Beyond Technical Metrics: The Case for Psychological Vulnerability Assessment in Cybersecurity

Giuseppe Canale, CISSP
Independent Researcher
kaolay@gmail.com
ORCID: 0009-0007-3263-6897
https://cpf3.org

Abstract

Despite massive investments in cybersecurity technologies, 85% of successful breaches exploit known vulnerabilities that organizations failed to patch. This persistent gap between vulnerability awareness and remediation suggests that psychological and organizational factors, rather than technical knowledge, determine security outcomes. We present the Cybersecurity Psychology Framework (CPF), a novel approach that identifies pre-cognitive vulnerability patterns through analysis of organizational behavior in vulnerability management data.

Initial deployment in three organizations demonstrates that psychological patterns—such as "patch procrastination" (ignoring vulnerabilities until external pressure), "organizational splitting" (treating identical vulnerabilities differently based on system categorization), and "repetition compulsion" (cyclical return of the same vulnerabilities)—predict actual exploitation better than technical severity scores alone. Organizations using CPF-adjusted prioritization achieved 20-23% improvement in mean time to mitigation and 30% better coverage of actually-exploited vulnerabilities, albeit with increased false positive rates (18.7% vs. 8.3%).

This position paper argues for incorporating psychological assessment into vulnerability prioritization, not as a replacement for technical metrics but as a complementary dimension addressing the human factors that dominate security failures. We outline a research agenda for validating and extending this approach, inviting collaboration from security and behavioral science communities to develop psychologically-informed security practices.

Keywords: vulnerability management, organizational psychology, behavioral security, human factors, security metrics

1 Introduction

Global cybersecurity spending exceeds $150 billion annually[3], yet breaches continue to increase in both frequency and severity. The 2023 Verizon Data Breach Investigations Report reveals a troubling statistic: 85% of successful breaches exploited vulnerabilities that were known to the organization for over 30 days[11]. This paradox—organizations possessing knowledge of vulnerabilities yet failing to remediate them—suggests that our fundamental approach to vulnerability management may be flawed.

Current vulnerability prioritization relies primarily on technical metrics such as the Common Vulnerability Scoring System (CVSS), which rates vulnerabilities based on exploitability, impact, and technical characteristics. While CVSS provides valuable technical assessment, it fails to account for the organizational and psychological factors that determine whether a vulnerability actually gets patched. A critical vulnerability in an executive's laptop may remain unpatched for months due to authority dynamics, while an identical vulnerability in a developer's system gets patched immediately. Technical severity alone cannot explain these disparities.

Recent advances in neuroscience have revealed that human decision-making occurs primarily below the threshold of consciousness[6, 10]. Brain imaging studies show that decisions are initiated 300-500 milliseconds before conscious awareness, with emotional and unconscious processes substantially influencing choices, especially under the time pressure and cognitive load characteristic of security operations. If security decisions are primarily pre-cognitive, then addressing only conscious awareness through training and policies will have limited effect.

This paper presents the Cybersecurity Psychology Framework (CPF), which identifies and quantifies psychological vulnerability patterns in organizations through analysis of their vulnerability management behaviors. Rather than asking organizations to self-report their security culture or undergo psychological assessment, CPF extracts psychological signals from existing operational data: how quickly different vulnerabilities are patched, which systems receive priority, when patches fail, and which vulnerabilities return despite remediation.

Our initial results from three pilot organizations suggest that psychological patterns provide significant predictive value beyond technical metrics. Organizations exhibiting high "manic defense" scores (ignoring threats until external pressure forces action) showed 3.7 times higher breach probability for vulnerabilities without public exploits. Those with severe "splitting" patterns (treating identical vulnerabilities differently based on system categorization) experienced targeted attacks through neglected systems 73% of the time.

This paper makes the case for integrating psychological assessment into vulnerability management, presenting it not as a replacement for technical approaches but as a necessary complement that addresses the human factors underlying most security failures. We outline the theoretical foundations, present initial empirical evidence, discuss implementation considerations, and propose a research agenda for developing psychologically-informed security practices.

2 The Limits of Technical-Only Approaches

2.1 The Knowing-Doing Gap

The security industry has operated under the assumption that vulnerability management is primarily an information problem: identify vulnerabilities, assess their severity, and patch them in order of risk. This rational model assumes that organizations, when provided with accurate vulnerability information, will act in their security interest. However, empirical evidence contradicts this assumption.

Analysis of breach data reveals that most exploited vulnerabilities were not zero-days or unknown threats, but well-documented vulnerabilities with available patches[9]. Organizations knew about these vulnerabilities, had the technical capability to fix them, but failed to act in time. This "knowing-doing gap" cannot be explained by technical factors alone.

Consider the WannaCry ransomware outbreak of 2017. The EternalBlue vulnerability it exploited had been patched by Microsoft two months before the attack. Organizations had the patch, understood the risk (the NSA exploit had been publicly leaked), yet hundreds of thousands of systems remained vulnerable. Technical knowledge was not the limiting factor—organizational and psychological dynamics were.

2.2 Cognitive Overload in Modern Environments

Modern enterprises face an overwhelming volume of vulnerabilities. A typical organization with 10,000 endpoints may have over 100,000 open vulnerabilities at any given time, with dozens of new critical vulnerabilities discovered weekly[8]. Security teams cannot patch everything

immediately; they must prioritize.

Current prioritization methods assume rational decision-making under conditions that make rationality impossible. Cognitive psychology research shows that human decision-making degrades severely under information overload[7]. When faced with too many choices, people resort to simple heuristics that may be systematically biased. In vulnerability management, this manifests as:

- Patching only vulnerabilities that make news headlines
- Focusing on perimeter systems while ignoring internal networks
- Repeatedly patching the same systems while others remain vulnerable
- Deferring difficult patches indefinitely

These patterns are not random failures but predictable consequences of cognitive overload combined with organizational psychology.

2.3 Organizational Dynamics Trump Individual Knowledge

Security training focuses on individual awareness, yet security decisions occur within organizational contexts that powerfully shape behavior. Bion's research on group dynamics[1] demonstrated that groups under stress regress to basic assumptions that override individual judgment:

- **Dependency**: Seeking an omnipotent protector (over-reliance on security vendors)
- **Fight-Flight**: Seeing threats as external enemies (ignoring insider risks)
- **Pairing**: Hoping for future salvation (the next security tool will solve everything)

These group dynamics operate unconsciously but profoundly influence security decisions. An organization in "dependency" mode may purchase expensive security tools but fail to configure them properly, unconsciously expecting the tool itself to provide protection. One in "fight-flight" may implement aggressive perimeter defenses while leaving internal systems vulnerable, unable to conceive of threats from within.

Individual security knowledge cannot overcome these organizational forces. A security professional may understand the importance of patching, but if the organization's unconscious culture treats certain systems as "invulnerable" or certain vendors as "trusted," patches will be delayed or skipped regardless of individual awareness.

3 The Cybersecurity Psychology Framework

3.1 Theoretical Foundation

The CPF integrates insights from psychoanalytic theory, cognitive psychology, and organizational behavior to create a comprehensive model of security vulnerability. Unlike traditional psychological approaches in security that focus on conscious attitudes and behaviors, CPF examines pre-cognitive and unconscious processes that determine security outcomes.

The framework rests on three theoretical pillars:

1. Pre-cognitive Processing: Decisions occur before conscious awareness[6]. By the time a security professional consciously decides whether to patch a vulnerability, their brain has already initiated the decision based on unconscious factors like anxiety tolerance, authority relationships, and group dynamics.

2. Object Relations: Organizations relate to systems and vulnerabilities as psychological objects imbued with emotional significance[5]. A "production server" is not just hardware but a "good object" that must be protected, while a "test system" may be a "bad object" that can be neglected. These unconscious categorizations determine security priorities more than technical risk assessments.

3. Repetition Compulsion: Organizations unconsciously repeat past traumas[2]. A company that experienced a data breach may obsessively patch database vulnerabilities while ignoring other vectors, compulsively repeating defensive patterns even when threats have evolved.

3.2 Core Psychological Patterns

Through analysis of vulnerability management data across multiple organizations, we identified five primary psychological patterns that predict security failures:

3.2.1 Pattern 1: Patch Procrastination (Temporal Vulnerability)

Organizations exhibit predictable temporal patterns in vulnerability response. "Patch procrastination" manifests as extended delays (¿90 days) in addressing known vulnerabilities, followed by panic responses when external events (public exploits, peer breaches, audits) create pressure.

Detection: Analyze the distribution of patch timing relative to vulnerability age and external events.

Indicator: Organizations with ¿65% of patches occurring after external pressure show 2.3x higher breach probability.

3.2.2 Pattern 2: Organizational Splitting

Splitting is a primitive defense mechanism where objects are categorized as "all good" or "all bad"[5]. In cybersecurity, this manifests as identical vulnerabilities being treated differently based on system categorization.

Detection: Compare patch rates for the same CVE across different system categories.

Indicator: Organizations with ¿70% patch rate disparity for identical vulnerabilities experience targeted attacks through neglected systems in 73% of breaches.

3.2.3 Pattern 3: Repetition Compulsion

Certain vulnerabilities return cyclically despite repeated patching, indicating unresolved organizational issues. This pattern suggests that technical remediation without addressing underlying psychological factors is ineffective.

Detection: Identify vulnerabilities that follow a patch-reappear cycle more than 3 times.

Indicator: Organizations with ¿5 compulsively recurring vulnerabilities show those exact CVEs involved in 67% of incidents.

3.2.4 Pattern 4: Authority Gradient Vulnerability

Authority dynamics create systematic security weaknesses in high-privilege systems. Security teams may be reluctant to enforce policies on executive systems, creating exploitable gaps.

Detection: Compare vulnerability density and patch timing between executive and standard systems.

Indicator: Executive systems with 3.5x higher vulnerability density than standard systems are initial compromise points in 73% of insider incidents.

3.2.5 Pattern 5: Cognitive Overload Cascade

When vulnerability counts exceed cognitive processing capacity, remediation effectiveness collapses. This creates a paradox where systems with the most vulnerabilities receive the least effective remediation.

Detection: Correlate system vulnerability count with patch success rate.

Indicator: Systems with ¿100 vulnerabilities show 60% lower patch success rates, creating persistent attack surfaces.

4 Initial Evidence and Results

4.1 Pilot Deployment

Three organizations participated in 90-day pilot deployments: - Financial services firm (10,000 endpoints) - Healthcare network (5,000 endpoints) - Technology company (8,000 endpoints)

The CPF system operated in parallel with existing vulnerability management, analyzing behavioral patterns without disrupting operations.

4.2 Quantitative Results

4.2.1 Improved Prioritization

CPF-adjusted prioritization showed significant improvements over CVSS-only approaches:

Table 1: Vulnerability Prioritization Performance

Metric	CVSS-Only	CPF-Adjusted
Coverage of exploited vulnerabilities	62%	81%
Mean time to mitigation (days)	19.4	15.2
False positive rate	8.3%	18.7%
False negative rate	12.1%	4.2%

The 30% improvement in covering actually-exploited vulnerabilities is particularly significant, as these represent prevented breaches.

4.2.2 Pattern Validation

Detected patterns correlated strongly with security outcomes:

- Organizations with high manic defense scores (¿0.7) experienced 3.7x more breaches through unpatched known vulnerabilities - Severe splitting (¿0.8) correlated with targeted attacks through neglected systems in 73% of cases - Repetition compulsion patterns predicted recurring incidents with 67% accuracy

4.3 Qualitative Insights

Beyond quantitative metrics, CPF revealed previously unknown organizational vulnerabilities:

Financial Services: Discovered severe splitting between trading systems (94% patch rate) and risk management systems (23% patch rate), despite identical technical criticality. This reflected unconscious organizational dynamics where profit-generating systems were idealized while control systems were devalued.

Healthcare: Identified temporal vulnerability windows at shift changes (7 AM, 7 PM) with 67% reduced incident response capability. Also found post-audit collapse patterns with 80% reduction in patching for 30 days following compliance audits.

Technology: Detected repetition compulsion with SQL injection vulnerabilities recurring every 87 days despite repeated patching, suggesting unresolved development practices rooted in organizational trauma from a previous data breach.

4.4 Trade-off Analysis

The CPF approach involves explicit trade-offs. The false positive rate increased from 8.3% to 18.7%, meaning more vulnerabilities were flagged as high-risk that didn't get exploited. However, the false negative rate decreased from 12.1% to 4.2%, meaning fewer exploited vulnerabilities were missed.

In security contexts, this trade-off is appropriate. The cost of patching an unexploited vulnerability (false positive) is orders of magnitude lower than suffering a breach (false negative). With average breach costs at $4.45 million[4] versus patching costs of $50-500, the system can tolerate thousands of false positives for each prevented true positive.

5 Implementation Considerations

5.1 Privacy-Preserving Design

A critical concern with psychological assessment is privacy. CPF addresses this through technical safeguards:

- **Aggregation**: All analysis operates on groups (minimum 10 individuals), never profiling individuals
- **Differential Privacy**: Noise injection (ε=0.1) prevents individual identification
- **Role-Based Analysis**: Focus on roles and departments, not persons
- **Temporal Delays**: 72-hour minimum delay prevents real-time surveillance

These safeguards ensure that CPF provides organizational intelligence without individual surveillance.

5.2 Integration Architecture

CPF integrates non-invasively with existing infrastructure:

1. Read-only API access to vulnerability scanners (Qualys, Tenable, Rapid7)
2. Parallel processing without modifying existing workflows

3. Risk multipliers (1.5x-3.0x) adjust existing CVSS scores

4. Standard output formats (CEF/LEEF) for SIEM integration

Organizations can adopt CPF incrementally, starting with monitoring mode before active prioritization.

5.3 Computational Requirements

Processing 100,000 vulnerabilities requires: - 2-3 seconds computation time - ¡500 MB memory - 2-4 CPU cores

These modest requirements enable deployment on existing infrastructure without significant investment.

6 Research Agenda

6.1 Validation and Refinement

While initial results are promising, extensive validation is needed:

1. Scale: Expand to 20+ organizations across diverse sectors to establish statistical significance and identify sector-specific patterns.

2. Duration: Conduct 12-month longitudinal studies to validate long-term predictive accuracy and measure organizational adaptation.

3. Cultural Factors: Investigate how psychological patterns vary across cultures, as current models derive from Western organizational psychology.

4. Causation: Design controlled experiments to establish causal relationships between psychological patterns and security outcomes.

6.2 Theoretical Extensions

Several psychological theories could enrich the framework:

- **Attachment Theory**: How organizational "attachment styles" to vendors and technologies create vulnerabilities
- **Trauma Response**: How organizations process and recover from breaches
- **Systems Theory**: How organizational structure influences vulnerability propagation
- **Cultural Psychology**: How national and organizational cultures shape security behavior

6.3 Intervention Development

Identifying psychological vulnerabilities is only valuable if we can address them. Research priorities include:

- Developing targeted interventions for specific patterns - Testing the effectiveness of psychological vs. technical remediation - Creating organizational "therapy" protocols for security dysfunction - Designing psychologically-informed security architectures

6.4 Automation and AI

Future research should explore:

- Machine learning for pattern discovery - Automated intervention triggering - AI-assisted psychological assessment - Predictive models for emerging patterns

7 Implications and Future Directions

7.1 For Security Practitioners

CPF offers practitioners a new lens for understanding persistent security failures. Rather than attributing unpatched vulnerabilities to "user stupidity" or "resource constraints," practitioners can identify specific psychological patterns and address root causes. This shifts the conversation from blame to understanding, from punishment to intervention.

Practitioners should: - Monitor for psychological patterns alongside technical indicators - Consider organizational psychology in security architecture - Design interventions addressing unconscious resistance - Recognize that technical solutions alone are insufficient

7.2 For Researchers

This work opens new research directions at the intersection of psychology and cybersecurity. The ability to detect psychological states from technical data enables studies previously impossible:

- How do organizational psychological states evolve during incidents? - Can we predict insider threats from psychological patterns? - How do different security tools affect organizational psychology? - What psychological factors determine security investment decisions?

The framework also raises methodological questions about privacy, validity, and intervention ethics that require interdisciplinary collaboration.

7.3 For Organizations

Organizations must recognize that security is not purely technical but fundamentally psychological. Investment in understanding and addressing psychological vulnerabilities may provide better returns than additional technical controls. This requires:

- Acceptance that unconscious factors influence security - Willingness to examine organizational dynamics - Investment in psychological alongside technical capabilities - Cultural change to address root causes

7.4 For Policy Makers

Current cybersecurity regulations focus on technical controls and compliance requirements. CPF evidence suggests that psychological factors may be more important determinants of security outcomes. Policy implications include:

- Incorporating psychological assessment into compliance frameworks - Funding research into behavioral security interventions - Developing standards for psychological security metrics - Creating incentives for addressing human factors

8 Limitations and Challenges

8.1 Current Limitations

The CPF approach has several limitations:

1. Validation Scope: Current evidence comes from three organizations over 90 days. Broader validation is essential before general adoption.

2. Cultural Specificity: Patterns identified in Western corporate environments may not generalize globally.

3. Gaming Potential: Organizations aware of assessment might attempt to manipulate metrics, though sustaining unconscious behavioral change is difficult.

4. Intervention Efficacy: While we can identify patterns, optimal interventions remain underdeveloped.

8.2 Adoption Challenges

Several factors may impede adoption:

- **Skepticism**: Security professionals may resist psychological approaches as "soft science"
- **Privacy Concerns**: Despite safeguards, organizations may fear psychological surveillance
- **Complexity**: Adding psychological dimensions increases system complexity
- **Cultural Resistance**: Examining unconscious dynamics challenges organizational self-image

9 Conclusion

The persistence of breaches through known vulnerabilities, despite massive security investments, indicates that our approach to vulnerability management is fundamentally incomplete. Technical severity metrics alone cannot explain why critical vulnerabilities remain unpatched while minor ones get immediate attention, why identical vulnerabilities receive different treatment across systems, or why certain vulnerabilities return cyclically despite remediation.

The Cybersecurity Psychology Framework offers a complementary approach that addresses these gaps by identifying and quantifying psychological vulnerability patterns. Initial results from three organizations demonstrate that psychological indicators—extracted from existing vulnerability management data—predict actual exploitation better than technical metrics alone, achieving 20-23% improvement in mean time to mitigation and 30% better coverage of exploited vulnerabilities.

This is not an argument for replacing technical assessment but for augmenting it with psychological dimensions. Just as modern medicine recognizes that health outcomes depend on both physical and psychological factors, cybersecurity must acknowledge that security outcomes depend on both technical and psychological vulnerabilities.

The framework raises important questions that require collaboration between security and behavioral science communities: How do organizational psychological states influence security outcomes? Can we develop effective interventions for psychological vulnerabilities? How do we balance psychological assessment with privacy? What are the ethical implications of organizational psychological analysis?

As cyber threats increasingly exploit human and organizational vulnerabilities rather than

purely technical ones, frameworks like CPF become essential. We invite researchers, practitioners, and organizations to collaborate in validating, refining, and extending this approach. Only by understanding and addressing the psychological dimensions of cybersecurity can we build truly resilient defenses.

The path forward requires courage to examine uncomfortable organizational truths, wisdom to address root causes rather than symptoms, and collaboration between disciplines traditionally kept separate. The stakes—in an era where cyber breaches can destabilize economies and societies—demand nothing less.

Acknowledgments

The author thanks the three pilot organizations for their participation and openness to psychological assessment. This work benefited from discussions with security practitioners who shared their frustrations with purely technical approaches, and from behavioral scientists who helped translate psychological theory into operational practice.

References

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

[2] Freud, S. (1920). Beyond the pleasure principle. In J. Strachey (Ed.), *The standard edition of the complete psychological works of Sigmund Freud* (Vol. 18). London: Hogarth Press.

[3] Gartner. (2023). Forecast: Information Security and Risk Management, Worldwide, 2021-2027. Gartner Research Report.

[4] IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

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

[6] Libet, B., Gleason, C. A., Wright, E. W., & Pearl, D. K. (1983). Time of conscious intention to act in relation to onset of cerebral activity. *Brain*, 106(3), 623-642.

[7] 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.

[8] National Vulnerability Database. (2023). CVE Statistics Report. NIST. Retrieved from https://nvd.nist.gov/general/visualizations/vulnerability-visualizations

[9] Cybersecurity and Infrastructure Security Agency. (2023). Ransomware Vulnerability Warning Pilot Program Report. CISA.

[10] Soon, C. S., Brass, M., Heinze, H. J., & Haynes, J. D. (2008). Unconscious determinants of free decisions in the human brain. *Nature Neuroscience*, 11(5), 543-545.

[11] Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Enterprise Solutions.