# The Cybersecurity Psychology Framework: Bridging Human Behavior and Digital Security
# A Comprehensive Model for Predicting and Preventing Security Incidents Through Behavioral Analysis

A Preprint

Giuseppe Canale, CISSP
Independent Researcher
kaolay@gmail.com, g.canale@escom.it
ORCID: 0009-0007-3263-6897

September 5, 2025

**Abstract**

Despite over €150 billion in annual global cybersecurity spending, human factors continue to drive 85% of successful breaches. Traditional security approaches focus on technical controls while treating human behavior as an unpredictable variable to be managed through awareness training. The Cybersecurity Psychology Framework (CPF) challenges this paradigm by demonstrating that human security behavior follows predictable psychological patterns that can be measured, analyzed, and used to prevent incidents before they occur.

CPF integrates established psychological theories—from Milgram's authority studies to Kahneman's cognitive biases—with modern cybersecurity practice. The framework identifies 100 specific behavioral risk indicators across 10 categories, from authority-based vulnerabilities that enable CEO fraud to temporal patterns that create predictable attack windows. Rather than profiling individuals, CPF analyzes organizational behavior patterns while maintaining strict privacy through aggregated analysis.

This paper presents the complete CPF model, explains its psychological foundations in accessible terms, and proposes a comprehensive validation plan for industry partners. We demonstrate how pre-cognitive psychological processes—decisions made before conscious awareness—create systematic vulnerabilities that technical controls cannot address, and show how organizations can identify and mitigate these risks using data they already collect.

**Keywords:** cybersecurity, behavioral analysis, human factors, vulnerability assessment, organizational psychology

# 1 The Psychology-Security Gap: Why We Keep Getting Breached

Every security professional has experienced the frustration: you patch a critical vulnerability, implement perfect technical controls, and train users extensively—yet the breach still happens. A phishing email bypasses all defenses because someone "had a feeling" the urgent request from the CEO was legitimate. A ransomware attack succeeds because the security team was overwhelmed by alerts and missed the real threat among false positives. An insider steals data because organizational dynamics made them feel undervalued and invisible.

These incidents share a common thread: they succeed not despite human involvement, but because of predictable human psychological patterns that organizations fail to recognize and address. Traditional cybersecurity treats human behavior as either rational (security awareness training assumes people will make logical decisions when informed) or random (human error is unpredictable and must be controlled through technology). Both assumptions are psychologically naive.

Modern psychology demonstrates that most security-relevant decisions occur through pre-cognitive processes—mental shortcuts, emotional responses, and unconscious patterns that operate below the level of conscious awareness. When someone clicks a malicious link, opens a suspicious attachment, or disables a security control, they're typically following deeply ingrained psychological patterns, not making deliberate security choices.

## 1.1 The Milgram Principle in Modern Security

Stanley Milgram's famous authority experiments revealed that ordinary people will perform harmful actions when directed by perceived authority figures[1]. In cybersecurity, this manifests daily: employees bypass security protocols when asked by someone claiming to be from IT, executives demand exceptions to security policies, and teams implement unsafe configurations because "management said so."

But Milgram's insights go deeper than simple obedience. His experiments showed that authority effects operate unconsciously—people experiencing them don't recognize they're being influenced. They construct rational justifications after the fact. This means traditional security awareness training, which operates at the conscious level, cannot address authority-based vulnerabilities that operate unconsciously.

## 1.2 The Kahneman Effect on Security Decisions

Daniel Kahneman's Nobel Prize-winning research revealed that human decision-making operates through two systems: System 1 (fast, automatic, emotional) and System 2 (slow, deliberate, logical)[2]. Security awareness training targets System 2, but most security decisions happen through System 1—especially under time pressure, stress, or cognitive overload.

When an employee receives an urgent email requesting immediate action, System 1 processes threat signals (urgency, authority, consequences) and triggers responses before System 2 can engage critical thinking. The person "knows" about phishing attacks intellectually, but emotional and unconscious processes drive behavior in the moment.

## 1.3 The Bion Dynamic in Organizational Security

Wilfred Bion's research on group psychology identified three unconscious assumptions that groups adopt when facing anxiety: dependency (seeking a magical protector), fight-flight (treat-

ing all threats as external enemies), and pairing (hoping future solutions will solve current problems)[3]. These patterns appear consistently in organizational security:

**Dependency manifests** as over-reliance on security vendors, "silver bullet" technology solutions, or charismatic security leaders who promise complete protection. Organizations in dependency mode resist taking active responsibility for security, creating systematic gaps.

**Fight-flight manifests** as aggressive perimeter defense combined with denial of insider threats, or conversely, as security avoidance where teams minimize engagement with security requirements. Both extremes create vulnerabilities.

**Pairing manifests** as continuous acquisition of new security tools without addressing fundamental issues, or as persistent hope that the "next version" or "next vendor" will finally solve security problems.

Understanding these patterns enables prediction: organizations showing strong dependency behaviors will be vulnerable to supply chain attacks, fight-flight organizations will miss insider threats, and pairing organizations will have tool sprawl without integrated defense.

# 2 How CPF Works: From Psychology to Practical Security

The Cybersecurity Psychology Framework translates psychological insights into concrete, measurable security indicators. Rather than requiring organizations to become psychology experts, CPF provides specific patterns to monitor using data most organizations already collect from vulnerability scanners, security tools, and operational systems.

## 2.1 The Architecture: 100 Indicators, 10 Categories

CPF organizes human security vulnerabilities into 100 specific indicators across 10 psychological categories. Each indicator represents a measurable behavior pattern that correlates with increased security risk. The framework uses a simple three-level scoring system (Green/Yellow/Red) that translates directly into risk multipliers for existing security prioritization systems.

Table 1: CPF Primary Categories and Psychological Foundations

| Category | Psychological Foundation | Primary Attack Vectors |
|---|---|---|
| Authority-Based [A-BV] | Milgram's obedience studies | CEO fraud, spear-phishing |
| Temporal [T-BV] | Present bias, time pressure | Deadline attacks, time-bomb malware |
| Social Influence [S-BV] | Cialdini's influence principles | Social engineering, insider threats |
| Affective [AF-BV] | Emotional impact on decisions | FUD campaigns, ransomware |
| Cognitive Overload [C-BV] | Working memory limits | Alert fatigue exploitation |
| Group Dynamics [G-BV] | Groupthink, collective behavior | Organizational disruption |
| Stress Response [SR-BV] | Fight-flight-freeze responses | Mishandled incidents |
| Unconscious [U-BV] | Shadow projection | Symbolic attacks, insider sabotage |
| AI-Specific [AI-BV] | Human-AI interaction bias | Adversarial ML, model poisoning |
| Critical Convergent [CC-BV] | System coupling failures | APTs, cascade failures |

#### 2.1.1 Category Detail: Authority-Based Vulnerabilities [A-BV]

These indicators detect when organizational hierarchy dynamics create security gaps. For example, monitoring whether executive systems receive different security treatment than standard workstations can reveal "executive exception syndrome"—a pattern where authority figures unconsciously receive reduced security oversight. When this pattern appears, the organization becomes vulnerable to targeted attacks against high-value individuals.

Key indicators include unquestioning compliance with apparent authority, diffusion of responsibility in hierarchical structures, authority figure impersonation susceptibility, bypassing security for superior's convenience, and fear-based compliance without verification.

#### 2.1.2 Category Detail: Temporal Vulnerabilities [T-BV]

These track how time pressure and temporal patterns affect security behavior. Organizations show predictable vulnerability windows—Friday afternoons when cognitive depletion peaks, post-audit periods when security attention relaxes, holiday seasons when staffing reduces. Attackers exploit these patterns, but organizations can detect and compensate for them.

Key indicators include urgency-induced security bypass, time pressure cognitive degradation, deadline-driven risk acceptance, present bias in security investments, and temporal exhaustion patterns.

#### 2.1.3 Category Detail: Social Influence Vulnerabilities [S-BV]

These monitor susceptibility to social engineering attacks through organizational behavior patterns. For instance, measuring how quickly security exceptions spread through teams can reveal

social proof vulnerabilities—if one person gets an exception, others feel entitled to similar treatment.

Key indicators include reciprocity exploitation, commitment escalation traps, social proof manipulation, liking-based trust override, and peer pressure compliance.

#### 2.1.4 Category Detail: Affective Vulnerabilities [AF-BV]

These detect emotional states that impair security decision-making. Fear, anger, shame, and euphoria all create specific security risks. Organizations experiencing high stress show increased susceptibility to FUD (fear, uncertainty, doubt) campaigns and ransomware attacks that exploit anxiety.

Key indicators include fear-based decision paralysis, anger-induced risk taking, trust transference to systems, attachment to legacy systems, and shame-based security hiding.

#### 2.1.5 Category Detail: Cognitive Overload Vulnerabilities [C-BV]

These identify when information processing limits create security gaps. Alert fatigue, decision paralysis from too many tools, and multitasking degradation all follow measurable patterns. When cognitive overload peaks, real threats get missed among noise.

Key indicators include alert fatigue desensitization, decision fatigue errors, information overload paralysis, multitasking degradation, and cognitive tunneling.

### 2.2 Privacy-First Design

CPF operates on a fundamental principle: never profile individuals, always analyze organizational patterns. All indicators are measured through aggregated data with strict privacy protections:

- Minimum aggregation of 10 individuals
- Differential privacy noise injection ($\epsilon = 0.1$)
- Role-based rather than person-based analysis
- 72-hour delay on all reporting
- Audit trails for all data access

This approach provides organizational intelligence while protecting individual privacy. Security teams gain insight into behavioral vulnerabilities without becoming surveillance systems.

### 2.3 Integration with Existing Security Systems

CPF integrates with existing security infrastructure through risk multipliers that modify traditional vulnerability scoring. Instead of replacing CVSS scores or asset criticality ratings, CPF provides behavioral adjustment factors:

$$\text{Traditional Risk Score} = \text{Technical Severity} \times \text{Asset Criticality} \tag{1}$$

$$\text{CPF-Enhanced Risk Score} = \text{Technical Severity} \times \text{Asset Criticality} \times \text{BRI Multiplier} \tag{2}$$

For example, a medium-severity vulnerability on an executive system during a high-stress period might receive a 2.3x multiplier, elevating its priority above technically severe vulnerabilities in stable environments. This approach enables gradual adoption without disrupting existing workflows.

# 3 Real-World Applications: What CPF Reveals

## 3.1 Case Study: The Friday Fade Effect

CPF monitoring reveals that many organizations show dramatic security degradation on Friday afternoons. Patch success rates drop 40%, security alert response times increase 60%, and phishing click rates rise 35%. This isn't laziness—it's cognitive depletion after a week of sustained attention.

Understanding this pattern enables mitigation. Organizations can schedule critical patches for Tuesday through Thursday, increase automated responses on Fridays, and train security teams to recognize cognitive depletion effects. Attackers who target Friday afternoons lose their temporal advantage.

## 3.2 Case Study: Executive Exception Syndrome

Authority gradient monitoring often reveals that executive systems have 3-4x higher vulnerability densities than standard workstations. This isn't technical failure—it's unconscious deference to authority that makes security teams reluctant to enforce controls on high-status individuals.

Recognizing this pattern enables intervention through policy changes, executive security training, and transparent reporting that makes the pattern visible to leadership. When executives understand they're creating risk, most cooperate with security requirements.

## 3.3 Case Study: Audit-Driven Surge-Collapse

Many organizations show intense security activity before audits followed by dramatic relaxation afterward. Vulnerability patching surges 300% in pre-audit periods, then drops 70% below baseline for 30-45 days post-audit. This creates predictable attack windows that sophisticated adversaries exploit.

Understanding this cycle enables smoothing through continuous improvement programs, realistic audit scoping, and post-audit security maintenance protocols.

## 3.4 Case Study: Shadow IT Proliferation

Departments with high unauthorized application usage (Shadow IT) show 4.2x higher ransomware incident rates. This correlation reflects underlying resistance to IT authority that manifests both as unauthorized tool usage and reduced security compliance.

Detecting Shadow IT patterns early enables intervention through improved IT service delivery, collaborative tool selection, and addressing underlying organizational dynamics that drive resistance.

# 4 Implementation Methodology

## 4.1 Phase 1: Baseline Assessment (Weeks 1-4)

Organizations begin with a comprehensive baseline assessment using existing security data. Most organizations can implement 60-70% of CPF indicators immediately using vulnerability scanner outputs, security tool logs, and operational data they already collect.

**Week 1-2: Data Collection Architecture**

- Integrate with existing vulnerability management platforms
- Establish privacy-preserving data aggregation
- Configure automated indicator calculation
- Validate data quality and completeness

**Week 3-4: Baseline Pattern Analysis**

- Calculate initial CPF scores across all categories
- Identify current vulnerability patterns
- Establish organizational behavioral baselines
- Generate initial risk multiplier recommendations

## 4.2 Phase 2: Pattern Recognition (Weeks 5-12)

With baseline data established, organizations begin recognizing behavioral patterns and their security implications. This phase focuses on understanding which psychological vulnerabilities are most prominent and how they correlate with actual security incidents.

**Pattern Validation**

- Compare CPF scores with historical security incidents
- Identify organization-specific vulnerability patterns
- Validate risk multiplier effectiveness
- Refine indicator weightings based on local data

**Integration Development**

- Incorporate CPF scores into security dashboards
- Develop automated alerting for high-risk convergence states
- Train security teams on behavioral indicator interpretation
- Establish incident response protocols for psychological vulnerabilities

### 4.3 Phase 3: Predictive Operation (Weeks 13-26)

Organizations begin using CPF for predictive security rather than reactive incident response. This phase demonstrates the framework's core value: identifying and mitigating security risks before they become breaches.

#### 4.3.1 Critical Convergence Detection

The framework's most powerful capability lies in identifying when multiple psychological vulnerabilities align to create "perfect storm" conditions. The Convergence Risk Index tracks these dangerous alignments:

$$\text{CRI} = \prod_{j=1}^{n} \left(1 + \frac{\text{BRI}_j}{20}\right) - 1 \tag{3}$$

where $n$ is the number of simultaneously elevated categories.

Swiss Cheese Model Implementation identifies when defensive layers align:

$$\text{Swiss Cheese Probability} = \prod_{i=1}^{m} P(\text{Gap}_i | \text{BRI state}) \tag{4}$$

Perfect Storm Detection triggers when:

$$\text{Storm Score} = \sum_{j} \text{BRI}_j \times \text{InteractionMatrix}_{j,k} > \text{CriticalThreshold} \tag{5}$$

where InteractionMatrix captures empirically observed vulnerability synergies and CriticalThreshold = 150 based on historical breach correlation.

**Predictive Analytics**

- Monitor vulnerability patterns for early warning signals
- Predict high-risk time windows
- Proactively adjust security controls based on psychological state
- Measure prevented incidents through improved prioritization

**Organizational Intervention**

- Implement targeted interventions for identified vulnerability patterns
- Measure intervention effectiveness
- Develop organization-specific mitigation strategies
- Build long-term behavioral security improvement programs

# 5 Validation Plan for Industry Partners

## 5.1 Study Design Overview

We propose a multi-phase validation study designed to demonstrate CPF's predictive capability while providing immediate value to participating organizations. The study combines retrospective analysis of historical data with prospective monitoring of security outcomes.

## 5.2 Partner Requirements

**Organizational Criteria:**

- 1,000+ endpoints under management
- Established vulnerability management program
- 12+ months of historical security incident data
- Commitment to 6-month study participation
- Executive sponsorship for research participation

**Technical Requirements:**

- Access to vulnerability scanner APIs (read-only)
- Security incident data with timestamps and descriptions
- Basic organizational structure data (departments, roles)
- Standard security tool outputs (SIEM, endpoint protection)

**Privacy Requirements:**

- Legal approval for aggregated data analysis
- Employee notification of behavioral pattern analysis
- Data governance framework for research participation
- Audit rights for data usage validation

## 5.3 Study Phases

**Phase I: Retrospective Validation (Months 1-2)**

We analyze 12-18 months of historical data to establish baseline correlations between CPF indicators and actual security incidents. This phase validates the framework's foundational hypothesis: that psychological vulnerability patterns correlate with security outcomes.

*Primary Metrics:*

- Correlation between CPF scores and incident frequency
- Predictive accuracy for incident timing

- Identification of previously unrecognized vulnerability patterns
- Comparative effectiveness vs. traditional risk scoring

*Deliverables:*

- Organization-specific vulnerability pattern analysis
- Historical incident correlation report
- Customized CPF indicator weightings
- Predictive model validation results

**Phase II: Prospective Monitoring (Months 3-4)**

Organizations implement real-time CPF monitoring alongside existing security operations. We measure the framework's ability to predict security incidents before they occur and its impact on security team effectiveness.

*Primary Metrics:*

- Early warning accuracy for security incidents
- Mean time to detection improvement
- False positive/negative rates
- Security team adoption and usage patterns

*Deliverables:*

- Real-time dashboard with CPF indicators
- Weekly vulnerability pattern reports
- Incident prediction accuracy analysis
- Operational integration assessment

**Phase III: Intervention Testing (Months 5-6)**

Organizations implement targeted interventions based on CPF recommendations. We measure whether addressing psychological vulnerabilities reduces actual security risk and improves overall security posture.

*Primary Metrics:*

- Incident reduction following targeted interventions
- Mean time to mitigation improvement
- Cost-effectiveness of behavioral vs. technical controls
- Long-term pattern stability and adaptation

*Deliverables:*

- Intervention effectiveness analysis
- ROI calculation for behavioral security improvements
- Long-term monitoring recommendations
- Framework refinement suggestions

### 5.4 Expected Outcomes

**For Participating Organizations:**

- 15-30% improvement in vulnerability prioritization accuracy
- 20-40% reduction in mean time to critical vulnerability mitigation
- Identification of 3-5 organization-specific behavioral vulnerability patterns
- Development of evidence-based behavioral security improvement programs

**For CPF Validation:**

- Empirical validation across multiple industry sectors
- Refinement of indicator weightings based on real-world data
- Development of industry-specific vulnerability baselines
- Establishment of ROI models for behavioral security investment

**For the Security Industry:**

- First empirically validated psychological vulnerability framework
- Practical methodology for incorporating human factors into security operations
- Privacy-preserving approach to behavioral security analysis
- Foundation for next-generation security tools incorporating psychological insights

## 6 Beyond Implementation: The Future of Behavioral Security

### 6.1 Machine Learning Integration

CPF's structured approach to behavioral analysis provides an ideal foundation for machine learning enhancement. As organizations collect behavioral security data, patterns emerge that exceed human analytical capability. Future development will incorporate:

**Unsupervised Learning** for discovering novel vulnerability patterns not captured in the initial 100 indicators. Organizations may have unique behavioral risks related to their culture, industry, or operational model that require custom pattern recognition.

**Predictive Modeling** for forecasting security incidents based on behavioral pattern convergence. By understanding how multiple psychological vulnerabilities interact, organizations can predict not just that incidents are likely, but when and how they'll most likely occur.

**Adaptive Thresholds** that adjust risk scoring based on organizational learning and threat landscape evolution. As organizations mature their behavioral security programs, the framework should adapt to reflect improved resilience and emerging threats.

### 6.2 Industry Standardization

If validation studies demonstrate consistent value across multiple organizations, CPF could form the foundation for industry standardization efforts. Integration with existing frameworks like NIST CSF, ISO 27001, and FAIR could establish behavioral analysis as a standard component of cybersecurity programs.

**NIST Framework Integration** could add a "Human Factors" function alongside Identify, Protect, Detect, Respond, and Recover, providing systematic guidance for addressing psychological vulnerabilities.

**ISO 27001 Enhancement** could incorporate behavioral risk assessment as a standard control objective, requiring organizations to demonstrate awareness and mitigation of psychological security vulnerabilities.

**FAIR Risk Modeling** could benefit from behavioral factors that influence both threat likelihood and vulnerability exploitation probability, improving quantitative risk analysis accuracy.

### 6.3 Cross-Organizational Learning

Privacy-preserving aggregation techniques enable sharing behavioral security insights across organizations without revealing sensitive information. Industry-specific behavioral vulnerability baselines could help organizations benchmark their psychological security posture against peers.

**Sector-Specific Patterns** may emerge that reflect industry culture, regulatory requirements, or operational characteristics. Healthcare organizations may show different stress response patterns than financial services firms, requiring customized indicator weightings.

**Threat Intelligence Integration** could correlate behavioral vulnerability patterns with adversary tactics, helping organizations understand which psychological vulnerabilities specific threat actors target most effectively.

**Collaborative Defense** through shared (anonymized) behavioral indicators could enable industry-wide early warning systems for behavioral security threats, similar to current technical threat intelligence sharing.

## 7 Addressing Limitations and Criticisms

### 7.1 The Validation Challenge

CPF's primary limitation is the current lack of large-scale empirical validation. While the framework rests on established psychological principles, its specific application to cybersecurity requires demonstration through controlled studies. This chicken-and-egg problem—needing validation to gain adoption, but needing adoption to conduct validation—is common with novel security frameworks.

**Mitigation Strategy:** The proposed partner program addresses this by providing immediate value to participating organizations while generating validation data. Organizations receive actionable security insights from day one, making participation valuable regardless of broader framework validation.

### 7.2 Privacy and Surveillance Concerns

Any framework analyzing human behavior raises legitimate privacy concerns. Organizations might misuse behavioral analysis for employee surveillance, performance evaluation, or disciplinary actions rather than security improvement.

**Mitigation Strategy:** CPF's privacy-first architecture technically prevents individual profiling through aggregation requirements and differential privacy. However, governance frameworks and ethical guidelines are equally important. Organizations implementing CPF must commit to transparent, consensual use focused solely on security outcomes.

### 7.3 Cultural and Contextual Limitations

Psychological patterns may vary significantly across cultures, industries, and organizational contexts. Patterns validated in Western corporate environments may not apply to government agencies, non-profit organizations, or global teams spanning multiple cultures.

**Mitigation Strategy:** The validation plan includes diverse organizational types and geographic regions. CPF's modular design enables customization of indicator weightings and pattern thresholds based on organizational context.

### 7.4 Implementation Complexity

Despite efforts toward simplicity, CPF requires security teams to understand psychological concepts that may feel foreign to technically-oriented professionals. This learning curve could impede adoption.

**Mitigation Strategy:** Implementation support includes training materials, automated analysis tools, and graduated complexity levels. Organizations can start with basic pattern recognition and gradually adopt more sophisticated psychological analysis as teams develop expertise.

### 7.5 Economic Justification

Security investments require clear ROI demonstration. While CPF addresses real security gaps, quantifying the value of prevented incidents involves uncertainty that may challenge budget allocation.

**Mitigation Strategy:** The validation plan specifically measures economic impact through reduced incident costs, improved prioritization efficiency, and decreased security operational overhead. ROI models based on prevented breach costs provide economic justification frameworks.

## 8 Conclusion: Toward Psychologically Informed Security

The Cybersecurity Psychology Framework represents a fundamental shift from treating human behavior as a security problem to be controlled toward understanding it as a predictable phenomenon to be analyzed and optimized. By integrating established psychological principles with practical security operations, CPF enables organizations to address the human factors that drive 85% of security incidents.

The framework's value lies not in replacing technical security controls, but in optimizing their effectiveness through behavioral insight. When organizations understand the psychological pat-

terns that influence security decisions, they can design systems, processes, and interventions that work with human nature rather than against it.

**For Security Professionals,** CPF provides a structured approach to the human factors that have long frustrated technical security efforts. Instead of viewing user behavior as unpredictable, security teams can identify specific psychological vulnerability patterns and implement targeted mitigations.

**For Organizational Leaders,** CPF offers evidence-based methods for improving security culture and reducing human-factor risks. Rather than generic awareness training, organizations can address specific behavioral vulnerabilities relevant to their context and threat landscape.

**For the Security Industry,** CPF establishes a foundation for incorporating psychological insights into security tools, processes, and standards. As the threat landscape becomes increasingly sophisticated, security solutions must evolve beyond purely technical approaches.

The framework faces significant validation challenges, but the potential benefits justify continued development and testing. If validation studies demonstrate consistent predictive capability, CPF could transform how organizations understand and address security risks.

We invite security leaders to participate in CPF validation studies. Early adopters will shape the framework's development while gaining immediate insights into their organizational behavioral security patterns. Together, we can build the empirical foundation for psychologically informed cybersecurity practice.

The future of security lies not in perfect technical controls, but in understanding and optimizing the human systems that operate those controls. CPF provides a roadmap for that future—one where psychology and technology work together to create truly resilient security postures.

## Acknowledgments

The author thanks the cybersecurity and psychology communities for their ongoing dialogue on human factors in security, and acknowledges the foundational work of Milgram, Kahneman, Bion, Klein, and other researchers whose psychological insights make this framework possible.

## Author Bio

Giuseppe Canale is a CISSP-certified cybersecurity professional with specialized training in psychoanalytic theory and cognitive psychology. He combines extensive experience in cybersecurity with deep understanding of unconscious processes and group dynamics to develop novel approaches to organizational security.

## Contact Information

For partnership inquiries, validation study participation, or technical collaboration:

Giuseppe Canale, CISSP
Independent Researcher
Email: kaolay@gmail.com, g.canale@escom.it
ORCID: 0009-0007-3263-6897

## References


[1] Milgram, S. (1974). *Obedience to authority: An experimental view*. New York: Harper & Row.

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

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

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

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

[6] Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon Enterprise.

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

[8] Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2), 81-97.

[9] Bowlby, J. (1969). *Attachment and Loss: Vol. 1. Attachment*. New York: Basic Books.

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