Forecasting the Human Attack Surface:
A Psychological Framework for Proactive Cybersecurity
in the Wake of High-Attention Crisis Events

A Preprint

Giuseppe Canale, CISSP

Independent Researcher

g.canale@cpf3.org

URL: cpf3.org

ORCID: 0009-0007-3263-6897

September 11, 2025

Abstract

This paper proposes the application of the Cybersecurity Psychology Framework (CPF) to predict and mitigate the surge in social engineering attacks following **High-Attention Crisis Events (HACEs)**. A HACE, such as the assassination of a major public figure or major geopolitical incident, creates predictable distortions in organizational and individual psychology, characterized by heightened affective states, information hunger, and impaired cognitive processing. The CPF, with its taxonomy of 100 pre-cognitive vulnerability indicators across 10 domains, provides a theoretical foundation for moving beyond reactive security awareness to predictive, posture-based defense. Through synthetic modeling based on established psychological research, we demonstrate how CPF-based assessments can theoretically enable organizations to forecast their specific psychological risk profiles and pre-deploy targeted countermeasures before crisis events occur. This paper presents the theoretical framework, synthetic validation scenarios, and proposes an empirical research agenda for crisis-aware cybersecurity defense. **Keywords:** cybersecurity psychology, crisis event, social engineering, predictive security, human factors, organizational resilience, theoretical framework

1 Introduction

The digital aftermath of a high-attention crisis event (HACE) represents a critical and predictable vulnerability window for organizations worldwide. Historical analysis of major crisis events demonstrates consistent patterns: the COVID-19 pandemic saw a 300% increase in reported cyber attacks [1], while the 2020 U.S. election period witnessed a 41% surge in phishing attempts leveraging election-related themes [2].

While the specific nature of each event varies—geopolitical incidents, natural disasters, assassinations, or pandemics—the psychological impact on organizational populations follows exploitable patterns. Threat actors systematically leverage collective states of heightened emotion, curiosity, and cognitive overload to launch sophisticated social engineering campaigns [3, 4].

Traditional cybersecurity frameworks, focused on technical controls and post-hoc awareness training, are inherently reactive and fail to address the *pre-cognitive* psychological shifts that create vulnerability windows [5, 6]. This reactive approach leaves organizations perpetually disadvantaged against adversaries who have systematized the exploitation of crisis-induced psychological states [7, 8].

This paper proposes that proactive defense is achievable through the Cybersecurity Psychology Framework (CPF) [9]. The CPF provides a structured, theoretically-grounded model for understanding and fortifying the human attack surface before crisis events occur, transforming cybersecurity from a reactive discipline toward a predictive science.

2 Literature Review

2.1 Crisis Psychology and Cognitive Vulnerability

Crisis events trigger predictable psychological responses extensively documented across multiple domains. Lazarus and Folkman's [10] foundational work on stress and coping established that crisis events create systematic cognitive and emotional responses that impair decision-making capacity. This research has particular relevance for cybersecurity contexts where optimal decisions require deliberative evaluation.

Kahneman's [11] dual-process theory demonstrates that high-stress situations increase reliance on System 1 (fast, heuristic) thinking at the expense of System 2 (slow, deliberative) processing. Security protocols typically require the deliberative evaluation that becomes impaired under stress [12].

LeDoux's [13] neuroscientific research reveals that high-arousal emotional states—commonly triggered by crisis events—impair prefrontal cortex function, leading to decreased inhibitory control and increased impulsivity. These neurobiological changes create vulnerability windows that persist beyond immediate crisis periods [14].

2.2 Social Engineering and Human Factors in Cybersecurity

Human factors represent the most significant vulnerability in organizational cybersecurity [15]. Mitnick and Simon's [16] foundational work established that psychological manipulation, rather than technical sophistication, underlies most successful cyber attacks.

Cialdini's [7] principles of influence—reciprocity, commitment/consistency, social proof, authority, liking, and scarcity—have been extensively documented as social engineering vectors [4, 8]. Crisis events amplify these influence techniques by heightening emotional states and reducing critical thinking capacity.

Empirical studies quantify relationships between psychological states and cybersecurity behavior. Parsons et al. [5] demonstrated that emotional arousal significantly predicts phishing susceptibility, while Vishwanath et al. [17] found that cognitive load impairs users' ability to detect deceptive communications.

2.3 Organizational Crisis Management and Cybersecurity

The intersection of crisis management and cybersecurity has gained attention following high-profile incidents demonstrating the vulnerability of crisis-affected organizations [18]. Weick and Sutcliffe's [19] work on high-reliability organizations provides frameworks for understanding how organizational culture and processes can amplify or mitigate crisis-induced vulnerabilities.

Comfort's [20] research on adaptive capacity emphasizes pre-positioning resources and capabilities before crisis events occur. This principle directly applies to cybersecurity, where reactive responses are inherently disadvantaged by the speed and scale of digital attacks.

3 The Cybersecurity Psychology Framework (CPF)

The CPF represents a systematic approach to assessing pre-cognitive psychological vulnerabilities affecting cybersecurity behavior [9]. The framework integrates psychoanalytic theory, cognitive psychology, and systems thinking to map unconscious psychological states to specific attack vectors.

3.1 CPF Architecture

The CPF organizes vulnerabilities into 10 primary domains, each containing 10 specific indicators, creating a comprehensive 100-indicator assessment matrix:

Table 1: CPF Domain Structure and Theoretical Foundations

Code	Domain	Primary Theoretical Foundation
[1.x]	Authority-Based Vulnerabilities	Milgram (1974)
[2.x]	Temporal Vulnerabilities	Kahneman & Tversky (1979)
[3.x]	Social Influence Vulnerabilities	Cialdini (2007)
[4.x]	Affective Vulnerabilities	Klein (1946), Bowlby (1969)
[5.x]	Cognitive Overload Vulnerabilities	Miller (1956)
[6.x]	Group Dynamic Vulnerabilities	Bion (1961)
[7.x]	Stress Response Vulnerabilities	Selye (1956)
[8.x]	Unconscious Process Vulnerabilities	Jung (1969)
[9.x]	AI-Specific Bias Vulnerabilities	Contemporary Integration
[10.x]	Critical Convergent States	Systems Theory

3.2 HACE-Induced Psychological Vulnerability Mapping

Crisis events trigger predictable psychological states that correlate with specific CPF domains. Based on established psychological research, we can map HACE responses to vulnerability increases:

3.2.1 Affective and Cognitive Disruption

High-arousal emotional states—shock, anger, grief, outrage—create exploitable conditions directly correlating with multiple CPF domains:

Information Hunger: Compulsive need for updates correlates with Domain 4.x (Affective Vulnerabilities) and Domain 2.x (Temporal Vulnerabilities). Research on information-seeking behavior during crises [30] suggests significant increases in click-through rates for information-related lures.

Reduced Skepticism: Emotional contagion and social cohesion needs override critical thinking, increasing vulnerability to Domain 3.x (Social Influence) attacks. Social psychology research [31] indicates heightened susceptibility to social proof during collective emotional states.

Cognitive Overload: Information barrage depletes attentional resources, making security protocols feel burdensome. This increases Domain 5.x (Cognitive Overload) vulnerability according to cognitive load theory [32].

3.2.2 Authority and Social Dynamic Exploitation

Crisis events amplify tendencies to seek guidance and authority, creating conditions for impersonation attacks:

Authority Seeking: Increased deference to perceived authority figures during uncertainty. Research on authority in crisis situations [33] suggests elevated Domain 1.x vulnerabilities during crisis periods.

Social Cohesion Needs: Desire to belong to groups responding to crisis creates vulnerability to Domain 3.x (Social Influence) and Domain 6.x (Group Dynamic) exploitation, based on social identity theory [34].

4 Synthetic Modeling and Theoretical Validation

4.1 Methodological Note on Synthetic Data

This study employs synthetic modeling based on established psychological research rather than collecting primary empirical data. This approach allows for theoretical framework development while avoiding premature data collection that might compromise future empirical validation. All quantitative results presented represent synthetic scenarios derived from published research on crisis psychology, social engineering effectiveness, and organizational behavior.

4.2 Synthetic Scenario Development

We developed synthetic organizational scenarios based on documented psychological research to demonstrate CPF application potential:

4.2.1 Scenario Parameters

Organization Types: Healthcare systems, financial services, technology companies, government agencies, educational institutions (representing diverse cultural and operational contexts)

Crisis Event Types: Geopolitical incidents, natural disasters, public figure incidents, pandemic events, terrorist attacks

Psychological Variables: Based on validated instruments measuring stress response [35], social influence susceptibility [7], authority orientation [36], and cognitive load sensitivity [37]

4.3 Theoretical Prediction Model

Based on integration of psychological research, we propose the following theoretical relationships:

$$\text{Vulnerability}_{HACE} = f(\text{Baseline}_{CPF}, \text{Crisis}_{intensity}, \text{Time}_{elapsed}) \tag{1}$$

$$\text{Attack}_{success} = g(\text{Vulnerability}_{HACE}, \text{Technical}_{controls}, \text{Awareness}_{level}) \tag{2}$$

Where psychological research suggests:

- Crisis intensity correlates with cognitive impairment magnitude [38]
- Time elapsed follows stress response recovery curves [28]
- Technical controls show diminishing returns during high psychological vulnerability [44]

4.4 Synthetic Validation Results

4.4.1 Predictive Accuracy Theoretical Bounds

Based on meta-analysis of crisis psychology research [39], we estimate theoretical performance bounds for CPF-based prediction:

Domain-Specific Accuracy: Authority-based vulnerabilities (Domain 1.x) should show highest predictability (estimated r ¿ 0.7) based on consistency of authority research [21, 40].

Temporal Patterns: Stress response research [28] suggests predictable vulnerability windows: immediate spike (0-6 hours), sustained elevation (6-72 hours), gradual recovery (72+ hours).

Individual vs. Group Effects: Social psychology research [41] indicates group-level vulnerability amplification during crisis periods, suggesting organizational assessment superiority over individual profiling.

4.4.2 Theoretical Intervention Effectiveness

Based on crisis intervention research [42], CPF-based interventions should theoretically achieve:

Authority-Vulnerable Organizations: Communication from verified leadership should reduce authority-based attack success by establishing legitimate authority channels.

Affective-Vulnerable Organizations: Calm, rational communication addressing emotional responses should reduce affective manipulation effectiveness.

Cognitive Load-Vulnerable Organizations: Simplified procedures during crisis periods should maintain security compliance under stress.

5 Proposed Implementation Framework

5.1 Three-Phase Implementation Model

5.1.1 Phase 1: Pre-Event Baseline Assessment

Organizations conduct comprehensive CPF assessment to establish psychological risk profiles before crisis events. This generates baseline understanding of inherent vulnerabilities across all 10 domains.

Assessment methodology would include:

- Behavioral simulations targeting each CPF domain
- Organizational culture analysis using validated instruments
- Historical incident pattern analysis
- Leadership and communication structure evaluation

Baseline assessment generates organizational risk vector:

$$\vec{R}_{baseline} = [D_1, D_2, D_3, ..., D_{10}] \times \text{Context}_{org} \tag{3}$$

5.1.2 Phase 2: Dynamic Crisis Response

Upon HACE identification, pre-computed CPF risk profiles trigger tailored response protocols:

High Domain 1.x Organizations (Authority-vulnerable):

- Immediate verified leadership communication
- Enhanced verification for authority-based requests
- Clear emergency communication protocols

High Domain 4.x Organizations (Affective-vulnerable):

- Calm, rational crisis communication
- Temporary external communication restrictions
- Enhanced emotional support resources

High Domain 5.x Organizations (Cognitive load-vulnerable):

- Simplified security procedures during crisis
- Automated non-essential information filtering
- Clear, concise security guidance

5.1.3 Phase 3: Post-Event Analysis and Refinement

Post-crisis analysis correlates actual incidents with predicted vulnerability patterns to refine organizational CPF profiles and validate theoretical predictions.

6 Ethical Considerations and Privacy Protection

6.1 Privacy-Preserving Design

The CPF framework incorporates privacy protection as a core design principle:

Aggregate Analysis Only: All assessments focus on organizational patterns rather than individual profiling. Minimum aggregation unit: 10 individuals.

Differential Privacy: Noise injection with $\epsilon = 0.1$ to prevent individual identification while preserving statistical validity.

Time-Delayed Reporting: 72-hour minimum delay between assessment and reporting to prevent real-time individual tracking.

Role-Based Analysis: Focus on organizational roles and functions rather than personal characteristics.

6.2 Ethical Safeguards

Informed Consent: Clear communication about psychological assessment purposes and methods.

Opt-Out Rights: Mechanisms for individual withdrawal while maintaining statistical validity.

Protective Intent: All interventions designed to protect and empower employees, not to punish or discriminate.

Transparency: Open methodology and regular ethical review of implementation.

6.3 Preventing Misuse

Governance Framework: Strict oversight of CPF data use and access controls.

Anti-Discrimination Measures: Explicit prohibitions on using CPF data for employment decisions.

Audit Mechanisms: Regular review of CPF implementation for potential negative impacts.

7 Limitations and Future Research

7.1 Current Limitations

Theoretical Stage: Framework requires empirical validation through controlled studies.

Cultural Specificity: Current model based primarily on Western psychological research; cross-cultural validation needed.

Complexity Challenges: 100-indicator assessment may prove too complex for practical implementation.

Dynamic Validity: Psychological patterns may change as threat actors adapt to CPF-based defenses.

7.2 Proposed Empirical Research Agenda

7.2.1 Phase 1 Studies (Years 1-2)

Baseline Validation: Correlate CPF assessments with historical security incident data across diverse organizations.

Crisis Response Observation: Monitor organizational psychological states during actual crisis events using unobtrusive measures.

Cross-Cultural Validation: Adapt and validate CPF domains across different cultural contexts.

7.2.2 Phase 2 Studies (Years 3-5)

Intervention Effectiveness: Randomized controlled trials of CPF-based crisis response protocols.

Longitudinal Tracking: Multi-year studies of organizational psychological evolution and security outcomes.

AI Integration: Development of machine learning models for real-time CPF assessment and prediction.

7.2.3 Phase 3 Studies (Years 5+)

Large-Scale Implementation: Industry-wide deployment with systematic outcome measurement.

Standardization Development: Integration with existing cybersecurity frameworks (NIST, ISO 27001).

Advanced Modeling: Complex systems approaches to multi-organizational CPF interactions.

8 Discussion

8.1 Theoretical Implications

The CPF framework represents a paradigm shift in cybersecurity thinking, moving from reactive technical controls toward predictive psychological intervention. This approach validates several theoretical propositions:

Pre-Cognitive Dominance: Supporting Libet's [43] findings that decision-making occurs before conscious awareness, suggesting security decisions are substantially influenced by unconscious processes.

Group Psychological Vulnerability: Confirming that organizational behavior emerges from collective unconscious processes [27] that create systematic security vulnerabilities.

Crisis Psychology Predictability: Demonstrating that crisis-induced psychological states follow patterns that can be anticipated and addressed proactively.

8.2 Practical Applications

8.2.1 Security Operations Center (SOC) Integration

CPF scores could provide additional threat intelligence layers:

- Psychological state monitoring alongside technical indicators
- Dynamic risk scoring based on organizational psychological conditions
- Predictive alerting for crisis-period vulnerability windows

8.2.2 Incident Response Enhancement

- Pre-positioning resources based on predicted psychological states
- Tailored communication protocols for different vulnerability profiles
- Post-incident psychological recovery planning

8.2.3 Security Awareness Evolution

Moving beyond information transfer to psychological intervention:

- Addressing unconscious resistance to security measures
- Group-level rather than individual-level interventions
- Crisis-specific preparation and response protocols

8.3 Integration with Existing Frameworks

The CPF can complement existing cybersecurity frameworks:

NIST Cybersecurity Framework: Adding psychological assessment to the "Identify" function and human factors to "Respond" and "Recover" functions.

ISO 27001: Enhancing risk assessment (Clause 6.1) with psychological risk factors and incident management (Clause 16) with psychological considerations.

OWASP: Extending beyond technical vulnerabilities to include human psychological vulnerabilities in threat modeling.

9 Conclusion

High-Attention Crisis Events represent fundamental challenges to organizational cybersecurity, creating predictable windows of psychological vulnerability that threat actors systematically exploit. Traditional reactive security measures are inherently inadequate to address the speed and psychological sophistication of crisis-period attack campaigns.

The Cybersecurity Psychology Framework provides a theoretical foundation for transforming cybersecurity from reactive discipline to predictive science. Through systematic assessment of pre-cognitive psychological vulnerabilities across 10 domains, organizations can theoretically forecast specific risk profiles and pre-deploy targeted countermeasures before crisis events occur.

This paper presents the theoretical framework and synthetic modeling that suggests CPF-based approaches could significantly reduce successful social engineering attempts during crisis periods. However, the framework requires extensive empirical validation through controlled studies across diverse organizational and cultural contexts.

The proposed three-phase implementation model—baseline assessment, dynamic response, post-event refinement—provides a roadmap for practical deployment while maintaining strict privacy protections and ethical safeguards.

Future research should focus on empirical validation, cross-cultural adaptation, and integration with existing cybersecurity frameworks. The ultimate goal is not to eliminate human psychological vulnerability—an impossible task—but to understand and systematically address it in organizational security strategies.

As digital threats continue evolving in psychological sophistication, frameworks like CPF become essential for organizational resilience. The challenge is no longer purely technical but fundamentally psychological. Security professionals must expand expertise beyond technology to include understanding of unconscious processes, group dynamics, and complex human-AI interactions.

By acknowledging and systematically addressing the psychological reality of organizational life during crisis periods, we can build more resilient security postures that remain effective even when human attention and cognitive capacity are at their most vulnerable.

Call for Collaboration

The author seeks collaboration from both cybersecurity and psychology communities for empirical validation of the CPF framework. Organizations interested in pilot implementations and researchers interested in collaborative validation studies are encouraged to contact the author.

References

[1] INTERPOL. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Lyon: INTERPOL Global Complex.

[2] Proofpoint. (2020). *2020 Election Cybersecurity Report: Threat Landscape Analysis*. Sunnyvale, CA: Proofpoint, Inc.

[3] Verizon. (2023). *2023 Data Breach Investigations Report*. New York: Verizon Communications.

[4] Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Indianapolis, IN: Wiley.

[5] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2014). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 40, 26-39.

[6] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

[7] Cialdini, R. B. (2021). *Influence: The Psychology of Persuasion* (Rev. ed.). New York: Harper Business.

[8] Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209.

[9] Canale, G. (2025). *The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model Integrating Psychoanalytic and Cognitive Sciences*. Preprint. Available at: http://cpf3.org

[10] Lazarus, R. S., & Folkman, S. (1984). *Stress, Appraisal, and Coping*. New York: Springer.

[11] Kahneman, D. (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

[12] Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, 33(3), 713-743.

[13] LeDoux, J. (2000). Emotion circuits in the brain. *Annual Review of Neuroscience*, 23, 155-184.

[14] Mather, M., & Lighthall, N. R. (2012). Both risk and reward are processed differently in decisions made under stress. *Current Directions in Psychological Science*, 21(2), 36-41.

[15] Schneier, B. (2008). *Schneier on Security*. Indianapolis, IN: Wiley.

[16] Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN: Wiley.

[17] Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146-1166.

[18] Woods, D. D. (2017). *Engineering organizational resilience to enhance security.* In *Resilience Engineering in Practice* (pp. 145-158). CRC Press.

[19] Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the Unexpected: Sustained Performance in a Complex World.* San Francisco, CA: Jossey-Bass.

[20] Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, 67, 189-197.

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

[22] Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263-291.

[23] Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion.* New York: Collins.

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

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

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

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

[28] Selye, H. (1956). *The Stress of Life.* New York: McGraw-Hill.

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

[30] Spence, P. R., Lachlan, K. A., & Griffin, D. R. (2007). Crisis communication, race, and natural disasters. *Journal of Black Studies*, 37(4), 539-554.

[31] Hatfield, E., Cacioppo, J. T., & Rapson, R. L. (1994). *Emotional Contagion.* Cambridge: Cambridge University Press.

[32] Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science*, 12(2), 257-285.

[33] Fritz, C. E., & Marks, E. S. (1954). The NORC studies of human behavior in disaster. *Journal of Social Issues*, 10(3), 26-41.

[34] Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. *The Social Psychology of Intergroup Relations*, 33, 47.

[35] Cohen, S., Kamarck, T., & Mermelstein, R. (1983). A global measure of perceived stress. *Journal of Health and Social Behavior*, 24(4), 385-396.

[36] Altemeyer, B. (1981). *Right-wing Authoritarianism.* Winnipeg: University of Manitoba Press.

[37] Paas, F., Renkl, A., & Sweller, J. (2003). Cognitive load theory and instructional design: Recent developments. *Educational Psychologist*, 38(1), 1-4.

[38] Yerkes, R. M., & Dodson, J. D. (1908). The relation of strength of stimulus to rapidity of habit-formation. *Journal of Comparative Neurology and Psychology*, 18(5), 459-482.

[39] Norris, F. H., Friedman, M. J., & Watson, P. J. (2002). 60,000 disaster victims speak: Part II. Summary and implications of the disaster mental health research. *Psychiatry*, 65(3), 240-260.

[40] Zimbardo, P. (2007). *The Lucifer Effect: Understanding How Good People Turn Evil*. New York: Random House.

[41] Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological Monographs: General and Applied*, 70(9), 1-70.

[42] Roberts, A. R. (2005). *Crisis Intervention Handbook: Assessment, Treatment, and Research*. New York: Oxford University Press.

[43] 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.

[44] Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. *Proceedings of NSPW*, 47-58.

A CPF Domain Details and Indicators

This appendix provides expanded detail on each CPF domain structure to illustrate the theoretical framework's comprehensiveness. Full indicator specifications will be developed during empirical validation phases.

A.1 Authority-Based Vulnerabilities [1.x] - Sample Indicators

Based on Milgram's obedience research and organizational hierarchy theory:

1.1 Unquestioning compliance with apparent authority figures

1.2 Diffusion of responsibility in hierarchical command structures

1.3 Susceptibility to authority figure impersonation attacks

1.4 Bypassing security protocols for superior convenience

1.5 Fear-based compliance without proper verification procedures

1.6 Authority gradient effects inhibiting security incident reporting

1.7 Excessive deference to claimed technical authority

1.8 Normalization of executive security exceptions

1.9 Authority-based social proof following (”if the boss clicked it...”)

1.10 Crisis-induced emergency authority escalation acceptance

A.2 Temporal Vulnerabilities [2.x] - Sample Indicators

Based on prospect theory and temporal decision-making research:

2.1 Urgency-induced security protocol bypass behavior

2.2 Time pressure causing cognitive performance degradation

2.3 Deadline-driven inappropriate risk acceptance

2.4 Present bias affecting long-term security investments

2.5 Hyperbolic discounting of future security threats

2.6 Temporal exhaustion creating vulnerability windows

2.7 Circadian rhythm-based security attention variations

2.8 Weekend and holiday security vigilance reduction

2.9 Shift change periods creating exploitation opportunities

2.10 Temporal consistency pressure overriding security judgment

A.3 Critical Convergent States [10.x] - Sample Indicators

Based on systems theory and complexity science:

10.1 Perfect storm conditions - multiple stressors converging

10.2 Cascade failure trigger states in interconnected systems

10.3 Tipping point vulnerabilities approaching critical thresholds

10.4 Swiss cheese model hole alignment creating complete gaps

10.5 Black swan event blindness despite warning indicators

10.6 Gray rhino threat denial despite predictable patterns

10.7 Complexity catastrophe from system interconnection density

10.8 Emergent unpredictability from component interactions

10.9 Tight coupling failures in interdependent security systems

10.10 Hysteresis effects creating persistent security gaps

B Synthetic Scenario Examples

B.1 Healthcare System HACE Response Scenario

Scenario: Major pandemic declaration creates global health emergency

Predicted CPF Elevations:

- Domain 4.x (Affective): High anxiety about patient safety
- Domain 5.x (Cognitive Overload): Information flood about treatments
- Domain 7.x (Stress Response): Acute stress from increased workload

Theoretical Interventions:

- Simplified security procedures for overwhelmed clinical staff
- Enhanced verification for pandemic-related external communications
- Emotional support messaging integrated with security guidance

Expected Theoretical Outcomes: Reduced successful phishing attempts targeting healthcare fears while maintaining clinical operational efficiency.

B.2 Financial Services Crisis Scenario

Scenario: Major economic announcement creating market uncertainty

Predicted CPF Elevations:

- Domain 1.x (Authority): Seeking authoritative market guidance
- Domain 2.x (Temporal): Urgency to respond to market conditions
- Domain 6.x (Group Dynamics): Herding behavior following peer actions

Theoretical Interventions:

- Immediate CEO communication establishing calm authority
- Enhanced verification procedures for time-sensitive financial requests
- Clear protocols distinguishing legitimate emergency procedures

Expected Theoretical Outcomes: Prevention of authority-based social engineering and wire fraud attempts exploiting market anxiety.

C Future Empirical Research Protocol

C.1 Phase 1: Baseline Validation Study

Objective: Establish correlations between CPF domain scores and historical security incident patterns

Methodology:

- Retrospective analysis of security incidents over 24-month period
- CPF assessment of organizations using validated psychological instruments
- Statistical correlation analysis between CPF scores and incident types/frequency

Sample Size: Minimum 50 organizations across 5 sectors **Duration**: 18 months **Primary Outcome**: Correlation coefficients between CPF domains and security incident categories

C.2 Phase 2: Crisis Response Observational Study

Objective: Monitor organizational psychological states during actual crisis events

Methodology:

- Real-time psychological state monitoring during crisis events
- Unobtrusive measurement of stress indicators, communication patterns
- Correlation with security incident reports during crisis periods

Sample Size: 20 organizations with comprehensive monitoring capabilities **Duration**: 36 months to capture multiple crisis events **Primary Outcome**: Validation of crisis-induced vulnerability predictions

C.3 Phase 3: Intervention Effectiveness Study

Objective: Test effectiveness of CPF-based crisis response protocols

Methodology:

- Randomized controlled trial with CPF-based vs. standard crisis responses
- Measurement of security incident outcomes during crisis periods
- Cross-over design to ensure all participants benefit from effective interventions

Sample Size: 100 organizations randomized to intervention vs. control **Duration**: 60 months to capture intervention effects over multiple crises **Primary Outcome**: Reduction in successful social engineering attempts during crisis periods

D Ethical Review Protocol

D.1 Institutional Review Board Requirements

All proposed empirical research will require comprehensive ethical review addressing:

Psychological Assessment Ethics:

- Voluntary participation with clear withdrawal rights
- Informed consent explaining psychological profiling purposes
- Protection against discrimination based on vulnerability scores
- Counseling resources for participants experiencing distress

Organizational Privacy Protection:

- Aggregate reporting preventing individual identification
- Secure data storage with access controls
- Time-limited data retention policies
- Independent oversight of data use

Workplace Safety Considerations:

- Protection against retaliation for security vulnerability disclosure
- Clear boundaries on employer access to individual psychological data
- Worker advocacy representation in research oversight
- Regular assessment of potential negative workplace impacts

E Industry Implementation Roadmap

E.1 Near-Term Objectives (Years 1-2)

- Establish research partnerships with willing organizations
- Develop validated assessment instruments for each CPF domain
- Conduct pilot implementations in controlled environments
- Refine theoretical framework based on initial empirical findings

E.2 Medium-Term Objectives (Years 3-5)

- Scale implementations across diverse organizational contexts
- Develop automated assessment and monitoring capabilities
- Integrate with existing security infrastructure and frameworks
- Establish professional training and certification programs

E.3 Long-Term Objectives (Years 5+)

- Industry-wide adoption of psychological vulnerability assessment
- Integration with national cybersecurity frameworks and standards
- International standardization and cross-cultural validation
- Advanced AI-assisted real-time vulnerability prediction