La Profondità Sottostante: Fondamenta Teoriche e Operative del Cybersecurity Psychology Framework

Technical Foundation Paper

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

16 dicembre 2025

Sommario

Il Cybersecurity Psychology Framework, come presentato nella sua pubblicazione iniziale, offre una tassonomia strutturata di cento indicatori attraverso dieci categorie che mappano le vulnerabilità psicologiche sugli esiti di sicurezza. Ciò che quella presentazione necessariamente non poteva trasmettere è la profondità dell'integrazione teorica, dell'architettura metodologica e dell'infrastruttura operativa che sottende questa classificazione apparentemente lineare. Questo paper apre quello strato più profondo. Esaminiamo le sfide fondamentali dell'integrare tradizioni psicologiche disparate in un modello predittivo coerente, articoliamo la scelta deliberata dell'orientamento diagnostico rispetto a quello prescrittivo, esponiamo l'architettura di assessment che traduce i costrutti teorici in fenomeni misurabili, e mappiamo le complesse interdipendenze tra indicatori che trasformano osservazioni isolate in profili di rischio sistemico. L'ecosistema operativo che circonda il framework, inclusi i meccanismi di scoring, i modelli di maturità e i percorsi di integrazione con i security operations center, emerge da queste fondamenta come conseguenza necessaria piuttosto che aggiunta arbitraria. Per coloro che vorrebbero contribuire all'evoluzione di questo lavoro, comprendere queste fondamenta non è preparazione opzionale ma prerequisito essenziale.

1 Introduzione: Il Visibile e l'Invisibile

Quando un framework si presenta come una matrice di categorie e indicatori, c'è un'inevitabile tentazione di valutarlo a quel livello superficiale. Il Cybersecurity Psychology Framework,

nella sua forma pubblicata, appare precisamente come tale struttura: dieci categorie, cento indicatori, scoring ternario, mappature dei vettori di attacco. Un lettore potrebbe ragionevolmente concludere che il lavoro consiste in questa tassonomia, forse informata dai riferimenti teorici citati accanto a ogni categoria. Tale conclusione sarebbe comprensibile. Sarebbe anche profondamente incompleta.

La tassonomia che i professionisti incontrano rappresenta l'interfaccia operativa di un apparato teorico e metodologico considerevolmente più complesso. Questa non è complessità fine a se stessa, né l'inflazione accademica che aggiunge elaborazione senza sostanza. La profondità esiste perché il problema la richiede. La vulnerabilità psicologica umana nei contesti di sicurezza non può essere adeguatamente catturata da semplici checklist o categorizzazioni intuitive. I fenomeni coinvolti operano attraverso molteplici livelli di coscienza, emergono sia da dinamiche individuali che collettive, si manifestano attraverso pattern comportamentali che resistono all'osservazione diretta, e interagiscono tra loro in modi che trasformano i profili di rischio in maniera non lineare.

Ciò che segue in questo paper è un'esposizione di ciò che giace sotto il framework visibile. Procediamo non per impressionare con sofisticazione teorica ma per equipaggiare coloro che lavorerebbero con questo materiale, sia come ricercatori che cercano di validarne le affermazioni, sia come professionisti che implementano le sue valutazioni, sia come contributori che ne estendono la portata. La superficie è dove avvengono le operazioni. La profondità è dove risiede la comprensione.

Il lettore che si è confrontato con la presentazione iniziale del framework possiede la mappa. Questo paper fornisce il terreno.

2 Il Problema dell'Integrazione

Le fondamenta teoriche citate nel Cybersecurity Psychology Framework abbracciano tradizioni che non comunicano naturalmente. La teoria delle relazioni oggettuali come sviluppata da Melanie Klein opera all'interno di un framework metapsicologico fondamentalmente diverso dalla psicologia cognitiva di Daniel Kahneman. Le dinamiche di gruppo di Wilfred Bion emergono dall'osservazione psicoanalitica di gruppi terapeutici, un contesto lontano dalla psicologia sociale sperimentale dell'influenza di Robert Cialdini. La psicologia analitica di Carl Jung, con la sua enfasi sui pattern archetipici e l'inconscio collettivo, condivide poco terreno metodologico con i modelli di elaborazione dell'informazione di George Miller. Semplicemente citare queste fonti accanto agli indicatori rilevanti, come fa la presentazione iniziale del framework, crea un'apparenza di fondamento teorico. L'integrazione effettiva richiede considerevolmente di più.

La sfida non è meramente terminologica, sebbene la confusione terminologica certamente esista. Quando Klein parla di "scissione" come meccanismo di difesa primitivo che divide gli oggetti in totalmente buoni o totalmente cattivi, e quando osserviamo tendenze organizzative a categorizzare gli insider come affidabili e gli outsider come minacciosi, la corrispondenza apparente può mascherare una distanza concettuale significativa. La scissione di Klein avviene intrapsichicamente, nel mondo interno delle rappresentazioni oggettuali. La scissione organizzativa si manifesta in policy, procedure e assunzioni culturali. Il passaggio dall'una all'altra richiede un ponte teorico che il framework psicoanalitico originale non fornisce.

Gap simili appaiono in tutte le basi teoriche del framework. Le assunzioni di base di Bion di dipendenza, attacco-fuga e accoppiamento descrivono stati regressivi nei gruppi sotto ansia, stati che interferiscono con la funzione lavorativa del gruppo. Applicare questi concetti ai security operations center o ai team di incident response richiede di specificare come queste dinamiche di gruppo inconsce si manifestano in contesti tecnologicamente mediati, procedu-

ralmente strutturati, organizzativamente incorporati. La teoria non rende questa applicazione automatica.

L'integrazione che abbiamo sviluppato affronta questi gap attraverso quello che potrebbe essere definito modellazione traduttiva. Per ogni costrutto teorico incorporato nel framework, abbiamo specificato le manifestazioni osservabili nei contesti di sicurezza organizzativa, gli approcci di misurazione che possono catturare queste manifestazioni senza violare il significato essenziale del costrutto, le condizioni al contorno entro le quali l'applicazione rimane valida, e le relazioni con altri costrutti che possono modificare o mediare il fenomeno. Questo lavoro traduttivo non è visibile nella presentazione operativa del framework. È, tuttavia, presente nella specificazione di ogni indicatore.

Consideriamo l'integrazione della teoria del doppio processo di Kahneman con le assunzioni di base di Bion. A prima vista, queste teorie affrontano fenomeni diversi: la cognizione individuale versus le dinamiche di gruppo. Eppure la loro interazione si rivela cruciale per comprendere la vulnerabilità di sicurezza. Quando un'organizzazione opera sotto un'assunzione di base di dipendenza, cercando protezione da un leader o vendor idealizzato, la risultante riduzione dell'ansia permette all'elaborazione del Sistema 2 di rimanere ingaggiata. La valutazione critica continua, anche se mal indirizzata. Quando la stessa organizzazione passa all'attacco-fuga, percependo minaccia esistenziale da attaccanti esterni, il Sistema 1 domina. Risposte rapide, euristiche, guidate emotivamente sostituiscono l'analisi deliberativa. L'assunzione di base non descrive meramente uno stato di gruppo; predice la modalità cognitiva che i singoli membri impiegheranno prevalentemente.

Questa interazione tra dinamiche di gruppo e cognizione individuale esemplifica la profondità integrativa che il framework richiede. L'indicatore per le posture di sicurezza attacco-fuga nella categoria sei non sta da solo. Si connette agli indicatori per la compromissione da stress acuto nella categoria sette, agli indicatori per la paralisi decisionale basata sulla paura nella categoria quattro, agli indicatori per il tunneling cognitivo nella categoria cinque. Queste connessioni non sono additive. Sono moltiplicative, trasformative, emergenti.

3 Il Paradosso Diagnostico-Intervento

Una risposta ragionevole a qualsiasi framework di valutazione delle vulnerabilità è chiedere cosa si dovrebbe fare riguardo alle vulnerabilità identificate. Il Cybersecurity Psychology Framework resiste deliberatamente nel fornire risposte prescrittive a questa domanda. Questa resistenza non è evasione ma principio.

L'istinto di abbinare diagnosi e prescrizione è profondamente radicato nei campi tecnici. Quando uno scanner di vulnerabilità identifica un sistema non patchato, la prescrizione è evidente: applicare la patch. Quando un penetration test rivela un firewall mal configurato, il percorso di remediation è chiaro: correggere la configurazione. Questo abbinamento diagnostico-prescrittivo funziona perché i sistemi tecnici, sebbene complessi, operano secondo specifiche documentate. La relazione tra problema identificato e soluzione efficace può essere stabilita con ragionevole certezza.

Le vulnerabilità psicologiche non condividono questa caratteristica. Quando una valutazione identifica elevata suscettibilità alla manipolazione basata sull'autorità in una particolare unità organizzativa, non esiste una patch equivalente. Il percorso di remediation dipende da fattori che il framework non può conoscere: le specifiche strutture di autorità in quell'unità, le esperienze storiche che hanno plasmato i pattern correnti, gli individui coinvolti e le loro particolari configurazioni psicologiche, la più ampia cultura organizzativa all'interno della quale l'unità

opera, le risorse disponibili per l'intervento, le priorità concorrenti che plasmeranno qualsiasi sforzo di cambiamento.

Un framework che fornisce soluzioni prescrittive per le vulnerabilità psicologiche affronta una scelta scomoda. Può offrire raccomandazioni generiche sufficientemente astratte da evitare errori specifici del contesto, nel qual caso quelle raccomandazioni forniscono poca guida azionabile. Alternativamente, può offrire interventi specifici, nel qual caso quegli interventi saranno inappropriati per molti contesti in cui vengono applicati. Nessuna delle due opzioni serve bene i professionisti.

Il CPF affronta questo paradosso mantenendo un focus strettamente diagnostico mentre articola pattern di intervento a un livello di astrazione che riconosce la variazione contestuale. Un pattern di intervento non è una prescrizione. È una classe di approcci che hanno dimostrato rilevanza per particolari tipi di vulnerabilità, dalla quale i professionisti devono selezionare e adattare in base alle loro specifiche circostanze.

Per le vulnerabilità basate sull'autorità, i pattern di intervento includono meccanismi che introducono attrito nella conformità alle richieste di autorità, requisiti di verifica multi-canale che non possono essere soddisfatti attraverso lo stesso vettore di comunicazione della richiesta originale, approcci formativi che costruiscono il riconoscimento delle tecniche di manipolazione dell'autorità, e cambiamenti organizzativi che riducono il gradiente di autorità che inibisce la segnalazione di problemi di sicurezza. Queste non sono istruzioni da seguire. Sono direzioni da esplorare.

La distinzione conta per la validazione così come per l'implementazione. Un framework prescrittivo invita alla valutazione basata sul fatto che le sue prescrizioni funzionino. Questa valutazione è diretta ma fuorviante, perché la qualità dell'implementazione varia enormemente tra i contesti. Un framework diagnostico con pattern di intervento invita alla valutazione basata sul fatto che le sue diagnosi identifichino accuratamente le vulnerabilità che, quando affrontate attraverso mezzi contestualmente appropriati, mostrano miglioramento misurabile. Questa valutazione è più complessa ma più significativa.

4 Architettura dell'Assessment

I cento indicatori del CPF non possono essere valutati attraverso cento domande. La relazione tra costrutto teorico e strumento di misurazione non è mai uno-a-uno, particolarmente per i fenomeni psicologici che resistono all'osservazione diretta. L'architettura di assessment sottostante al framework comprende approssimativamente 2.300 item organizzati attraverso molteplici modalità di misurazione, ogni item mappato a specifici indicatori attraverso collegamenti teorici espliciti.

L'architettura riflette un principio fondamentale di misurazione: la validità convergente richiede molteplici operazionalizzazioni. Una singola domanda sulla suscettibilità al bypass di sicurezza indotto dall'urgenza, per quanto attentamente formulata, non può catturare adeguatamente quel fenomeno. La desiderabilità sociale di apparire competenti sotto pressione distorcerà l'auto-report. La variabilità delle esperienze di urgenza tra i ruoli introdurrà rumore. La natura retrospettiva della maggior parte dei contesti di valutazione distorcerà il ricordo. Una misurazione adeguata richiede di approcciare il costrutto da angoli multipli, usando tipi di item multipli, e aggregando attraverso istanze multiple.

L'assessment quindi incorpora item basati su scenari che presentano situazioni realistiche che richiedono giudizio, item sulla frequenza comportamentale che catturano azioni passate in contesti rilevanti per la sicurezza, item attitudinali che misurano credenze e valori rilevanti per il

comportamento di sicurezza, item di conoscenza che stabiliscono una comprensione di baseline contro la quale le deviazioni possono essere rilevate, e item di giudizio situazionale che presentano circostanze ambigue che richiedono prioritizzazione. Ogni indicatore attinge a item attraverso queste modalità, con pesi delle modalità calibrati sulla specificazione teorica dell'indicatore.

Consideriamo la valutazione della desensibilizzazione da alert fatigue, indicatore 5.1 nella categoria del sovraccarico cognitivo. L'auto-report diretto della fatica si rivela inaffidabile; i professionisti normalizzano la loro esperienza e sottostimano il degrado. L'assessment quindi approccia questo indicatore attraverso item di scenario che presentano volumi di alert e chiedono decisioni di prioritizzazione, con scoring basato sulla deviazione dai pattern di prioritizzazione ottimali. Incorpora item sulla frequenza comportamentale riguardo specifiche pratiche di gestione degli alert che indicano scorciatoie guidate dalla fatica. Include item che valutano le credenze sull'utilità degli alert che predicono il disengagement. Impiega item basati sull'attenzione che misurano indirettamente l'esaurimento delle risorse cognitive. Il punteggio dell'indicatore emerge dall'aggregazione pesata attraverso questi approcci, fornendo robustezza che nessun singolo tipo di item potrebbe raggiungere.

L'architettura di assessment affronta anche la dimensione temporale che si rivela cruciale per gli indicatori psicologici. A differenza delle vulnerabilità tecniche che esistono o non esistono in un dato momento, le vulnerabilità psicologiche fluttuano con le circostanze. La visione a tunnel indotta dallo stress catturata nell'indicatore 7.7 può essere assente durante periodi di calma e acuta durante le crisi. Un assessment condotto durante la stabilità organizzativa non rileverà vulnerabilità che si manifestano sotto pressione. L'architettura quindi incorpora item condizionali che chiedono del comportamento sotto circostanze specificate, creando un profilo temporale più ricco di quanto l'assessment point-in-time permetta.

I meccanismi di protezione della privacy sono incorporati nell'architettura a molteplici livelli. Le soglie minime di aggregazione prevengono l'identificazione delle risposte individuali. Le tecniche di privacy differenziale introducono rumore calibrato che preserva la validità statistica proteggendo i dati individuali. Il reporting con ritardo temporale assicura che i risultati non possano essere correlati a eventi o decisioni specifiche. L'analisi basata sui ruoli piuttosto che sugli individui mantiene il focus sui pattern organizzativi piuttosto che sulle caratteristiche personali. Questi meccanismi non sono ripensamenti ma vincoli di progettazione che hanno plasmato lo sviluppo degli item fin dall'inizio.

5 Interdipendenze degli Indicatori

I cento indicatori del CPF non funzionano come misurazioni indipendenti. Costituiscono nodi in una rete di dipendenze condizionali che trasforma osservazioni isolate in profili di rischio sistemico. Questa struttura a rete non è meramente utile per l'analisi; riflette l'effettiva realtà psicologica che il framework tenta di catturare. La vulnerabilità umana emerge dall'interazione, non dall'aggregazione.

La struttura delle interdipendenze è formalmente modellata come una rete bayesiana in cui ogni indicatore mantiene una distribuzione di probabilità condizionale sui suoi indicatori genitori. La probabilità congiunta attraverso tutti gli indicatori segue la fattorizzazione standard:

$$P(I_1, I_2, ..., I_{100}) = \prod_{i=1}^{100} P(I_i | parents(I_i))$$

Questa fattorizzazione cattura l'intuizione che conoscere certi stati degli indicatori cambia drammaticamente le nostre aspettative su altri. La struttura non è assunta ma appresa dalle relazioni

teoriche e, dove disponibile, dall'osservazione empirica.

Diverse interdipendenze si rivelano particolarmente significative per la valutazione operativa. Lo stress amplifica la conformità all'autorità: quando l'indicatore 7.1 che misura la compromissione da stress acuto mostra valori elevati, la probabilità condizionale dell'indicatore 1.1 che misura la conformità incondizionata aumenta sostanzialmente. La nostra stima corrente pone questa probabilità condizionale approssimativamente a 0.8, significando che le organizzazioni che mostrano pattern di stress acuto mostreranno vulnerabilità di conformità all'autorità quattro volte su cinque. Questa non è coincidenza ma meccanismo. Lo stress restringe l'elaborazione cognitiva, aumenta l'affidamento sulle euristiche, e riduce la funzione esecutiva richiesta per questionare l'autorità.

La pressione temporale si propaga al sovraccarico cognitivo attraverso percorsi similmente meccanicistici. Punteggi elevati sugli indicatori 2.1 fino a 2.3, che misurano il bypass indotto dall'urgenza, il degrado da pressione temporale, e l'accettazione del rischio guidata dalle scadenze, aumentano sostanzialmente la probabilità di punteggi elevati attraverso la categoria del sovraccarico cognitivo. La probabilità condizionale di vulnerabilità della categoria 5 data la vulnerabilità della categoria 2 si avvicina a 0.7 nel nostro modello corrente. Di nuovo, questo riflette meccanismo psicologico piuttosto che correlazione statistica. La pressione temporale esaurisce le risorse cognitive richieste per un comportamento di sicurezza attento.

Le dinamiche di gruppo introducono un effetto di mascheramento che complica la valutazione. Quando gli indicatori 6.1 fino a 6.5, che misurano groupthink, risky shift, diffusione di responsabilità, social loafing ed effetto bystander, mostrano valori elevati, le vulnerabilità affettive individuali nella categoria 4 diventano più difficili da rilevare. Lo stato di gruppo assorbe e oscura la variazione individuale. Il nostro modello rappresenta questo attraverso una probabilità condizionale di approssimativamente 0.6 che gli indicatori della categoria 4 appariranno normali nonostante la vulnerabilità sottostante quando la categoria 6 mostra dominanza delle dinamiche di gruppo. Questo effetto di mascheramento ha implicazioni profonde per la progettazione dell'assessment, richiedendo approcci che possano penetrare i fenomeni a livello di gruppo per rivelare gli stati individuali.

La struttura a rete abilita query predittive che estendono l'assessment oltre gli indicatori osservati. Data un'osservazione parziale dello spazio degli indicatori, gli algoritmi di propagazione delle credenze possono calcolare le probabilità a posteriori per gli indicatori non osservati. Un'organizzazione che mostra elevata vulnerabilità all'autorità e pressione temporale, anche senza valutazione diretta del sovraccarico cognitivo, può essere assegnata un'alta probabilità di vulnerabilità al sovraccarico cognitivo basata sull'inferenza della rete. Questa capacità predittiva trasforma il framework dalla diagnosi retrospettiva all'identificazione prospettica del rischio.

La rete delle interdipendenze rivela anche stati convergenti dove molteplici vulnerabilità si allineano per creare profili di rischio qualitativamente diversi da qualsiasi singola vulnerabilità. La categoria 10 del framework affronta esplicitamente questi stati convergenti, ma la struttura a rete rivela pattern di convergenza aggiuntivi non catturati nei singoli indicatori. Quando la conformità all'autorità, la pressione temporale, il sovraccarico cognitivo e le dinamiche di gruppo mostrano simultaneamente vulnerabilità elevata, lo stato risultante non è la somma di queste vulnerabilità ma il loro prodotto. L'indice di convergenza per tali stati segue un modello moltiplicativo piuttosto che additivo:

$$CI = \prod_{i \in \text{elevated}} (1 + v_i)$$

dove v_i rappresenta il punteggio di vulnerabilità normalizzato per ogni indicatore elevato. Le organizzazioni in stati di alta convergenza affrontano profili di rischio qualitativamente diversi

che richiedono risposte qualitativamente diverse.

6 Livelli di Operazionalizzazione

Il framework teorico, l'architettura di assessment e la rete delle interdipendenze richiedono espressione operativa per raggiungere impatto pratico. L'ecosistema CPF include molteplici livelli di operazionalizzazione che traducono i costrutti teorici in capacità organizzative.

La dashboard di scoring fornisce l'interfaccia primaria attraverso la quale le organizzazioni si confrontano con i risultati dell'assessment. Il suo design riflette principi derivati dal framework stesso, particolarmente gli indicatori di sovraccarico cognitivo che avvertono contro la densità informativa che eccede la capacità di elaborazione. La dashboard presenta viste gerarchiche che si muovono dai punteggi aggregati organizzativi attraverso i breakdown a livello di categoria fino ai dettagli dei singoli indicatori. La codifica a colori segue lo schema ternario del framework, con verde, giallo e rosso che forniscono orientamento immediato. Il trending temporale rivela pattern invisibili nella valutazione point-in-time, mostrando se le vulnerabilità sono stabili, in miglioramento o in deterioramento.

Il modello di maturità incorporato nella dashboard riflette l'osservazione che la psicologia organizzativa evolve attraverso stadi di sviluppo piuttosto che miglioramenti discreti. Un'organizzazione non può muoversi direttamente da alta vulnerabilità all'autorità a bassa vulnerabilità all'autorità; deve passare attraverso stati intermedi caratterizzati da aumentata consapevolezza, intervento sperimentale, miglioramento parziale e cambiamento consolidato. Il modello di maturità specifica cinque livelli per ogni categoria, con criteri dettagliati per l'assegnazione del livello e guida per la progressione di livello. Questo framing di sviluppo previene lo scoraggiamento che accompagna aspettative irrealistiche di trasformazione rapida.

L'integrazione con il security operations center rappresenta il livello di operazionalizzazione più tecnicamente impegnativo. Gli indicatori psicologici del framework devono connettersi ai flussi di telemetria, alla logica di rilevamento e ai protocolli di risposta che costituiscono l'infrastruttura del SOC. Questa integrazione opera bidirezionalmente. I dati comportamentali dagli strumenti di sicurezza informano la valutazione psicologica, fornendo correlati comportamentali che supplementano le misure di auto-report. Le valutazioni dello stato psicologico informano le operazioni di sicurezza, aggiustando le soglie di rilevamento e i protocolli di risposta basati sui profili di vulnerabilità organizzativa.

Il livello di integrazione SOC implementa lo schema OFTLISRV per ogni indicatore: gli Osservabili definiscono quali dati rivelano lo stato dell'indicatore; le Fonti di Telemetria specificano dove quei dati originano; i parametri di Temporalità governano i tassi di campionamento e le finestre di osservazione; la Logica articola gli algoritmi di rilevamento; le Interdipendenze collegano agli indicatori correlati; le Soglie stabiliscono i confini di scoring; i protocolli di Risposta specificano le azioni innescate dal superamento delle soglie; e i meccanismi di Validazione assicurano l'accuratezza continuata. Questo schema assicura copertura sistematica mentre accomoda le caratteristiche distinte di ogni indicatore.

Consideriamo l'operazionalizzazione dell'indicatore 2.1, bypass di sicurezza indotto dall'urgenza. Gli osservabili includono pattern nei log di autenticazione che mostrano tempi di sessione abbreviati, metadati email che rivelano risposte rapide a richieste con marcatori di urgenza, e record della catena di approvazione che mostrano periodi di revisione compressi. Le fonti di telemetria includono i log di Active Directory, i dati del gateway email e i sistemi di workflow management. I parametri temporali specificano campionamento a intervalli di cinque minuti con una finestra di osservazione di un'ora e soglia di persistenza di sei ore. La logica di rilevamento combina l'identificazione rule-based di specifici pattern di urgenza con il rilevamento

statistico di anomalie usando la distanza di Mahalanobis per tenere conto della correlazione tra osservabili. Le interdipendenze collegano agli indicatori 2.2 e 2.3 nella stessa categoria e agli indicatori di stress 7.1 e 7.7 nella categoria stress. Le soglie seguono la calibrazione baseline organizzativa con confini di deviazione standard. I protocolli di risposta vanno dall'escalation automatica del monitoraggio a severità più bassa alla notifica dell'analista umano a severità più alta. La validazione impiega testing sintetico con pattern di urgenza iniettati e analisi di correlazione contro gli esiti degli incidenti.

Questa specificazione operativa trasforma l'indicatore astratto in una capacità di rilevamento funzionante. La trasformazione non è banale. Ogni indicatore richiede una specificazione simile, e le specificazioni devono mantenere coerenza con il framework teorico mentre si adattano alle realtà tecniche delle fonti di dati disponibili e delle capacità di elaborazione.

7 L'Imperativo della Validazione

Un framework senza validazione è affermazione senza evidenza. Il CPF fa affermazioni sulle vulnerabilità psicologiche, la loro misurabilità, le loro interdipendenze e la loro relazione con gli esiti di sicurezza. Queste affermazioni richiedono testing empirico per raggiungere la credibilità necessaria per l'adozione e il raffinamento necessario per l'accuratezza.

La validazione del CPF affronta sfide distinte da quelle che confrontano i framework puramente tecnici. I costrutti psicologici non possono essere osservati direttamente; devono essere inferiti da indicatori comportamentali e di auto-report che sono essi stessi proxy imperfetti. I fenomeni di interesse fluttuano con le circostanze, complicando l'identificazione di baseline stabili. Gli effetti dell'intervento che dimostrerebbero la validità predittiva richiedono tempi estesi per manifestarsi. I contesti organizzativi nei quali avviene l'assessment variano in modi che possono moderare l'applicabilità del framework.

La metodologia di validazione che abbiamo sviluppato affronta queste sfide attraverso molteplici approcci complementari. La valutazione della validità di costrutto esamina se gli strumenti di assessment misurano effettivamente i costrutti psicologici che affermano di misurare. Questo richiede analisi fattoriale per confermare che gli item si raggruppano secondo le loro assegnazioni teoriche, testing di validità convergente per verificare la correlazione con misure stabilite di costrutti correlati, e testing di validità discriminante per assicurare la differenziazione da costrutti non correlati. Le analisi preliminari supportano la struttura fattoriale intesa, ma la validazione comprensiva richiede campioni più ampi attraverso contesti organizzativi più diversi.

La valutazione della validità predittiva esamina se i punteggi del framework predicono effettivamente esiti rilevanti per la sicurezza. Questo richiede tracking longitudinale delle organizzazioni dall'assessment attraverso i successivi incidenti di sicurezza, con analisi di se i punteggi degli indicatori al tempo uno predicono i tassi di incidenti al tempo due. La sfida qui è il problema del tasso base: gli incidenti di sicurezza sono sufficientemente rari che rilevare relazioni statistiche richiede o campioni molto grandi o periodi di osservazione molto lunghi. Stiamo perseguendo entrambi gli approcci, costruendo database di assessment attraverso molteplici organizzazioni mentre manteniamo relazioni longitudinali con gli early adopter.

La valutazione della validità incrementale esamina se il framework aggiunge valore predittivo oltre gli approcci di assessment di sicurezza esistenti. Un'organizzazione potrebbe ragionevolmente chiedere se i punteggi CPF le dicono qualcosa che non potrebbero apprendere dalle valutazioni convenzionali di maturità della sicurezza. Dimostrare la validità incrementale richiede confronto diretto, valutando le organizzazioni con sia strumenti CPF che convenzionali e confrontando l'accuratezza predittiva. I risultati preliminari suggeriscono una validità in-

crementale sostanziale, particolarmente per gli incidenti con componenti significative di fattori umani, ma la dimostrazione definitiva attende studi su scala più ampia.

L'imperativo della validazione plasma il nostro approccio alla collaborazione. I ricercatori che possono contribuire alla metodologia di validazione, che possono fornire accesso a contesti organizzativi per l'assessment, o che possono estendere i periodi di osservazione attraverso partnership longitudinali, offrono contributi di valore sostanziale. L'evoluzione del framework dipende da tale collaborazione, non come miglioramento di un sistema già completo ma come completamento essenziale di un processo di sviluppo necessariamente iterativo.

8 Conclusione: Un'Apertura Piuttosto Che una Chiusura

Ciò che abbiamo presentato in questo paper non è il framework stesso ma le sue fondamenta. Il framework esiste nella sua forma pubblicata, disponibile per esame e applicazione. Le fondamenta spiegano perché il framework assume la forma che assume, cosa giace sotto la sua apparente semplicità, e cosa sarebbe richiesto per estenderlo, validarlo o implementarlo su scala operativa.

Il lettore che ha seguito questa esposizione ora possiede una comprensione che la presentazione superficiale del framework non può trasmettere. L'integrazione di tradizioni psicologiche disparate non è mera citazione ma attenta modellazione traduttiva. L'orientamento diagnostico piuttosto che prescrittivo non è limitazione ma principio. L'architettura di assessment non è un questionario ma un sistema di misurazione multi-modale progettato per la validità convergente. Gli indicatori non sono osservazioni indipendenti ma nodi in una rete di interdipendenze che abilita l'inferenza predittiva. I livelli operativi non sono aggiunte ma espressioni necessarie dei costrutti teorici in capacità organizzativa.

Questa comprensione conta diversamente per diversi lettori. Per i professionisti che considerano l'implementazione, rivela la profondità delle fondamenta che supportano quella che altrimenti potrebbe apparire come un'altra tassonomia di consulenti. Per i ricercatori che considerano l'investigazione, espone gli impegni teorici che richiederebbero testing e le scelte metodologiche che richiederebbero giustificazione. Per i potenziali contributori, mappa il terreno all'interno del quale il contributo avverrebbe, né sottostimando il lavoro già fatto né sovrastimando la sua completezza.

Il CPF non è finito. Nessun framework che affronta fenomeni complessi come la vulnerabilità psicologica umana nei contesti di sicurezza organizzativa potrebbe essere finito. È, tuttavia, sostanzialmente sviluppato, teoricamente fondato, operativamente specificato, e pronto per l'estensione collaborativa che le sue ambizioni richiedono. Ciò che rimane è il lavoro di validazione, raffinamento e implementazione che trasforma il framework in pratica e la pratica in migliori esiti di sicurezza.

La superficie è dove avvengono le operazioni. La profondità è dove risiede la comprensione. Questo paper è stato un invito in quella profondità, esteso a coloro che sono preparati a confrontarsi con essa seriamente. Il lavoro continua.

Nota sulla Composizione Assistita da AI

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 coerenza formattativa. Le idee fondamentali, l'ar-

chitettura del CPF, l'integrazione teorica e l'analisi strategica sono esclusivamente il prodotto dell'expertise dell'autore. L'autore è interamente responsabile dell'accuratezza e dell'integrità del contenuto pubblicato.

Ringraziamenti

L'autore riconosce il dialogo continuo con le comunità di ricerca della cybersecurity e della psicologia che continua a plasmare lo sviluppo di questo lavoro.

Riferimenti bibliografici

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

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

[3] Jung, C. G. (1969). *The Archetypes and the Collective Unconscious*. Princeton: Princeton University Press.

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

[5] Kernberg, O. (1998). *Ideology, conflict, and leadership in groups and organizations*. New Haven: Yale University Press.

[6] Klein, M. (1946). Notes on some schizoid mechanisms. *International Journal of Psychoanalysis*, 27, 99-110.

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

[8] Miller, G. A. (1956). The magical number seven, plus or minus two. *Psychological Review*, 63(2), 81-97.

[9] Selye, H. (1956). *The stress of life*. New York: McGraw-Hill.

[10] Winnicott, D. W. (1971). *Playing and reality*. London: Tavistock Publications.