Digital transformation in banca, come cambiano il ruolo e la figura del security manager

intervista a Pier Luigi Martusciello, Head of Corporate Security BNL/BNPARIBAS Italia | componente comitato scientifico OSSIF

Quanto corrisponde oggi al vero la vulgata degli anni passati che il responsabile della sicurezza aziendale bancaria debba avere attitudini, competenze e perfino caratteristiche soggettive diverse dai suoi omologhi operanti in ambiti diversi, ad esempio, l'industria, il retail, la logistica?

Ormai sono 30 anni che mi occupo di sicurezza aziendale e non ho iniziato nel mondo bancario ma nelle telecomunicazioni. Quando sono entrato in banca 14 anni fa, non ho dovuto cambiare approccio in modo radicale ma, anzi, provenire da un'altra realtà mi ha forse aiutato ad avere una visione delle cose diversa da quella fino ad allora consolidata ed imperante nel mondo bancario. Certo, quello che cambiava era sicuramente l'asset da proteggere (il cash e le cassette di sicurezza) e gli strumenti che venivano usati per farlo.

In particolare, i responsabili della sicurezza delle banche gestivano fondamentalmente l'antirapina e le guardie giurate erano la soluzione principale, a parte qualche timido primo approccio alla videosorveglianza.

Cercavano di contenere il rischio attacco agli ATM senza riuscire ad entrare in modo determinante nelle tematiche di scelta della macchina, della sua protezione e del suo caricamento.

Avevano a disposizione investimenti limitati e possibilità di sperimentare pari a zero, impossibilitati, quindi, a lavorare in modo "prospettico" dovendo gestire prevalentemente situazioni di emergenza.

La trasversalità della struttura e la partecipazione attiva alle scelte del business erano inesistenti come, ad esempio, nella definizione del layout delle agenzie. Si muovevano in un contesto di assoluta mancanza di cultura della security, fare accettare scelte "protettive" era davvero problematico e le soluzioni proposte erano viste (e spesso lo erano) come un mero ostacolo al business.

Adesso è tutto cambiato in qualsiasi realtà aziendale. Il responsabile della sicurezza assomiglia sempre di più ad un manager del settore finanziario che produce

continuamente business case, avendo sempre come unico target il raggiungimento del giusto compromesso tra le spese necessarie per "fare sicurezza" ed alle sempre più cangianti e diversificate esigenze del business.

Quanto ha influito la digitalizzazione della materialità nel cambiamento dei processi di security aziendale, anche in un'ottica di integrazione cyber-physical security?

Il processo di trasformazione del denaro non ha ancora terminato il suo ciclo e il contante in giro è ancora tanto e sempre "appetitoso": in un solo ATM possono esserci anche 200K€ e la loro protezione è sempre più importante diventando, di fatto, il core business del responsabile della sicurezza in banca.

Tuttavia, l'evoluzione delle tecnologie applicate alla sicurezza e l'invasione a tutto campo dell'Internet of Things nel loro complesso ci costringe a cambiare il paradigma dell'approccio alla sicurezza, mettendo in discussione le categorie con cui sono state pensate fino ad ora le contromisure agli attacchi dei beni materiali ed immateriali e delle persone dell'azienda. Questo comporta un profondo ripensamento in termini di approccio filosofico e operativo al tema, in quanto la

definizione di un modello di sicurezza efficace può e deve comprendere numerosi alert/segnali provenienti da settori finora scarsamente considerati o, perlomeno, la cui interrelazione deve essere maggiormente considerata.
Di conseguenza, l'evoluzione spontanea (ma comunque necessaria) che porta all'annullamento dei confini tra cyber e physical security non è dettata solamente dal livello di innovazione tecnologica quanto dall'esigenza di affrontare in modo "olistico" la parte computazionale e la parte fisica, da un lato per mitigare le minacce, dall'altro per cogliere opportunità, (es. generare sinergie).
Ecco che si cercano nuovi strumenti metodologici e progettuali, in quanto le componenti physical e quelle cyber hanno caratteristiche tra loro diverse. E' quindi necessario immaginare nuovi modelli progettuali, nuove competenze e nuovi mindsets per coniugare le differenze, individuare i migliori trade off, costruire nuove soluzioni capaci di enfatizzare i punti di forza delle due anime e, nel contempo, ridurre l'effetto dei punti di debolezza.

Quali sono le opportunità future, dal suo punto di vista, per la funzione di security management nel sistema bancario?

Tutto dipenderà dalla visione del management della singola azienda su dove e come posizionare la struttura di sicurezza all'interno dell'organigramma aziendale.
La tendenza delle aziende maggiori è di unificare in un'unica struttura, guidata da un CSO a diretto riporto del CEO o del COO, tutte le anime della sicurezza (logica, fisica, antifrode, business continuity).
Approcciare in modo olistico la gestione dei rischi è, a mio parere, la migliore delle soluzioni, la strada più veloce e più efficace per raggiungere la tanto agognata meta per chi fa il nostro mestiere: la "security by design".
Nel mondo bancario questa visione è meno consolidata e diffusa e la cosa è assolutamente comprensibile in ragione della circostanza che il cash, le cassette di sicurezza, sono qualcosa di molto "fisico" e le modalità di protezione di questi asset hanno anch'esse caratteristiche fondamentalmente fisiche.
Queste peculiarità portano con sé skill e caratteristiche molto specifiche che demarcano ancora in molti casi un confine che non aiuta al cambio di paradigma. Ormai però le cose stanno cambiando e le agenzie bancarie assomigliano molto di più a dei negozi retail.
La gestione del contante è sempre più demandata a personale fiduciario esterno alle banche, l'accesso alla agenzia è libero senza essere più mediato e controllato dalle bussole.
Questa tendenza, ormai consolidata, porta a cambiare il modello di filiale, cambiare l'esigenza di sicurezza fisica cambiare l'esigenza gestionale della sicurezza fisica.
In sintesi:
- non solo analisi dei sistemi antintrusione-antifurto e dei sistemi di videosorveglianza connessi a sistemi di centralizzazione più o meno evoluti, ma è necessaria anche

la capacità di analizzare in modo intelligente un evento o un insieme di eventi e di discriminare gli stessi in funzione di parametri gestionali diversi
- non basta più la sola generazione di un semplice output di allarme ma bisogna analizzare un insieme di elementi o situazioni anche se provenienti da tecnologie diverse, al fine di ottenere un output di segnalazione dettagliato e che consenta immediatamente di capire la natura dell'anomalia
- la risposta tecnologica della sicurezza si concretizza attuando il concetto di intelligenza distribuita, ponendo in unica piattaforma il governo di sicurezza fisica, sicurezza logica, safety, crisis management ed anche il controllo accessi in stretta connessione con temi di identity access management.

Ritiene ci saranno le condizioni per lo sviluppo dell'outsourcing in un ottica di open innovation, anche delle funzioni di responsabilità, strategia e controllo dopo quello delle attività esecutive di security negli anni passati?
Secondo me molto dipende dal core business della azienda e dalla sua grandezza.
Le grandi aziende accelereranno ulteriormente sulla esternalizzazione delle attività meramente operative/ esecutive ma manterranno in casa tutte le attività di governance , policy e controllo; le società invece medio/ piccole potranno invece affidarsi a professionisti del settore per le attività di consulenza su temi di impostazione della gestione del rischio a 360 gradi.
E' mia opinione che in tema di consulenza il mercato sia maturo e conti numerose eccellenze in grado di aiutare e supportare le aziende ad impostare un modello di security vincente e costruito in maniera "sartoriale" a seconda delle specifiche esigenze del cliente.
Per fare questo passo, tuttavia, è indispensabile avere il supporto tecnologico di strumenti che consentano ai responsabili della governance di monitorare dinamicamente i rischi che, come sappiamo, cambiano continuamente, le performance della sale, la perfetta funzionalità degli impianti. Anche in questo ambito fondamentale il mercato offre molte eccellenze.
A questo proposito, penso che i naturali partner per garantire questo supporto possano essere gli istituti di vigilanza con le loro control room ma, purtroppo, non mi pare abbiano finora colto questa opportunità.
Mi piace parlare di confini che si abbattono e tra questi a tendere ci sarà la differenza tra un soc ed una control room. Quest'ultima dovrà essere sempre più somigliante ad un soc e con ciò cambierà anche lo skill dell'operatore che avrà da gestire un allarme sempre meno generico ma ben diagnosticato perché a monte il sistema ha già valutato ed incrociato tutte le info utili e, quindi, se lo propone come allarme è molto probabile che sia reale.
L'evoluzione delle control room faciliterà l'outsourcing di molte attività ma il security manager sarà ancora centrale e serve ancora (e meno male) per vincere la più importante sfida che ci aspetta perché avremo:
- un numero sempre più grande numero di informazioni
- una sempre più grande capacità di stivaggio delle stesse;
- una velocità di analisi delle info e del loro continuo aggiornamento;
- la capacità di mettere in relazione le informazioni tra loro e nel più breve tempo possibile;
- possibilità ormai reale di sfruttare moduli di intelligenza artificiale e di utilizzare algoritmi predittivi che consentano di prevenire, oltre gli incidenti, anche eventuali problematiche funzionali (manutenzione predittiva) ed anche suggerire al management gli interventi evolutivi e manutentivi per incrementare i livelli di sicurezza di qualsiasi infrastruttura ci si trovi a gestire.

Il problema vero che ci si pone e che, ripeto, è anche la sfida dei prossimi anni, è cosa farcene di tutta questa marea di informazioni, come utilizzarle, come, renderle strumentali ai nostri obiettivi.
Attualmente è ancora enorme il gap tra la infinita serie di informazioni che possiamo avere e quelle che riusciamo ad usare in modo davvero utile e funzionale ai nostri obiettivi.
Solo se riusciremo a "farci la domanda giusta" e "trovare la risposta corretta" saremo in grado di domare lo tsunami di informazioni che ci stanno travolgendo dando alle informazioni stesse il valore aggiunto che ci aspettiamo.