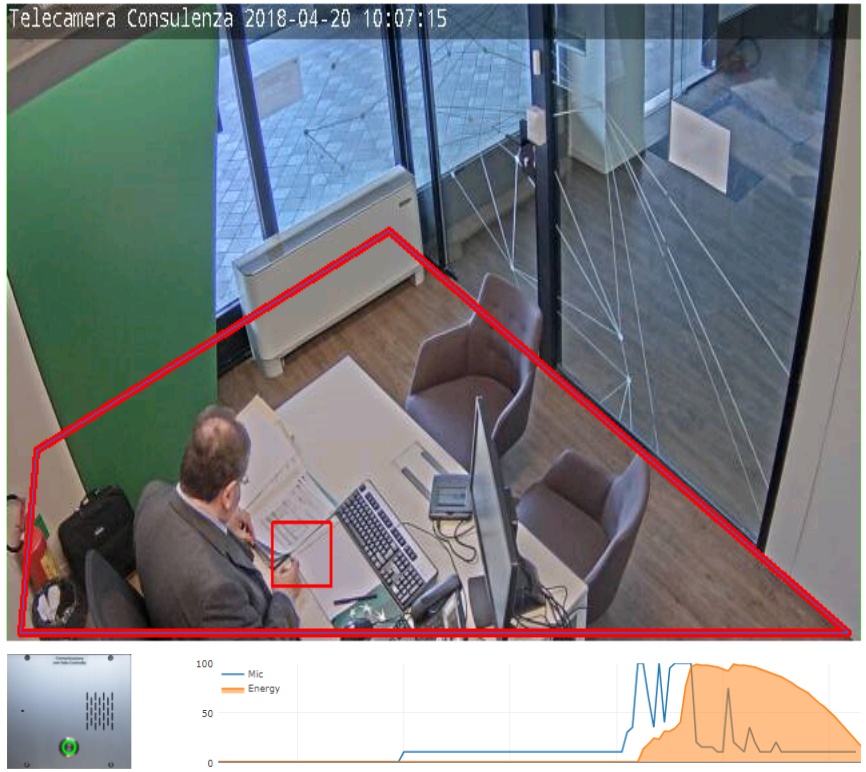
Nelle piccole agenzie si può anche lavorare da soli ed in questo caso la safety diventa il tema centrale con l'utilizzo della analisi video con questo approccio.

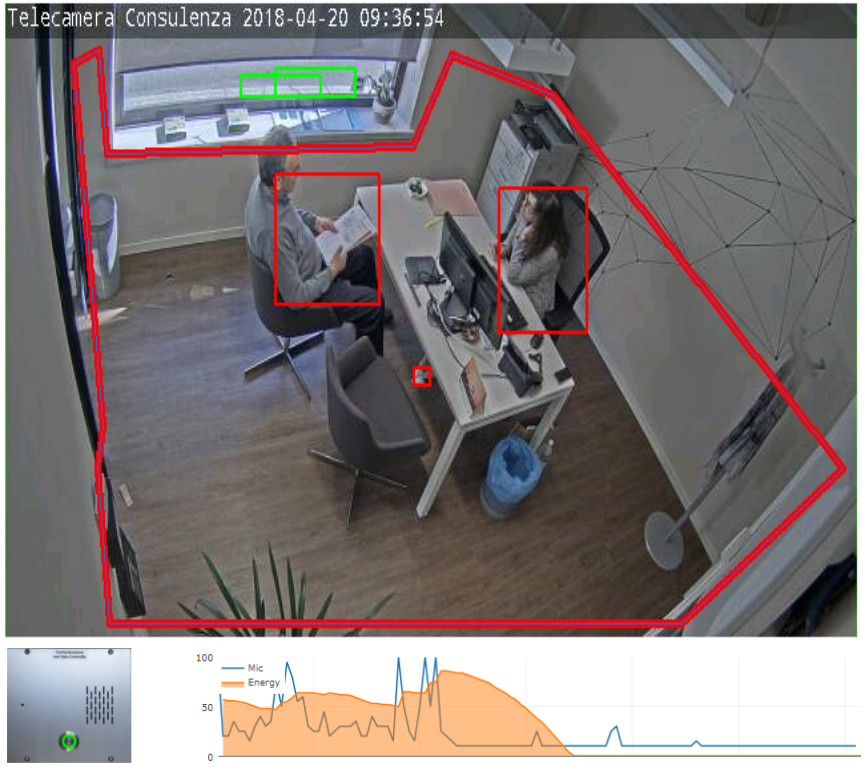
La risposta tecnologica della sicurezza si concretizza attuando il concetto di intelligenza distribuita ponendo in unica piattaforma il governo della sicurezza fisica, della sicurezza logica e della safety.

- La sicurezza antintrusione
- La sicurezza antifurto
- La video-registrazione
- La video-sorveglianza
- La video-analisi
- L'audio bi-direzionale
- Il controllo degli accessi
- La safety

Approccio olistico alla sicurezza del sito e delle risorse che vi lavorano

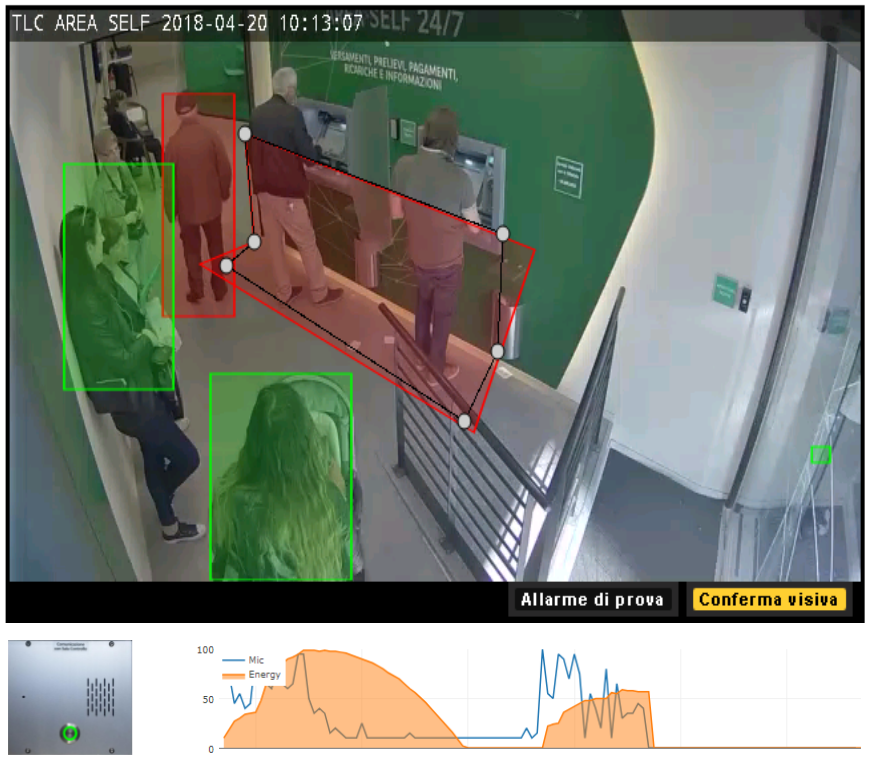
La security e la safety si fondono sempre di più





La particolarità delle Micropop è che possono essere aperte anche da una persona sola; per fare ciò bisogna garantire la safety del collega che viene monitorato grazie all'analisi video e audio; in caso di immobilità prolungata arriva un pop-up in video che attiva la VDS.

Qualche esempio di analisi audio/video per le aree self



L'analisi video per provare a prevenire attacchi e occupazione dei clochard

La nuova modalità di accesso alle cassette di sicurezza

La nuova modalità di accesso alle cassette di sicurezza

L’attacco agli ATM non passa mai di moda

Premessa

Con la tendenza sempre più spinta alla chiusura delle agenzie e/o alla loro trasformazione in agenzie senza gestione di contante da parte del personale di banca, L’ATM è diventato il principale distributore di cash nel paese, un paese in cui la percentuale di transazioni in contante rispetto a quelle con carte e simili si mantengono ancora alte rispetto al resto dell’europa.

Conseguenza logica è che l’ATM sia diventato l’oggetto di maggiore attenzione da parte dei nostri antagonisti e che quindi sulla sua protezione ci sia la maggiore attenzione da parte dei security manager delle banche.

Infine l’ATM è il più evidente esempio di come la sua protezione sarà efficace solo se si avrà un approccio olistico abbattendo le barriere tra sicurezza fisica e logica tenendo sempre nella giusta considerazione le esigenze di business. Solo così sarà possibile raggiungere il necessario e giusto compromesso, nel senso più ampio, tra le esigenze di business e di security.

Contesto

Anche se il numero totale degli attacchi nel 2023 è in diminuzione, in questi ultimi mesi i primi dati sembrano evidenziare come il numero degli attacchi sia in sensibile aumento.

Tali attacchi vengono realizzati da parte di bande più o meno organizzate che adottano tecniche sempre più avanzate e sofisticate specialmente nelle tipologie di attacchi con gli esplosivi e negli attacchi cyber-physical. Si nota infatti una crescita esponenziale dei c.d. attacchi multivettoriali (black box).

L’approccio di un percorso pluriennale alla sicurezza degli ATM

Approccio

- Credere nell’**invalidazione e neutralizzazione delle banconote**.
- In Italia a differenza di altri paesi non è obbligatoria la macchiatura delle banconote, in Francia per esempio lo è, ed un importante supporto investigativo.
- **Dialogo** immaginario **tra Banca e Offender**.
- **Evoluzione degli Offender**.
- **Nuovi metodi** per bypassare le difese tradizionali.

Facendo una piccola storia cominciamo con:

Gas Esplosivo

Marmotte esplosive

AntiGas

Macchiatore

Ghigliottina

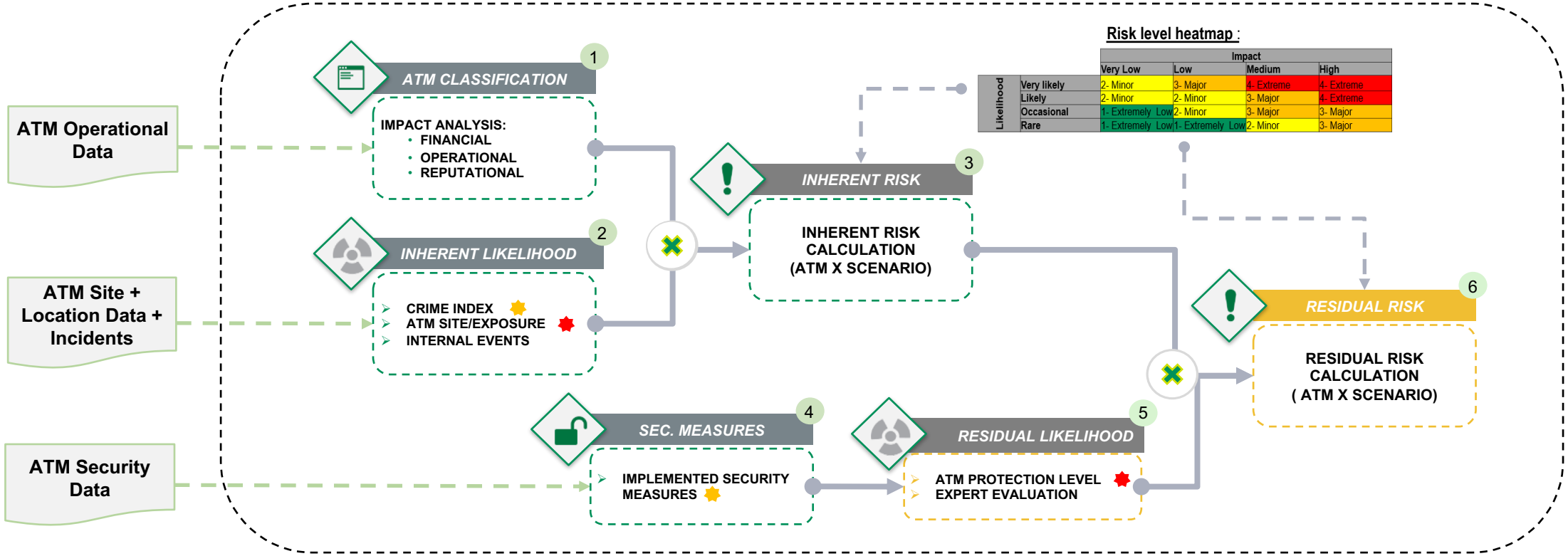
Esplosivo posizionato in modo da proiettare i cassetti fuori dalla cassaforte prima che l’elettronica dia input della macchiatura

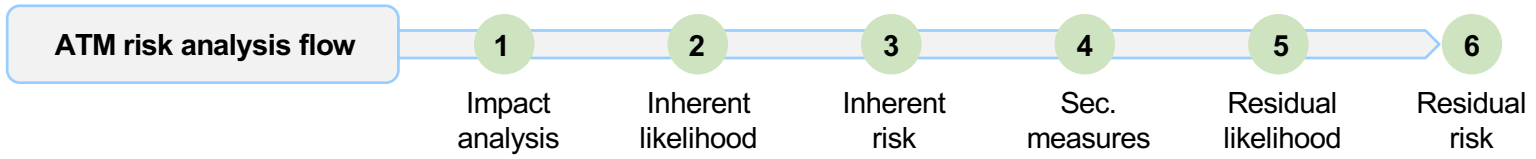
Sistema Ibrido di macchiatura con doppia tecnologia (Attiva e Passiva)

Attacco Informatico con l’ausilio di speciali dispositivi in grado di far **erogare direttamente le banconote** a comando

Soluzione SW (Cifratura Canale, Aggiornamenti Patch etc.) in combinazione **a soluzione HW** in grado di bloccare l’erogazione di cash

Metodologia di Analisi del Rischio ATM





New parameter *New data source*

Parametri di Impatto e Probabilità ATM

Parametri di impatto ATM (Finanziario - Operativo - Immagine del marchio)

		Vey Low	Low	Medium	High
	Finanziario (Cassandra)	0 < X<= € 60.000	€ 61.000 < X<= € 100.000	€ 101.000 < X<= € 150.000	X > € 150.000
Non Finanziario	Operativo	Minimo tempo e sforzo richiesti per ripristinare il servizio. Minimo danno/interruzione dell'ATM. Nessuna perdita misurabile della quota di mercato o del numero di clienti o dei costi legali.	Bassi tempi e sforzi necessari per ripristinare il servizio. Minima perdita di quote di mercato o di numero di clienti. Costi legali minimi.	Danni al funzionamento con conseguenti danni gravi e tempi e sforzi considerevoli per ripristinare il servizio. Alcune perdite di quote di mercato o di numero di clienti. Alcune spese legali.	Indisponibilità estesa del servizio e problemi critici per ripristinare il servizio. Perdita significativa della quota di mercato o del numero di clienti. Costi legali significativi.
	Immagine del marchio	Nessun danno al marchio	Media locali/attenzione pubblica	Media nazionali/attenzione pubblica	Prolungata attenzione dei media/pubblico nazionale

N.B:

- La matrice d'impatto ATM è attualmente definita concentrandosi sullo scenario di rischio ATM analizzato: "Furto di contanti ATM causato da un attacco fisico (furto o danno ATM)".

  Queste dimensioni d'impatto potrebbero anche essere considerate per altri eventi rischiosi che implicano un attacco fisico o cyber-fisico all'ATM (per esempio, Black Box, Skimmer).

- Altre dimensioni d'impatto "non finanziarie" (per esempio, Data Disclosure e Legal & Regulatory) potrebbero essere definite in caso di estensione dell'analisi ad altri scenari di rischio informatico.

In fase di valutazione: questi parametri di impatto potrebbero essere derivati attraverso la classificazione ATM

Parametri di probabilità ATM (Punteggio dell'indice di criminalità - Posizione/esposizione sicura - Misure di sicurezza)

Scala di occorrenza	**< once of every 5 years**	**Once every 5Y < X < Once Every 3Y**	**Once every 3Y < X < Once Every Y**	**X => Every Y**
	Rare	Occasional	Likely	Very Likely
Punteggio dell'indice di criminalità	1	2	3	4
Posizione/esposizione sicura	Posizione: centrale Contesto stradale: pedonale Distanza dai siti delle forze armate: < 1 KM	Posizione: semi-periferica Contesto stradale: traffico veicolare lento e limitato Distanza dai siti delle forze armate: < 3 KM	Posizione: periferica Contesto stradale: traffico veicolare veloce Distanza dai siti delle forze armate: < 5 KM	Posizione: isolato Contesto stradale: vicinanza dell'autostrada e delle arterie principali Distanza dai siti delle forze armate: > 5 KM

- ✓ Punteggio dell'indice di criminalità: Dati esterni sugli attacchi ATM (Ossif/Geocrime, ecc.) + Dati storici BNL sugli eventi ATM (attacchi/incidenti).
- ✓ Posizione/Esposizione sicura: CRC della banca - controlli di sicurezza dell'agenzia (posizione, contesto stradale, vicinanza ai siti delle forze armate) + Valutazione del sito da parte di esperti.

N.B:

- Il calcolo della probabilità potrebbe essere rivisto introducendo un parametro di correzione basato sulla valutazione dell'esperto in materia della BNL. Questo parametro dovrebbe essere definito per ogni ATM e basato su informazioni specifiche sull'ATM o su informazioni "osint" (open source intelligence) (es. ubicazione, avvisi della polizia, ecc.).

Approccio RISK BASED

La **nuova metodologia di rischio ATM** proposta può essere adottata dalla sicurezza aziendale.

La metodologia di rischio ATM illustrata nasce (oltre 10 anni fa) partendo dallo scenario di rischio **"Furto ATM"**: Furto di contanti dell'ATM causato da un attacco fisico (furto del cash o asportazione dell'ATM). L'approccio utilizzato ci ha consentito di estenderne l'uso anche su altri scenari di rischio (attacchi Black-box, Skimmer, ecc.), rivedendo o introducendo nuovi parametri di impatto o probabilità.

L'affidabilità della operazione di valutazione del rischio passa necessariamente da una approfondita conoscenza sia delle modalità di attacco (in continua evoluzione) ma anche dalla conoscenza dei singoli modelli di ATM che statisticamente risultano attaccati. Per arrivare a questo è necessaria ed utile una puntuale condivisione delle informazioni da parte di tutti gli stakeholders e su questo il contributo di OSSIF tramite lo strumento Geo Crime Analyst diventa fondamentale.

L'adozione di una nuova metodologia di rischio ATM non può escludere la **stima dell'esperto nel processo di valutazione del rischio** (simile a quanto accade per gli asset IT).

Grazie all'adozione di un **approccio risk based**, le dotazioni di sicurezza da applicare agli ATM si possono orientare rispetto al livello di rischio identificato.

THANK

merci

YOGGRA

mèsitak

chokrane

ZAHRIG

dhanyavad

dziękuję

ATÔ

GRACIAS danke ευχαριστώ NANDRI

MAH

спасибо

teşekkür

ALO

ederim spas JËRËJËF