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 10, 2025

Abstract

This paper explores the application of the Cybersecurity Psychology Framework (CPF) to predict and mitigate the predictable surge in social engineering attacks following a **High-Attention Crisis Event (HACE)**. A HACE, such as the assassination of a major public figure, creates a temporary but severe distortion in organizational and individual psychology, characterized by heightened affective states, information hunger, and impaired cognitive processing. Threat actors systematically exploit these psychological conditions. The CPF, with its taxonomy of 100 pre-cognitive vulnerabilities, provides a model for moving beyond reactive security awareness to a predictive, posture-based defense. By conducting a baseline CPF assessment, organizations can forecast their specific psychological risk profile and pre-deploy tailored technical, procedural, and communicative countermeasures before a HACE occurs. This paper outlines the mechanistic relationship between HACE-induced psychological states and CPF categories, proposes a dynamic response model, and discusses the ethical imperative of this human-centric approach. **Keywords:** cybersecurity psychology, crisis event, social engineering, predictive security, human factors, psychoanalytic cybersecurity

1 Introduction

The digital aftermath of a high-attention crisis event (HACE) represents a critical and predictable vulnerability window for organizations worldwide. While the specific nature of each event varies—be it a geopolitical incident, a natural disaster, or the assassination of a prominent individual—the psychological impact on the human element within organizations follows a consistent and exploitable pattern. Threat actors, acting as opportunistic predators, immediately leverage the collective state of heightened emotion, curiosity, and cognitive overload to launch social engineering campaigns [1].

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 this vulnerability. This paper argues that a proactive defense is possible through the application of the Cybersecurity Psychology Framework (CPF), which provides a structured model for understanding and fortifying the human attack surface before a crisis even occurs.

2 The HACE-Induced Psychological Landscape

A HACE triggers a cascade of psychological responses that directly map to the vulnerability categories within the CPF.

2.1 Affective and Cognitive Overload

The immediate response to a HACE is characterized by high-arousal emotional states—shock, anger, grief, or outrage. Neuroscience confirms that such states impair prefrontal cortex function, leading to increased reliance on heuristic, System 1 thinking [2, 3]. This manifests as:

- **Information Hunger:** A compulsive need for updates, leading to lowered guards when clicking links or downloading files.
- **Reduced Skepticism:** Emotional contagion and a desire for social cohesion override normal critical thinking.
- **Cognitive Overload:** The constant barrage of information depletes attentional resources, making security protocols feel like an unbearable burden.

These states directly correlate with high scores in CPF categories **[4.x] Affective Vulnerabilities** and **[5.x] Cognitive Overload Vulnerabilities**.

2.2 Exploitation of Social and Authority Dynamics

Threat actors weaponize the natural human responses to crisis. The search for guidance and authority figures creates a prime environment for impersonation attacks. The desire to take action or belong to a group is channeled into malicious requests.

- **Authority Exploitation:** Phishing lures impersonating executives ("The CEO mandates a donation in light of recent events...") or IT support ("Urgent security update required due to the crisis...").
- **Social Proof Manipulation:** Malicious links shared within seemingly trusted social circles or communities galvanized by the event.

This exploits vulnerabilities mapped in CPF **[1.x] Authority-Based** and **[3.x] Social Influence Vulnerabilities**.

3 A Predictive Model Using the CPF

The CPF enables a shift from reactive warning to predictive pre-positioning. The model operates in three phases:

3.1 Phase 1: Pre-Event Baseline Assessment

An organization conducts a full CPF assessment to establish its baseline psychological posture. This identifies innate strengths and weaknesses *before* a crisis.

$$\text{Org}_{\text{risk-profile}} = f(\text{CPF}_{[4.x]}, \text{CPF}_{[3.x]}, \text{CPF}_{[1.x]})$$

An organization scoring high in **[4.1] Fear-based decision paralysis** and **[3.3] Social proof manipulation** now knows it is highly susceptible to HACE-based phishing.

3.2 Phase 2: Dynamic Response During a HACE

Upon the occurrence of a HACE, the pre-computed CPF risk profile triggers a pre-defined response protocol.

- **Targeted Communication:** The CISO immediately issues calm, clear guidance addressing specific predicted vulnerabilities: *"Team, in light of recent news, be extra vigilant. Remember: no official request for donations or urgent clicks will come via email without secondary verification."*
- **Enhanced Monitoring:** The SOC temporarily tunes its SIEM and EDR rules to elevate the priority of alerts containing keywords related to the event and to scrutinize outgoing traffic to newly registered domains.
- **Process Adjustment:** Recognizing cognitive overload (**CPF [5.x]**), the organization may temporarily simplify critical security procedures to reduce the chance of error.

3.3 Phase 3: Post-Event Integration and Learning

Post-crisis, the organization analyzes its performance. Did the measures mitigate the expected volume of incidents? This data is fed back into the CPF model, refining the organization's understanding of its own psychological vulnerabilities and improving its response for future events.

4 Ethical Considerations

Applying psychological models in security requires rigorous ethical safeguards. The CPF, as designed, mitigates risk by:

- Focusing on **aggregate, group-level patterns**, not individual profiling.
- Being **transparent** with employees about the rationale behind crisis-specific security measures.
- Using predictive models to **empower and protect** employees, not to punish or discriminate.

5 Conclusion

A High-Attention Crisis Event is a psychological phenomenon as much as a news event. By recognizing the predictable human vulnerabilities it creates, organizations can abandon a purely reactive stance. The Cybersecurity Psychology Framework provides the necessary scientific foundation to forecast the human attack surface. By pre-emptively addressing the psycho-cognitive vulnerabilities mapped by the CPF, organizations can build a more resilient, human-aware security posture that remains effective even when human attention is at its most vulnerable.

References

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

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

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

[4] Canale, G. (2025). *The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model*. Preprint. http://dx.doi.org/10.2139/ssrn.5387222