Commercial Banking Cybersecurity Psychology Framework (CB-CPF v1.0):

Sicurezza delle Operazioni di Filiale, Call Center e Servizi Finanziari Retail Attraverso la Valutazione delle Vulnerabilità Pre-Cognitive

Giuseppe Canale, CISSP
Ricercatore Indipendente
g.canale@cpf3.org
URL: cpf3.org
ORCID: 0009-0007-3263-6897

18 Novembre 2025

Abstract

Il commercial banking—la "Main Street" dei servizi finanziari—presenta un profilo di vulnerabilità psicologica fondamentalmente distinto dall'investment banking e dai mercati dei capitali. Mentre gli ambienti di trading algoritmico affrontano pressioni di latenza nell'ordine dei microsecondi, le operazioni bancarie retail confrontano la sfida inversa: il degrado cognitivo indotto dalla routine attraverso milioni di transazioni ripetitive elaborate da cassieri di filiale, operatori di call center e personale di back-office. Questo paper presenta il Commercial Banking Cybersecurity Psychology Framework (CB-CPF v1.0), mappando i fenomeni del retail banking sulla tassonomia Core 10 del CPF. Dimostriamo che l'imperativo culturale "Service First", la cecità indotta dalla routine derivante dall'esecuzione di task ripetitivi, la frustrazione da legacy system che spinge all'adozione di shadow IT, e le dinamiche di gruppo a livello di filiale che creano l'aggiramento delle policy rappresentano *manifestazioni calibrate* delle Categorie 1, 3, 5, 6 e 9 piuttosto che nuove categorie psicologiche. Il framework affronta la sfida unica di proteggere organizzazioni dove i dipendenti frontline elaborano centinaia di interazioni quotidiane con i clienti sotto aspettative di service-level che confliggono con i requisiti di verifica di sicurezza. Presentiamo funzioni di detection adattate per la telemetria di filiale, strategie di intervento che affrontano la tensione servizio-sicurezza, e un case study del "Bonifico del Venerdì Pomeriggio" che dimostra lo sfruttamento convergente della deferenza all'autorità e dello stress temporale negli ambienti di filiale.

Keywords: commercial banking, retail banking, sicurezza di filiale, sicurezza call center, social engineering, routine blindness, legacy systems, operazioni frontline, implementazione CPF

1 Introduzione: La Psicologia della Filiale e del Back Office

1.1 Distinguere il Commercial Banking dall'Investment Banking

Il Financial Services CPF (FS-CPF v2.0) affronta le vulnerabilità psicologiche negli ambienti di trading caratterizzati da latenze nell'ordine dei microsecondi, decision-making algoritmico e correlazioni con la volatilità di mercato (Canale, 2025d). Il commercial banking occupa uno spazio psicologico fondamentalmente diverso. Dove i trader affrontano il degrado cognitivo per eccessiva velocità, i banker retail affrontano il degrado cognitivo per eccessiva *ripetizione*. Dove i trading floor eliminano il processing del System 2 attraverso la compressione temporale, le

operazioni di filiale eliminano il processing del System 2 attraverso l'autopilota indotto dalla monotonia.

Questa distinzione è critica. Gli interventi progettati per ambienti ad alta frequenza falliscono nei contesti retail, e viceversa. Il CB-CPF fornisce calibrazioni appropriate per le dinamiche psicologiche distintive di:

- **Operazioni di filiale**: Transazioni di cassa, servizi di conto, origination prestiti
- **Call center**: Customer service, verifica account, gestione dispute
- **Back office**: Elaborazione pagamenti, data entry, riconciliazione
- **Retail lending**: Origination mutui, credito al consumo, small business banking

Questi ambienti condividono caratteristiche assenti dall'investment banking: interazione diretta con il cliente su larga scala, aspettative di service-level misurate in minuti non millisecondi, filiali fisiche con relazioni con la comunità locale, e infrastrutture tecnologiche legacy accumulate attraverso decenni di operazioni retail.

1.2 Il Paradosso "Service First"

La cultura del commercial banking consacra il customer service come valore organizzativo supremo. I direttori di filiale sono valutati sui punteggi di customer satisfaction. Gli operatori di call center sono monitorati sui tassi di "first call resolution". Le campagne marketing promettono servizio personalizzato e relationship banking. Questo orientamento culturale produce un paradosso fondamentale di sicurezza.

La disposizione psicologica richiesta per un eccellente customer service—empatia, reattività, accommodamento, orientamento al problem-solving—è precisamente la disposizione che i social engineer sfruttano. Il cassiere addestrato a "rendere speciale la giornata del cliente" diventa vulnerabile a richieste inquadrate come imperativi di customer service: "Per favore mi aiuti ad accedere al mio conto, sono bloccato fuori." L'operatore di call center misurato sulla velocità di risoluzione diventa vulnerabile alla manipolazione dell'urgenza: "Ho bisogno che questo sia risolto ora, ho un'emergenza."

Il paradosso si approfondisce perché la friction di sicurezza confligge direttamente con le metriche di servizio. Ogni domanda di verifica estende la durata della chiamata. Ogni richiesta di documenti ritarda il completamento della transazione. Ogni escalation per attività sospetta produce reclami dei clienti. I dipendenti affrontano un'ottimizzazione impossibile: massimizzare il servizio *oppure* massimizzare la sicurezza, ma non entrambi simultaneamente.

1.3 La Routine-Induced Blindness

La teoria del dual-process di Kahneman (Kahneman, 2011) descrive la cognizione del System 1 (veloce, automatica) e del System 2 (lenta, deliberativa). Negli ambienti di trading, il dominio del System 1 emerge dalla pressione temporale—non c'è tempo per la deliberazione. Nel retail banking, il dominio del System 1 emerge dalla ripetizione—non c'è *stimolo* per la deliberazione.

Un cassiere di filiale che elabora 200 transazioni giornaliere sviluppa pattern di risposta automatici. Le transazioni dalla 1 alla 199 sono legittime; il pattern-matching del cassiere approva correttamente ciascuna. La transazione 200 contiene indicatori di frode, ma il System 1 del cassiere la elabora identicamente alle 199 precedenti. Gli indicatori di frode che attiverebbero l'engagement del System 2 in un contesto nuovo falliscono nel registrarsi in un contesto di routine.

Questo fenomeno—routine-induced blindness—differisce qualitativamente dall'alert fatigue descritta nella letteratura sulle security operations. L'alert fatigue risulta da un eccessivo volume di segnali che sovraccarica la capacità di attenzione. La routine-induced blindness risulta da un'insufficiente variazione dei segnali che fallisce nell'attivare l'attenzione. Il cassiere non è

sopraffatto da troppi alert; il cassiere non riceve alcun alert perché la transazione fraudolenta *appare come* le transazioni legittime che l'hanno preceduta.

1.4 La Frustrazione da Legacy System

Le banche commerciali operano ambienti tecnologici accumulati attraverso decenni di crescita organica e acquisizioni. I core banking system possono risalire agli anni '70, con successivi layer di integrazione che aggiungono complessità senza rimuovere i componenti legacy sottostanti. L'impatto psicologico di questo debito tecnologico è sostanziale ma poco studiato nei contesti di sicurezza.

I dipendenti costretti a navigare legacy system lenti e poco intuitivi sperimentano una frustrazione cronica che si manifesta in comportamenti rilevanti per la sicurezza:

(1) **Sviluppo di Workaround**: I dipendenti scoprono procedure non ufficiali che bypassano le funzioni lente del sistema. Questi workaround spesso aggirano i controlli di sicurezza incorporati nelle procedure standard.

(2) **Adozione di Shadow IT**: I dipendenti frustrati adottano strumenti non autorizzati (email personale, file-sharing consumer, database su spreadsheet) per svolgere task che i legacy system gestiscono male.

(3) **Risentimento verso i Controlli**: I dipendenti che percepiscono i controlli di sicurezza come "solo altri ostacoli" in un ambiente tecnologico già frustrante resistono ai requisiti di sicurezza più intensamente di quanto farebbero in un ambiente moderno e usabile.

(4) **Learned Helplessness**: I dipendenti che sperimentano ripetutamente fallimenti di sistema sviluppano aspettative che i sistemi non funzioneranno correttamente, riducendo la loro attenzione ai messaggi di errore e agli avvisi di sicurezza che potrebbero indicare minacce genuine.

1.5 Struttura del Documento

La Sezione 2 mappa i fenomeni del commercial banking sulle categorie Core 10 con calibrazione retail-specifica. La Sezione 3 presenta la metodologia di intervento CPIF adattata per gli ambienti di filiale e call center. La Sezione 4 fornisce l'implementazione tecnica OFTLISRV per la telemetria del retail banking. La Sezione 5 presenta il case study "Bonifico del Venerdì Pomeriggio". La Sezione 6 conclude con le considerazioni di deployment per le reti di filiali distribuite.

2 Manifestazioni del Commercial Banking: Mappare i Fenomeni Retail sulla Tassonomia Core 10

Il commercial banking non introduce nuove vulnerabilità psicologiche; piuttosto, attiva categorie di vulnerabilità esistenti attraverso le dinamiche distintive delle operazioni ripetitive customer-facing, del relationship banking locale e degli ambienti tecnologici legacy.

2.1 Manifestazione Categoria 1: La Sindrome del Cliente VIP

2.1.1 Fondamento Teorico

La Categoria 1 (Authority-Based Vulnerabilities) comprende i pattern di deferenza verso figure di autorità percepita. Nel commercial banking, l'autorità opera attraverso due canali distinti: la gerarchia organizzativa (come nel CPF standard) e lo *status del cliente*—l'autorità economica e sociale dei clienti ad alto valore.

L'imprenditore locale che mantiene depositi commerciali significativi, il cliente di lunga data conosciuto personalmente dallo staff di filiale, la figura della comunità la cui relazione precede il mandato dei dipendenti attuali—questi clienti esercitano un'autorità informale che inibisce la normale verifica di sicurezza.

2.1.2 Caratteristiche della Manifestazione

La Sindrome del Cliente VIP descrive il rilassamento sistematico dei controlli di sicurezza per i clienti ad alto status:

(1) **Bypass della Verifica d'Identità**: "Conosco il Sig. Rossi da vent'anni—non ho bisogno di vedere il suo documento." La familiarità personale si sostituisce alla verifica procedurale, creando vulnerabilità quando la familiarità è prodotta artificialmente o sfruttata.

(2) **Accommodamento AML/KYC**: I requisiti anti-riciclaggio e know-your-customer sono rilassati per i clienti il cui valore relazionale supera il rischio di compliance percepito. I direttori di filiale affrontano una pressione implicita per evitare di "offendere" clienti preziosi con richieste di documentazione.

(3) **Inflazione delle Exception Authorization**: I clienti VIP ricevono approvazioni di eccezione che sarebbero negate ai clienti standard. Queste eccezioni stabiliscono precedenti che erodono l'efficacia dei controlli attraverso l'intera base clienti.

(4) **Avversione ai Reclami**: I clienti VIP che si lamentano delle procedure di sicurezza ricevono accommodamenti per prevenire danni alla relazione. Gli avversari che comprendono questa dinamica producono reclami strategicamente.

(5) **Vulnerabilità all'Impersonation**: Il cliente VIP conosciuto "a vista" diventa un target di impersonation. Gli avversari ricercano i clienti VIP e si presentano a membri dello staff che riconoscono il nome ma non il volto.

2.1.3 Mapping Matematico

La Sindrome del Cliente VIP si mappa sugli indicatori 1.1, 1.4 e 1.8 con calibrazione del valore relazionale:

Indicatore 1.1 (Unquestioning Compliance) - Calibrazione Commercial Banking:

$$C_r^{CB}(c,t) = \frac{V_{bypass}(c,t)}{V_{required}(c,t)} \cdot \left(1 + \alpha \cdot \frac{R_{value}(c)}{R_{threshold}}\right) \tag{1}$$

Dove:

- $V_{bypass}(c,t)$ = step di verifica bypassati per il cliente c nel periodo t
- $V_{required}(c,t)$ = step di verifica richiesti dalla policy
- $R_{value}(c)$ = valore della relazione (depositi, prestiti, ricavi da commissioni)
- $R_{threshold}$ = soglia per la designazione "VIP"

La detection si attiva quando il tasso di bypass correla positivamente con il valore della relazione ($\rho(V_{bypass}, R_{value}) > 0.5$).

Indicatore 1.4 (Convenience-Based Bypassing) - Calibrazione Commercial Banking:

$$CBR^{CB}(b,t) = \frac{E_{VIP}(b,t)}{E_{standard}(b,t)} \cdot \frac{N_{VIP}(b)}{N_{total}(b)} \tag{2}$$

Dove b indicizza la location della filiale. La detection si attiva quando i clienti VIP (piccola frazione della popolazione) rappresentano un volume sproporzionato di eccezioni.

2.1.4 Aggiornamento Probabilità Condizionata

$$P^{CB}(1.1|3.4) = 0.82 \quad \text{(versus base } P(1.1|3.4) = 0.55) \tag{3}$$

L'elevata probabilità condizionata riflette che l'influenza basata sul liking (Categoria 3.4) predice fortemente il bypass di compliance nei contesti di relationship banking—i dipendenti a cui piacciono i clienti li verificano meno rigorosamente.

2.2 Manifestazione Categoria 3: Frontline Empathy e Sfruttamento del Likability

2.2.1 Fondamento Teorico

La Categoria 3 (Social Influence Vulnerabilities) affronta lo sfruttamento della programmazione sociale umana fondamentale, basata sui principi di influenza di Cialdini (2007). Le operazioni frontline del commercial banking presentano un'esposizione concentrata all'influenza sociale: ogni interazione con il cliente è un'opportunità per il deployment di tattiche di influenza.

Il cassiere di filiale e l'operatore di call center occupano ruoli progettati per l'engagement sociale. La formazione enfatizza la costruzione del rapport, l'ascolto attivo e lo sviluppo della relazione con il cliente. Questi requisiti professionali creano superfici psicologiche sfruttabili.

2.2.2 Caratteristiche della Manifestazione

Frontline Empathy e Sfruttamento del Likability descrive le tattiche di social engineering che prendono di mira lo staff customer-facing:

(1) **Performance del Distress**: Gli avversari simulano distress emotivo (pianto, panico, disperazione) per attivare risposte empatiche che superano i requisiti di verifica. "Per favore, ho bisogno di accedere al conto di mia madre—è in ospedale e devo pagare le sue bollette."

(2) **Accelerazione del Rapport**: Gli avversari impiegano tecniche di costruzione rapida del rapport (uso del nome, disclosure personale, umorismo) per stabilire dinamiche relazionali che inibiscono lo scetticismo. Il cassiere a cui "piace" il cliente resiste a trattarlo come una potenziale minaccia.

(3) **Sfruttamento dell'Identità di Helper**: Lo staff frontline spesso si auto-identifica come helper. Gli avversari inquadrano le richieste in termini di ricerca di aiuto: "Può aiutarmi a capire perché non riesco ad accedere al mio conto?" L'identità di helper del dipendente motiva l'accommodamento.

(4) **Induzione della Reciprocità**: Gli avversari forniscono piccoli favori o complimenti prima di fare richieste, attivando obblighi di reciprocità. "È stato così gentile—ho solo un'altra piccola domanda sul trasferimento di questi fondi."

(5) **Fabbricazione del Social Proof**: "L'operatore con cui ho parlato ieri ha detto che andava bene." Un'autorizzazione precedente fabbricata crea social proof percepito che legittima le richieste.

2.2.3 Mapping Matematico

Frontline Empathy si mappa sugli indicatori 3.1, 3.4 e 3.7 con calibrazione della densità di interazione:

Indicatore 3.4 (Liking-Based Trust Override) - Calibrazione Commercial Banking:

$$LTO^{CB}(e,t) = \frac{\sum_{i \in I(e,t)} S_{rapport}(i) \cdot V_{bypass}(i)}{\sum_{i \in I(e,t)} S_{rapport}(i)} \tag{4}$$

Dove:

- $I(e,t)$ = interazioni per il dipendente e nel periodo t
- $S_{rapport}(i)$ = punteggio di intensità del rapport per l'interazione i (derivato dall'analisi della comunicazione)
- $V_{bypass}(i)$ = indicatore di bypass della verifica per l'interazione i

La detection si attiva quando le interazioni ad alto rapport correlano con il bypass della verifica ($\rho(S_{rapport}, V_{bypass}) > 0.4$).

Metrica Specifica Call Center: Security Question Bypass Rate

$$SQBR(a,t) = \frac{N_{questions\_waived}(a,t)}{N_{questions\_required}(a,t)} \cdot \frac{T_{avg}(a,t)}{T_{target}} \tag{5}$$

Dove T_{avg}/T_{target} cattura se i bypass correlano con la pressione sulla durata della chiamata. La detection si attiva quando SQBR supera la soglia E i tempi di chiamata sono sotto target (indicando bypass guidato dalla velocità).

2.2.4 Aggiornamento Probabilità Condizionata

$$P^{CB}(3.x|4.x) = 0.78 \quad \text{(versus base } P(3.x|4.x) = 0.60) \tag{6}$$

Gli stati affettivi (Categoria 4) predicono fortemente la suscettibilità all'influenza sociale nei contesti frontline—i dipendenti emotivamente coinvolti sono più suscettibili alle tattiche di influenza.

2.3 Manifestazione Categoria 5: Alert Fatigue e Autopilota

2.3.1 Fondamento Teorico

La Categoria 5 (Cognitive Overload Vulnerabilities) affronta le condizioni in cui le richieste di sicurezza superano la capacità di elaborazione umana. Gli indicatori standard assumono un overload da eccessivo volume o complessità delle informazioni. Il commercial banking presenta un pattern di overload distintivo: il degrado cognitivo dalla *ripetizione* piuttosto che dalla complessità.

Il meccanismo psicologico differisce dall'alert fatigue standard. L'alert fatigue implica la desensibilizzazione a segnali frequenti. L'autopilota indotto dalla routine implica il fallimento nel generare segnali in primo luogo—l'anomalia che attiverebbe un alert in un contesto nuovo fallisce nel registrarsi in un contesto di routine perché i processi di pattern-matching la categorizzano come "più dello stesso."

2.3.2 Caratteristiche della Manifestazione

Alert Fatigue e Autopilota nel commercial banking si manifesta come:

(1) **Automaticità nell'Approvazione delle Transazioni**: Dopo aver elaborato centinaia di transazioni legittime, i dipendenti sviluppano automaticità motoria per le azioni di approvazione. Il click di approvazione diventa un riflesso disconnesso dalla valutazione cognitiva.

(2) **Recitazione dello Script di Verifica**: Gli operatori di call center recitano le domande di verifica senza elaborare le risposte. La domanda viene posta, una risposta viene data, la domanda successiva segue—ma le risposte anomale non attivano indagini.

(3) **Normalizzazione della Gestione delle Eccezioni**: Le eccezioni che inizialmente richiedevano deliberazione diventano routine attraverso la ripetizione. L'eccezione che richiedeva l'approvazione del manager al mese uno viene gestita automaticamente al mese sei.

(4) **Degrado di Fine Turno**: La vigilanza cognitiva degrada attraverso la giornata lavorativa. Le transazioni elaborate nell'ultima ora prima della fine del turno ricevono meno scrutinio delle transazioni identiche elaborate nella prima ora.

(5) **Errori di Pattern Completion**: Quando elaborano informazioni presentate parzialmente, i dipendenti completano inconsciamente i pattern basandosi sulle aspettative. La transazione a cui mancano campi obbligatori viene "completata" mentalmente e approvata come se fosse completa.

2.3.3 Mapping Matematico

L'Autopilota si manifesta attraverso gli indicatori 5.1, 5.2 e 5.8 con calibrazione specifica per la ripetizione:

Indicatore 5.1 (Alert Fatigue) - Riformulazione Commercial Banking:

Alert fatigue standard: $F_a = 1 - \frac{investigated}{presented}$

L'autopilota del commercial banking richiede riformulazione perché gli alert non vengono presentati—falliscono nel generarsi:

$$AP^{CB}(e,t) = 1 - \frac{N_{flagged}(e,t)}{N_{flaggable}(e,t) \cdot P_{baseline}} \tag{7}$$

Dove:

- $N_{flagged}(e,t)$ = transazioni segnalate dal dipendente e nel periodo t
- $N_{flaggable}(e,t)$ = transazioni contenenti caratteristiche meritevoli di segnalazione
- $P_{baseline}$ = tasso di segnalazione baseline da elaborazione attenta

La detection si attiva quando il tasso di segnalazione scende sotto il baseline, indicando elaborazione in autopilota.

Indicatore 5.8 (Attention Residue) - Calibrazione Commercial Banking:

$$AR^{CB}(e,h) = \frac{E_{rate}(e,h)}{E_{rate}(e,h_0)} \cdot \frac{h - h_0}{H_{shift}} \tag{8}$$

Dove h indicizza l'ora all'interno del turno e h_0 è l'inizio del turno. Il rapporto cattura l'aumento del tasso di errore durante la durata del turno, normalizzato per la lunghezza del turno.

Nuova Metrica: Transaction Processing Rhythm Analysis

$$TPR(e,t) = \sigma\left(\{\Delta t_i\}_{i \in T(e,t)}\right) \tag{9}$$

Dove Δt_i è il tempo inter-transazione. Bassa varianza nel ritmo di elaborazione indica elaborazione automatica senza deliberazione. Le transazioni anomale dovrebbero produrre disruption del ritmo; l'assenza di disruption indica autopilota.

2.3.4 Aggiornamento Probabilità Condizionata

$$P^{CB}(5.x|2.x) = 0.65 \quad \text{(versus base } P(5.x|2.x) = 0.70) \tag{10}$$

La probabilità condizionata *ridotta* riflette che la pressione temporale (Categoria 2) è meno dominante nel retail banking che negli ambienti di trading. L'autopilota emerge dalla ripetizione piuttosto che dall'urgenza.

2.4 Manifestazione Categoria 6: Branch Loyalty vs. Policy

2.4.1 Fondamento Teorico

La Categoria 6 (Group Dynamic Vulnerabilities) affronta i processi psicologici collettivi che operano a livello di team e organizzativo, fondati sulla teoria delle dinamiche di gruppo di Bion (1961). Le filiali bancarie commerciali esibiscono dinamiche di gruppo distintive: team piccoli e stabili con lunga tenure, radicamento nella comunità locale, e co-localizzazione fisica che crea intensa identificazione in-group.

2.4.2 Caratteristiche della Manifestazione

Branch Loyalty vs. Policy descrive la prioritizzazione della solidarietà del team locale rispetto alla compliance con la policy organizzativa:

(1) **Condivisione Credenziali**: Lo staff di filiale condivide password, PIN e badge di accesso per consentire la copertura durante pause, assenze o picchi di carico di lavoro. "Siamo una squadra—ci aiutiamo a vicenda."

(2) **Mutual Exception Authorization**: I colleghi autorizzano le richieste di eccezione reciproche senza genuina revisione, creando reti di accommodamento reciproco che bypassano la segregation of duties.

(3) **Occultamento delle Violazioni**: I membri dello staff che osservano colleghi violare la policy non segnalano le violazioni, proteggendo i membri del team dalle conseguenze. La solidarietà di filiale supera l'obbligo di compliance.

(4) **Istituzionalizzazione dei Workaround**: Le procedure non ufficiali sviluppate dai singoli dipendenti diventano "come facciamo le cose qui" attraverso l'adozione del team, istituzionalizzando i bypass dei controlli a livello di filiale.

(5) **Percezione di Minaccia Esterna**: Le funzioni corporate di security e compliance sono percepite come minacce esterne al team di filiale piuttosto che risorse organizzative. Le preparazioni agli audit coinvolgono l'occultamento coordinato delle pratiche del team.

2.4.3 Mapping Matematico

Branch Loyalty si mappa sugli indicatori 6.3, 6.4 e 6.9 con calibrazione della co-localizzazione:

Indicatore 6.3 (Diffusion of Responsibility) - Calibrazione Commercial Banking:

$$DR^{CB}(b,t) = \frac{N_{shared\_auth}(b,t)}{N_{total\_auth}(b,t)} \cdot \frac{T_{tenure\_avg}(b)}{T_{baseline}} \tag{11}$$

Dove le autorizzazioni condivise aumentano con la tenure media, indicando che i team con maggiore anzianità sviluppano un accommodamento reciproco più esteso.

Nuova Metrica: Impossible Travel Within Branch

Detection della condivisione credenziali attraverso l'impossibilità fisica:

$$IT^{CB}(c,t) = \mathbf{1}\left[\exists(l_1, l_2, \Delta t) : d(l_1, l_2) > v_{max} \cdot \Delta t\right] \tag{12}$$

Dove c indicizza la credenziale, l_1, l_2 sono le location di login, Δt è il tempo tra i login, e v_{max} è la velocità massima plausibile di movimento. Login a postazioni fisicamente separate entro timeframe implausibili indicano condivisione delle credenziali.

Indicatore 6.9 (Organizational Splitting) - Calibrazione Commercial Banking:

Detection dello splitting filiale vs. corporate:

$$OS^{CB}(b,t) = \frac{S^{corporate}_{negative}(b,t)}{S^{corporate}_{total}(b,t)} - \frac{S^{branch}_{negative}(b,t)}{S^{branch}_{total}(b,t)} \tag{13}$$

Dove S rappresenta punteggi di sentiment dalle comunicazioni interne. Valori positivi elevati indicano splitting: il corporate è "cattivo," il team di filiale è "buono."

2.4.4 Aggiornamento Probabilità Condizionata

$$P^{CB}(6.x|7.x) = 0.75 \quad \text{(versus base } P(6.x|7.x) = 0.60) \tag{14}$$

Le condizioni di stress (Categoria 7) attivano fortemente i comportamenti protettivi del gruppo negli ambienti di filiale, poiché i team si chiudono sotto pressione.

2.5 Manifestazione Categoria 9: Dipendenza da Chatbot e CRM

2.5.1 Fondamento Teorico

La Categoria 9 (AI-Specific Bias Vulnerabilities) affronta i pattern di interazione human-AI. Il commercial banking ha estensivamente deployato AI attraverso chatbot customer-facing, sistemi di raccomandazione CRM e strumenti di autenticazione automatizzati. Gli operatori di call center dipendono sempre più dalle raccomandazioni di verifica cliente fornite dall'AI e dalla guida alle interazioni.

2.5.2 Caratteristiche della Manifestazione

Dipendenza da Chatbot e CRM descrive l'over-trust nei sistemi AI che supportano le interazioni con i clienti:

(1) **Delega della Verifica**: Gli operatori di call center deferiscono agli indicatori "cliente verificato" forniti dal CRM senza valutazione indipendente. Se il sistema dice che il cliente è verificato, l'operatore procede—anche quando il contenuto della conversazione suggerisce preoccupazioni sull'identità.

(2) **Over-Trust nell'Autenticazione Vocale**: I sistemi biometrici vocali sono fidati oltre la loro accuratezza. Gli operatori che ricevono "corrispondenza vocale confermata" ignorano anomalie comportamentali che suggeriscono che la corrispondenza vocale potrebbe essere spoofata o l'account compromesso nonostante la voce legittima.

(3) **Assunzione di Handoff dal Chatbot**: Quando i clienti passano dal chatbot all'operatore umano, gli operatori assumono che la verifica condotta dal chatbot fosse adeguata. Gli avversari che compromettono le interazioni con il chatbot ereditano la verifica assunta.

(4) **Seguire le Raccomandazioni CRM**: Gli operatori seguono gli script e le risposte suggeriti dal CRM senza valutazione critica. Quando le raccomandazioni CRM sono manipolate (attraverso il poisoning della storia dell'account o il social engineering delle interazioni precedenti), gli operatori eseguono la guida manipolata.

(5) **Vulnerabilità Deepfake Voice**: Con l'avanzare della tecnologia di sintesi vocale, i sistemi biometrici vocali affrontano attacchi adversarial. Gli operatori che si fidano dello status "voce verificata" potrebbero interagire con voci sintetiche costruite da campioni vocali trapelati.

2.5.3 Mapping Matematico

Dipendenza da Chatbot/CRM si mappa sugli indicatori 9.2, 9.4 e 9.7:

Indicatore 9.2 (Automation Bias Override) - Calibrazione Commercial Banking:

$$OR^{CB}(a,t) = \frac{N_{human\_override}(a,t)}{N_{AI\_flag}(a,t) + N_{AI\_clear}(a,t)} \tag{15}$$

La detection si attiva quando il tasso di override scende sotto 0.03 (gli operatori overridano l'AI meno del 3% delle volte, indicando eccessiva deferenza).

Nuova Metrica: Verification Source Correlation

$$VSC(t) = \rho\left(V_{AI}(t), V_{human}(t)\right) \tag{16}$$

Dove V_{AI} e V_{human} sono decisioni di verifica. Correlazione che si avvicina a 1.0 indica che la verifica umana rispecchia la verifica AI piuttosto che fornire una valutazione indipendente.

Indicatore 9.7 (AI Hallucination Acceptance) - Calibrazione Voice Authentication:

$$VAR^{CB} = P(\text{frode} \mid \text{voice\_verified}) \cdot \frac{1}{\text{confidence}_{voice}} \tag{17}$$

Un tasso di frode elevato tra le interazioni "voce verificata" indica sfruttamento del sistema di autenticazione vocale.

2.5.4 Aggiornamento Probabilità Condizionata

$$P^{CB}(9.x|5.x) = 0.80 \quad (\text{versus base } P(9.x|5.x) = 0.55) \tag{18}$$

L'overload cognitivo/autopilota (Categoria 5) predice fortemente l'over-reliance sull'AI nel commercial banking—gli operatori in modalità autopilota deferiscono all'AI piuttosto che ingaggiare il giudizio indipendente.

3 Strategia di Intervento CPIF nel Commercial Banking

Il Cybersecurity Psychology Intervention Framework (CPIF) fornisce la metodologia per tradurre la valutazione delle vulnerabilità in cambiamento organizzativo (Canale, 2025c). L'applicazione al commercial banking richiede adattamento alle reti di filiali distribuite, alle culture basate sulle metriche di servizio e alle dinamiche della workforce frontline.

3.1 Fase 1: Readiness Assessment nel Commercial Banking

3.1.1 Service-Security Culture Assessment

La domanda fondamentale di readiness nel commercial banking: L'organizzazione percepisce la sicurezza come un enabler del business o un impedimento al business?

$$R_{culture} = \frac{W_{security}}{W_{security} + W_{service}} \cdot A_{leadership} \tag{19}$$

Dove:

- $W_{security}$ = peso assegnato alle metriche di sicurezza nella valutazione delle performance
- $W_{service}$ = peso assegnato alle metriche di servizio nella valutazione delle performance
- $A_{leadership}$ = allineamento della leadership sull'integrazione sicurezza-servizio

Quando $R_{culture} < 0.3$ (peso della sicurezza inferiore al 30% del peso combinato sicurezza-servizio), il readiness-building deve precedere l'implementazione dell'intervento.

3.1.2 Branch Network Readiness Variance

A differenza delle operazioni centralizzate, la readiness del commercial banking varia attraverso la rete di filiali:

$$R_{network} = \mu(R_b) - \lambda \cdot \sigma(R_b) \tag{20}$$

Dove la media della readiness a livello di filiale è penalizzata dalla varianza. Alta varianza indica readiness inconsistente che complica il deployment dell'intervento a livello di network.

3.1.3 Legacy Technology Readiness Factor

I vincoli dei legacy system limitano le opzioni di intervento:

$$R_{tech} = \frac{N_{modern}}{N_{total}} \cdot \frac{C_{integration}}{C_{replacement}} \tag{21}$$

Dove il rapporto cattura sia la prevalenza dei sistemi moderni sia la fattibilità di integrare controlli di sicurezza versus sostituire i legacy system.

3.2 Fase 2: Vulnerability-Intervention Matching

3.2.1 Interventi per la Sindrome del Cliente VIP (Manifestazione Categoria 1)

(1) **Verifica Relationship-Blind**: Implementare procedure di verifica che non possono essere bypassate indipendentemente dalla relazione con il cliente. Verifica biometrica, codici di conferma transazione e callback automatizzati operano indipendentemente dalla discrezione del dipendente.

(2) **VIP-Specific Threat Awareness**: Training che enfatizza che i clienti VIP sono *target di maggior valore* per l'impersonation, non relazioni a minor rischio. La prominenza del cliente aumenta, non diminuisce, l'importanza della verifica.

(3) **Intensità di Audit sulle Eccezioni**: Implementare attenzione di audit sproporzionata alle eccezioni per clienti VIP. I dipendenti che sanno che le eccezioni VIP ricevono scrutinio enhanced applicheranno la verifica standard.

(4) **Accountability del Relationship Manager**: Assegnare accountability di sicurezza esplicita ai relationship manager. Le perdite per frode attribuite al bypass della verifica impattano le metriche di performance del relationship manager.

3.2.2 Interventi per Frontline Empathy (Manifestazione Categoria 3)

(1) **Empathy-Security Integration**: Formare lo staff frontline che la sicurezza *è* customer service—proteggere i clienti dalla frode è il servizio ultimo. Reframe della verifica come cura, non sospetto.

(2) **Manipulation Recognition Training**: Fornire training specifico sulle tattiche di social engineering che sfruttano l'empatia. Lo staff che riconosce le tecniche di manipolazione può mantenere l'empatia mentre resiste allo sfruttamento.

(3) **Structured Verification Scripts**: Implementare script di verifica che non possono essere abbreviati sotto pressione sociale. I campi obbligatori devono essere completati; il sistema enforza ciò che i dipendenti potrebbero bypassare.

(4) **Supervisor Escalation Protocols**: Fornire path di escalation chiari per situazioni in cui i clienti fanno pressione sui dipendenti per bypassare la verifica. Il dipendente che escala è protetto; il dipendente che accommoda è accountable.

3.2.3 Interventi per l'Autopilota (Manifestazione Categoria 5)

L'autopilota emerge dalla ripetizione; l'intervento deve interrompere la ripetizione:

(1) **Programmi di Job Rotation**: Ruotare i dipendenti attraverso ruoli e funzioni per prevenire il radicamento dei pattern. Il dipendente che elaborava depositi il mese scorso elabora prelievi questo mese.

(2) **Deliberate Friction Injection**: Introdurre variazioni procedurali che richiedono attenzione consapevole. Ordine randomizzato delle domande di verifica. Schermate periodiche di "conferma" che richiedono acknowledgment attivo.

(3) **Transaction Sampling Alerts**: Campionare casualmente transazioni per enhanced review, creando incertezza su quali transazioni riceveranno scrutinio. I dipendenti che non possono prevedere lo scrutinio non possono selettivamente ingaggiare l'attenzione.

(4) **Elementi di Gamification**: Introdurre elementi competitivi o game-like nell'elaborazione di routine. "Fraud detection leaderboard." Riconoscimento per anomalie segnalate. Meccanismi di engagement che attivano l'attenzione.

(5) **Shift Structure Optimization**: Analizzare i pattern di errore per posizione nel turno e ottimizzare timing delle pause, sequenziamento dei task e durata del turno per minimizzare le finestre di autopilota.

3.2.4 Interventi per Branch Loyalty (Manifestazione Categoria 6)

(1) **Cross-Branch Rotation**: Rotazione periodica dello staff attraverso le filiali interrompe le dinamiche di team radicate. I dipendenti con esperienza multi-filiale sono meno catturati dalla loyalty verso una singola filiale.

(2) **Individual Accountability Reinforcement**: Implementare tracking individuale delle credenziali che rende la condivisione delle credenziali immediatamente rilevabile e individualmente attribuibile. Rimuovere l'anonimato che abilita la condivisione.

(3) **Compliance Integration into Team Identity**: Reframe della compliance come valore del team piuttosto che imposizione esterna. I team di filiale competono sulle metriche di compliance; la sicurezza diventa fonte di orgoglio del team.

(4) **Anonymous Reporting Channels**: Fornire meccanismi per segnalare violazioni di policy senza identificazione dei peer. I dipendenti che non segnalerebbero pubblicamente potrebbero segnalare anonimamente.

3.2.5 Interventi per AI Over-Reliance (Manifestazione Categoria 9)

(1) **AI Confidence Display**: Richiedere ai sistemi AI di visualizzare i livelli di confidence in modo prominente. Gli operatori vedono non solo "verificato" ma "verificato (78% confidence)"—calibrando l'attenzione umana all'incertezza dell'AI.

(2) **Mandatory Independent Verification**: Per transazioni ad alto rischio, richiedere step di verifica umana che non possono essere soddisfatti dall'AI da sola. Raccomandazione AI più verifica umana, non raccomandazione AI come verifica.

(3) **AI Failure Training**: Formare gli operatori sui limiti e le modalità di fallimento dei sistemi AI. Gli operatori che comprendono come l'AI può essere ingannata mantengono appropriato scetticismo.

(4) **Voice Authentication Supplementation**: Supplementare la biometria vocale con fattori comportamentali e contestuali. Corrispondenza vocale più consistenza comportamentale più plausibilità contestuale, non corrispondenza vocale da sola.

3.3 Fase 3: Resistance Navigation

3.3.1 Resistenza "Non Ho Tempo per la Sicurezza"

Pattern di Resistenza: "Ho clienti in attesa. Non ho tempo di fare tutti questi step di verifica."

Strategia di Navigation: Affrontare il conflitto di metriche sottostante. Se i dipendenti sono misurati sul throughput e penalizzati per l'investimento di tempo in sicurezza, la resistenza è razionale. L'intervento richiede ridisegno delle metriche: il tempo di sicurezza è contato positivamente nelle metriche di produttività, o le metriche di sicurezza sono pesate equivalentemente alle metriche di servizio.

La funzione di ribilanciamento delle metriche:

$$M_{rebalanced} = \alpha \cdot M_{service} + \beta \cdot M_{security} + \gamma \cdot M_{quality} \tag{22}$$

Dove $\beta \geq \alpha$ elimina il trade-off servizio-sicurezza che genera resistenza.

3.3.2 Resistenza "Il Sistema È il Problema"

Pattern di Resistenza: "Se i sistemi non fossero così lenti e complicati, non avrei bisogno di workaround."

Strategia di Navigation: Questa resistenza spesso riflette una lamentela legittima. La frustrazione da legacy system è reale. La navigation richiede di riconoscere la lamentela legittima mentre si separa il miglioramento del sistema (che dovrebbe procedere) dalla compliance di sicurezza (che non può aspettare il miglioramento del sistema). Soluzioni intermedie che riducono la friction legittima mantenendo i controlli di sicurezza dimostrano responsività organizzativa.

3.3.3 Resistenza "Siamo una Famiglia Qui"

Pattern di Resistenza: "Ci fidiamo l'uno dell'altro. Non abbiamo bisogno di questi controlli—non siamo criminali."

Strategia di Navigation: Reframe dei controlli come protezione del team, non sospetto verso di esso. "Questi controlli ti proteggono quando qualcuno fuori dal team cerca di sfruttare i nostri sistemi. Proteggono i tuoi colleghi dall'essere incolpati quando qualcosa va storto." I controlli servono la famiglia piuttosto che controllarla.

3.4 Fase 4: Performance Metric Redesign

L'intervento sostenibile nel commercial banking richiede un ridisegno fondamentale delle metriche che elimini il conflitto servizio-sicurezza:

Table 1: Commercial Banking Metric Redesign Framework

Metrica Tradizionale	Problema di Sicurezza	Metrica Ridisegnata
Average Handle Time (AHT)	Penalizza verifica approfondita	AHT con esclusione step di sicurezza
First Call Resolution	Incoraggia accommodamento	Punteggio di qualità della risoluzione
Transazioni Per Ora	Premia velocità su accuratezza	Transazioni accurate per ora
Customer Satisfaction	Penalizza friction di verifica	Soddisfazione con protezione frodi

4 Implementazione Tecnica: Schema OFTLISRV per il Commercial Banking

4.1 Integrazione Data Source

Fonti di telemetria del commercial banking:

Table 2: Commercial Banking Data Source Mapping

Data Source	Categorie CPF	Metodo di Integrazione
Core Banking System	1.x, 5.x	Analisi transaction log
Workstation Access Logs	6.x	Pattern di utilizzo credenziali
Call Recording Systems	3.x, 4.x, 9.x	Pipeline speech analytics
CRM/Customer Data	1.x, 9.x	Correlazione valore relazione
Physical Access Systems	6.x	Pattern utilizzo badge
Workforce Management	5.x, 7.x	Analisi turni/fatigue

4.2 Branch-Level Detection: Condivisione Credenziali

La metrica "Impossible Travel Within Branch" richiede integrazione con la topologia fisica:

$$D_{6.x}^{CB}(c,t) = \sum_{(l_1,l_2,\Delta t)\in L(c,t)} \mathbf{1}\left[\frac{d(l_1,l_2)}{\Delta t} > v_{threshold}\right] \cdot w(l_1,l_2) \tag{23}$$

Dove $w(l_1, l_2)$ pesa per separazione fisica delle postazioni. Le detection a postazioni fisicamente distanti ricevono peso maggiore delle detection a postazioni adiacenti (che potrebbero riflettere movimento rapido legittimo).

4.3 Call Center Detection: Security Question Correlation

La metrica del call center che correla durata della chiamata con completamento delle domande di sicurezza:

$$D_{3.x}^{CB}(a,t) = \rho\left(\frac{T_{call}(a,i)}{T_{target}}, \frac{Q_{completed}(a,i)}{Q_{required}(a,i)}\right)_{i\in C(a,t)} \tag{24}$$

Correlazione negativa (chiamate più brevi associate a meno domande di sicurezza) indica bypass guidato dalla pressione.

4.4 Transaction Rhythm Analysis

Detection dell'autopilota attraverso il ritmo di elaborazione:

$$D_{5.x}^{CB}(e,t) = 1 - \frac{\sigma(\{\Delta t_i\})_{i\in T(e,t)}}{\sigma_{baseline}} \tag{25}$$

Dove varianza del ritmo ridotta (elaborazione più metronomica) indica elaborazione automatica piuttosto che deliberativa.

4.5 Convergence Index: Calibrazione Commercial Banking

$$CI^{CB} = \prod_{i=1}^{n}(1 + v_i^{CB}) \cdot F(t) \tag{26}$$

Dove il fattore temporale:

$$F(t) = \begin{cases} 1.0 & \text{operazioni normali} \\ 1.3 & \text{elaborazione fine mese} \\ 1.5 & \text{venerdì pomeriggio} \\ 2.0 & \text{venerdì pomeriggio fine mese} \\ 2.5 & \text{festività/staff ridotto} \end{cases} \tag{27}$$

5 Case Study: Il Bonifico del Venerdì Pomeriggio

5.1 Panoramica dell'Incidente

Il [Data Redatta], alle 16:23 di un venerdì, la filiale [Banca Redatta] di [Location Redatta] ha elaborato un bonifico di €847.000 basandosi su una telefonata presumibilmente dall'AD di un cliente commerciale. Il trasferimento era fraudolento, rappresentando una variante di business email compromise (BEC) eseguita via voce piuttosto che email. Il direttore di filiale ha approvato il trasferimento senza la richiesta doppia autorizzazione, bypassando i controlli che avrebbero prevenuto la perdita.

5.2 Sequenza dell'Attacco

5.2.1 Fase 1: Ricognizione (T-30g a T-7g)

Gli avversari hanno raccolto intelligence:

- Struttura organizzativa dell'azienda (nome AD, nome CFO, relazioni bancarie)
- Informazioni sulla filiale (nome direttore, pattern tipici di transazione)
- Intelligence temporale (programma viaggi CFO, pattern di staffing venerdì pomeriggio)
- Campioni vocali (registrazioni di public speaking dell'AD per potenziale sintesi vocale)

5.2.2 Fase 2: Sviluppo del Pretesto (T-7g a T-0)

Preparazione dell'attacco:

- Setup spoofing dominio email (dominio aziendale dell'AD con sostituzione caratteri)
- Email di "preavviso" al direttore di filiale: "Potrei aver bisogno di raggiungerla urgentemente venerdì pomeriggio per una transazione confidenziale"
- Apertura conto beneficiario per ricevere i fondi

5.2.3 Fase 3: Esecuzione (T-0, Venerdì 16:23)

Condizioni ambientali all'esecuzione:

- Direttore di filiale in turno dalle 7:30 (8+ ore trascorse)
- Staff ridotto per partenze tipiche del venerdì pomeriggio
- Prossimità fine mese che crea pressione da backlog di elaborazione
- Coda clienti visibile dall'ufficio del direttore

La telefonata:

- Chiamante identificatosi come AD, ha fatto riferimento all'email di "preavviso"
- Ha spiegato acquisizione confidenziale che richiedeva trasferimento fondi immediato
- Ha enfatizzato segretezza: "Non ne parli con nessuno—neanche col CFO per ora"
- Ha creato urgenza: "Il venditore ha bisogno dei fondi entro le 17 o l'affare salta"
- Ha applicato pressione d'autorità: "Conto su di lei per far succedere questo"

5.2.4 Fase 4: Bypass dei Controlli

Il direttore di filiale:

- Non ha verificato l'identità del chiamante attraverso callback a numero conosciuto
- Non ha ottenuto la richiesta doppia autorizzazione (firma secondo funzionario)
- Non ha verificato il conto beneficiario attraverso canali stabiliti
- Ha elaborato il trasferimento come "autorizzato AD" con singola approvazione

Convergence index al momento della transazione: $CI^{CB} = 3.2$ (soglia critica: 2.5)

5.2.5 Fase 5: Scoperta e Risposta

La scoperta è avvenuta lunedì mattina quando:

- Il CFO ha revisionato i report delle transazioni del weekend
- L'AD ha confermato nessuna attività di acquisizione
- I fondi erano stati accreditati su conto estero, irrecuperabili

5.3 Analisi CPF

Table 3: Bonifico del Venerdì Pomeriggio: Mapping delle Categorie

Categoria	Manifestazione	Sfruttamento
1.x	Cliente VIP (autorità)	Autorità AD invocata per bypassare controlli
2.x	Pressione temporale	Venerdì 16:23, urgenza fine giornata
3.x	Influenza sociale	Reciprocità (email precedente), liking (relazione)
5.x	Fatigue cognitiva	Turno 8+ ore, elaborazione fine mese
7.x	Risposta allo stress	Pressione temporale, pressione autorità combinate
10.x	Stato convergente	Multiple categorie allineate

5.4 Lezioni per l'Implementazione CB-CPF

(1) **Mandatory Callback Verification**: Le richieste di bonifico sopra soglia richiedono callback a numeri pre-registrati, indipendentemente dall'identità asserita dal chiamante o dalle affermazioni di urgenza.

(2) **Dual Authorization Enforcement**: Doppia autorizzazione enforced dal sistema che non può essere bypassata da singolo utente, indipendentemente dal livello di autorità o pressione temporale.

(3) **Strategic Pause Implementation**: Per transazioni ad alto valore, periodi di ritardo obbligatori ("cooling off") che forniscono tempo per la verifica e riducono l'efficacia dello sfruttamento dell'urgenza.

(4) **Convergent State Monitoring**: Monitoraggio real-time del convergence index con escalation automatica quando CI^{CB} supera le soglie durante l'elaborazione delle transazioni.

(5) **Friday Afternoon Protocols**: Controlli enhanced attivati automaticamente durante finestre temporali ad alto rischio (venerdì pomeriggio, fine mese, pre-festività).

6 Conclusione

6.1 L'Ultimo Miglio della Sicurezza Bancaria

La sicurezza del commercial banking dipende ultimamente dalle decisioni umane prese ai banconi delle filiali, alle scrivanie dei call center e alle postazioni di back-office. I controlli tecnici stabiliscono confini; il giudizio umano opera all'interno di quei confini. Il CB-CPF affronta i fattori psicologici che determinano se il giudizio umano rafforza o mina i controlli tecnici.

Le sfide distintive del commercial banking—tensione servizio-sicurezza, cecità indotta dalla routine, autorità basata sulle relazioni, dinamiche di team di filiale—richiedono approcci calibrati distinti dai contesti dell'investment banking o assicurativi. Il CB-CPF fornisce queste calibrazioni mantenendo la compatibilità con la tassonomia Core 10 e l'architettura dell'Implementation Companion.

6.2 Resilienza Operativa Attraverso la Consapevolezza Psicologica

Le banche commerciali che implementano il CB-CPF acquisiscono la capacità di:

- Rilevare la condivisione credenziali attraverso l'analisi impossible-travel
- Identificare l'elaborazione in autopilota attraverso l'analisi del ritmo
- Monitorare il trade-off servizio-sicurezza attraverso la correlazione delle metriche
- Predire le finestre di stato convergente attraverso l'analisi dei pattern temporali
- Intervenire proattivamente prima che le vulnerabilità psicologiche siano sfruttate

6.3 Roadmap di Validazione

Il lavoro futuro validerà le calibrazioni CB-CPF attraverso:

(1) Implementazioni pilota attraverso reti di filiali diverse

(2) Analisi di correlazione tra punteggi CB-CPF e tassi di incidenti di frode

(3) A/B testing nei call center dell'efficacia degli interventi

(4) Studio longitudinale dell'impatto del ridisegno delle metriche sugli outcome di sicurezza

La sicurezza del Main Street banking dipende dalla comprensione della psicologia dei Main Street banker. Il CB-CPF fornisce quella comprensione.

Nota sulla Composizione AI-Assistita

Questo manoscritto presenta il framework teorico originale e i contributi intellettuali dell'autore. Nel processo di composizione, l'autore ha utilizzato un large language model come strumento ausiliario per il raffinamento stilistico e la consistenza della formattazione. Le idee core, l'architettura CB-CPF, l'integrazione teorica e l'analisi strategica sono esclusivamente il prodotto dell'expertise dell'autore. L'autore è interamente responsabile per l'accuratezza e l'integrità del contenuto pubblicato.

Ringraziamenti

L'autore riconosce il lavoro fondazionale nelle operazioni di retail banking, nella psicologia della gestione di filiale e nei fattori umani dei call center su cui il CB-CPF si costruisce.

References

Bion, W. R. (1961). *Experiences in groups*. London: Tavistock Publications.

Canale, G. (2025a). The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model. *CPF Technical Report Series*.

Canale, G. (2025b). Operationalizing the Cybersecurity Psychology Framework: A Systematic Implementation Methodology. *CPF Technical Report Series*.

Canale, G. (2025c). The Cybersecurity Psychology Intervention Framework: A Meta-Model for Addressing Human Vulnerabilities. *CPF Technical Report Series*.

Canale, G. (2025d). Financial Services Cybersecurity Psychology Framework (FS-CPF v2.0). *CPF Technical Report Series*.

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York: Collins.

Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

Milgram, S. (1974). *Obedience to authority*. New York: Harper & Row.