WHITE PAPER

December 2024

Leveraging Cognitive Security and Cyber Psychology for Enhanced Cyber Defense

Written by:
Brian McElyea and Sumona Banerji

RELI Group

MindShield INSTITUTE

RELI Group MindShield INSTITUTE

Leveraging Cognitive Security and Cyber Psychology for Enhanced Cyber Defense

The Crisis in the Security Landscape

More than 90% of successful cyber attacks are due to social engineering and human error.

The human suffering associated with cyber attacks is immeasurable, and mental health issues caused by digital threats are on the rise.

$9.5 Trillion Cyber crime now accounts for $9.5 trillion in financial losses.

$1 Trillion Poor mental health is estimated to cost $1 trillion per year in lost productivity.

Cybersecurity is like a fortress—strong walls mean nothing if the gatekeeper can be deceived. With more than 90% of cyber attacks exploiting human vulnerabilities through social engineering and error, it's clear the battlefield isn't just digital; it's psychological. RELI Group's cyber platform integration and MindShield's pioneering approach blend cybersecurity and cognitive sciences to create a new approach to defense called Cognitive Security (CogSec), aims to mitigate these vulnerabilities while simultaneously fostering workforce mental health. This approach will strengthen every organization's frontline defense: humans.

Our approach doesn't just protect systems—it builds resilient individuals equipped to counter evolving digital threats.

Cybersecurity is like a fortress—strong walls mean nothing if the gatekeeper can be deceived.

Why Now? Why Should You Care?

As of today, cyber crimes cost the global economy $9.5 trillion, with ransomware attacks surging by 38% in 2023. Beyond just financial loss, cyber crime exacts an even greater toll on an ill-prepared workforce, including anxiety, burnout and an onslaught of ever-more-sophisticated threats.

More importantly, the United States is facing unprecedented challenges in the cognitive warfare domain. The use of cognitive warfare to target a nation's human capital is a growing threat vector. Cognitive warfare degrades the capacity to know, produce or thwart knowledge, and it is not limited to the military or institutional world. Since the early 1990s, this capability has tended to be applied to the political, economic, cultural and societal realms. Any user of modern information technologies is a potential target, because cognitive warfare targets the whole of a nation's human capital.

Costing businesses $4.65 million per incident (IBM, 2023), an estimated 98% of cyber attacks leverage social engineering techniques (Verizon, 2023). Phishing alone accounts for 90% of successful breaches. Humans represent a critical weak point in most organization's cybersecurity systems.

MindShield's innovative solutions aim to support the fight against cognitive warfare with a goal of transforming the weakest link—the human factor—into the strongest point of defense.

This white paper outlines two immediate use cases of Cognitive Security:

- Personalized Training with Cyber-Psychological Mapping
- Enhancing Decision-Making During Cyber Incidents with Cognitive Cyber Engineering.

These cases demonstrate how leveraging cognitive insights can transform cybersecurity training and fortify human defenses against digital threats.

Why is Cognitive Security Crucial?

Cognitive security focuses on protecting human minds from manipulation, social engineering and psychological attacks that exploit cognitive vulnerabilities.

Recent, sharp increases in cyber harassment (nearly 40% of internet users now report experiencing online abuse [Pew, 2023]) further exacerbate the situation, harming not only individuals, but also increasing the threat to workforce well-being and damage to organizational reputations.

The U.S. is facing unprecedented challenges in the Cognitive Warfare domain.

Attackers increasingly manipulate cognitive biases, using fear, urgency and authority to compromise decision-making. Combating this demands innovative strategies that blend cyber-psychology expertise with tailored and personalized AI tools and training. Cognitive security is essential for modern cybersecurity frameworks, safeguarding both technological systems and the people behind them.

Organizations must adopt comprehensive cognitive security strategies integrating awareness, education, proactive policy and technology to combat these pervasive threats.

The convergence of Cyber-Psychology and Cognitive Security is shaping the future of cybersecurity by addressing the critical human element often overlooked in traditional approaches.

Use Case 1: Personalized Training with Cyber-Psychological Mapping

Scenario Overview

A government agency augments its current standardized "one size fits all" phishing campaign with a tailored phishing training program using cyber psychological profiling. By segmenting employees based on personality traits such as openness, agreeableness and risk tolerance, as well as influence traits such as emotional influence, social influence, informational influence and so forth, the program delivers targeted interventions to mitigate cognitive vulnerabilities.

Implementation Details

Organizations using this program can opt in for different levels of certification such as "MindShield Level 1 Certified" or "MindShield Level II Certified" and so on, as different organizations will want to implement things progressively and customized to specific needs. Many HR and software quality programs use similar structures such as CMM Level 1 to Level 3 in the software industry.

For example, Level I would be quick and easy, with an average completion time of 8-10 days from assessment to general cognitive security awareness. It would include guidelines to follow with a curated threat and response log to maintain and sign off on every quarter. A list of potential stages for each level is included below.

Implementation Stages

1. Psychological Assessment
   - Employees complete an assessment identifying individual decision-making processes as well as specific areas of susceptibility to manipulation and influence. For instance, high agreeableness may increase susceptibility to phishing emails with altruistic appeals or authoritative commands.
2. Tailored Training Modules
   - Employees prone to urgency cues receive training to recognize emotional or anxiety triggers.
   - Risk-tolerant individuals focus on validating unexpected communications.
3. Gamified Simulations
   - Real-life phishing scenarios are customized to employee profiles, enhancing engagement and practical learning.

Expected Outcomes

- Reduced susceptibility to phishing attacks
- Higher engagement and effectiveness through personalized content
- Improved workforce resilience by addressing cognitive biases.

Supporting Theories

This approach is grounded in Protection Motivation Theory (Sutton, 2015), emphasizing personalized threat relevance to motivate protective behaviors.

Expected Outcomes

- **Reduced susceptibility to phishing attacks**
- **Higher engagement and effectiveness through personalized content**
- **Improved workforce resilience by addressing cognitive biases**

Use Case 2: Enhancing Decision-Making During Cyber Incidents with Cognitive Cyber Engineering

Scenario Overview

A multinational agency faces a surge in phishing attacks targeting employees across various departments. Recognizing that quick, transparent decision-making is critical during incidents, the agency integrates cognitive cyber engineering into its response strategy. By leveraging insights into employees' cognitive strengths and stress responses, the enterprise ensures that decisions during cyber incidents are optimized for speed, accuracy and resilience.

Implementation Details

1. Cognitive Profiling and Stress Response Mapping:
   - Employees undergo a brief assessment to identify their cognitive styles (e.g., analytical vs. intuitive) and stress thresholds.
   - Profiles are created to map how individuals handle pressure, focusing on judgment and decision-making clarity under stress.
2. Customized Incident Response Training:
   - Employees with analytical strengths are trained in methodical, step-by-step threat analysis.
   - Intuitive thinkers receive training that hones rapid recognition of anomalous patterns and emotional triggers.
   - Stress-prone individuals are trained in mindfulness techniques to maintain focus during high-pressure situations.
3. Adaptive Cybersecurity Incident Playbooks:
   - Incident response plans are tailored to align with team members' cognitive profiles, assigning roles best suited to their strengths.
   - For example, during a phishing attack, an analytical employee might verify technical details while an intuitive team member identifies emotional manipulation tactics.
4. Simulated Stress Training:
   - Realistic scenarios replicate the pressure of real cyber incidents.
   - Employees practice maintaining composure, adhering to procedures, and leveraging their unique cognitive strengths under stress.

Expected Outcomes

- Faster, more accurate responses to cyber incidents
- Reduced decision-making errors under pressure
- Enhanced teamwork through role alignment with individual cognitive profiles
- Improved organizational resilience by addressing stress-induced vulnerabilities.

Supporting Theories

The approach incorporates the Yerkes-Dodson Law, which suggests optimal performance occurs at moderate stress levels, as well as the Cognitive Load Theory, which emphasizes the need to manage mental resources during high-pressure scenarios.

Expected Outcomes

- **Faster, more accurate responses to cyber incidents**
- **Reduced decision-making errors under pressure**
- **Enhanced teamwork through role alignment with individual cognitive profiles**
- **Improved organizational resilience by addressing stress-induced vulnerabilities**

MindShield Solutions

MindShield, in partnership with RELI Group, offers a groundbreaking blend of cognitive security, digital resilience and mental health integration to redefine how organizations approach cybersecurity.

We propose the next level up from traditional cybersecurity awareness training to Cognitive-Cyber Awareness Training™ (CCAT™). At the heart of this innovative training is the Cyber-Psychological Mapping, Cognitive Cyber Engineering, and the Cognitive Risk Assessment, psychometric tools designed to uncover knowledge gaps and behavioral vulnerabilities within teams. By identifying weaknesses in human defenses, organizations can implement targeted interventions that enhance their overall security posture and resilience.

To complement this, MindShield deploys AI-Driven Simulation Games that mimic real-world scenarios, training employees to respond effectively under high-pressure situations. These dynamic, interactive tools are tailored to reflect evolving threat landscapes, equipping teams with practical skills and confidence to handle complex cyber and psychological challenges.

Additionally, CCAT empowers employees to recognize and counteract social engineering attacks with foundational knowledge and advanced techniques. Together, these solutions create a robust cybersecurity framework that not only strengthens defenses but fosters a proactive, resilient culture, enabling organizations to stay ahead of ever-evolving digital threats.

MindShield, in partnership with RELI Group, offers a groundbreaking blend of cognitive security, digital resilience and mental health integration to redefine how organizations approach cybersecurity.

The convergence of Cyber-Psychology and Cognitive Security is shaping the future of cybersecurity by addressing the critical human element often overlooked in traditional approaches. Together, MindShield and RELI Group offer solutions that go beyond mitigating financial risks, fostering resilience by enhancing mental well-being and organizational awareness. The personalized training use cases demonstrate how leveraging psychological profiling can transform cybersecurity practices, empowering organizations to proactively defend against evolving threats while building a culture of adaptability and strength.

> **“The sphere of operations will expand from the physical domain and the information domain to the domain of consciousness; the human brain will become a new combat space.”**
>
> **—HeFuchu, Vice President of the PLA’s Academy of Military Sciences**