Cognitive Defense

A Thoughtful Approach to Human Risk Management

Human Risk Management Metrics

Cognitive Defense ™ is *the* trustworthy source of research, advisory, and training to improve **Human Risk Management (HRM)**.

We focus on measuring and improving the human element of people, process, and technology for sound cybernetic operations. We help improve **human cognition** to counter threats that attack **your** organization's content, technology, people, and relationships. At the same time, we help to adapt the technology to compensate for human limitations without reducing human performance.

Our attention is on the dramatically increasing threat posed by **influence operations, social engineering, phishing/spear-phishing, and multi-modal attempts to subvert your organization's operations.**

Malicious subversion leads to headline-grabbing security breaches that like the Coca Cola IP theft incident and the MGM breach. Both were ultimately realized through cognitive attacks on the human element. The list continues to grow and with it, the cost of breaches and business impacts.

> *While reasonable technical safeguards are often in place, it is painfully obvious that these safeguards can and will be bypassed either knowingly or unwittingly. Arguably, at the center of most cyber incidents are cognitive failures by **humans**.*

Training by Gaming

Key to our offering is our Training by Gaming experience, which provides a unique, tailored approach to counter-influence operations. Your people will learn how to deal with *influence operations* in a competitive and enjoyable environment. And you will learn their capabilities and limitations, so you can mitigate the residual risk through other methods. Our unique experiences use results from ongoing information gathering sessions to generate company specific scenarios that your workers will relate to and quickly learn from.

Doug Simmons, Cognitive Defense's CEO, President and co-founder has spent more than 30 years advising organizations around the world on their security strategies and architectures. As the Global Vice President of Gartner's (and Burton Group's) Security and Risk Management consulting group over many years, he helped and led hundreds of organizations develop, assess, and revise their approaches to information protection. He and his team have developed methods to identify human risk and measurable key risk indicators (KRIs) and key performance indicators (KPIs) associated with Human Risk Management and cyber issues.

> *Today more than ever, organizations need reliable advice that cannot be found by simply, searching the web for answers to important questions. In fact, with the advancement of Generative AI, many sources of once-reliable information are being tainted by hallucinogenic AI responses that can severely affect your ability to decide on the right path for your cybersecurity architecture, policies, processes, and governance.*

We serve security decision-makers, providing them with the content and tools they need to make and execute better security management decisions faster and more reliably. We do this by addressing the people and process issues as well as the technology issues at the business decision-making level.

Cognitive Defense

A Thoughtful Approach to Human Risk Management

Service Offering Overview

1. Each month, our analyst spends two hours guiding you through our online web tools that support the Judgment and Decision Making (JDM) application used for implementing standards of practice, which covers your organization specific cyber HRM issues broadly as follows:
   - The structure and makeup of cybernetic (IT) systems, content, mechanisms and related infrastructure.
   - Understanding of how your organization's specific cybernetic mechanisms operate and how those mechanisms support and limit success.
   - Understanding external regulatory environments, internal oversight requirements and responsibilities, and identifying established protection mechanisms and policies.
   - Identifying and understanding the current human risk management processes and potentials for loss.
   - Identifying the structure of cyber security and its management, including feedback and decision-making mechanisms that support control of the cyber security function within the organization.
   - Understanding the current HRM control architecture, including but not limited to protection objectives, access facilitation and controls, functional control units, trust, and change management processes.
2. After the first session's information capture, we prepare a unique Training by Gaming application to provide an ongoing learning experience for each target, modeling what an identified threat actor might typically do.
   - Using this gamified approach to influence operations training and awareness, these workers will learn about and deal with influence operations in a competitive and enjoyable environment.
   - These ongoing training exercises will help your workers improve skills without punishment and across multiple delivery media – and without interfering with Production operations or systems.
   - We do this by using characteristics of targets and consequences of actions, generating samples to test resistance. Using our customized, prepared templates from CogDef's library and augmenting this library with new templates over time, we prepare sample communications in different media (e.g., phone / email / text / social media)
   - This training by gaming application will apply AI methods for generation after analysis.
   - Preparation for deploying the training by gaming platform will be informed by requirements to measure effects, with the measurements to be pre-determined and agreed with you, so that appropriate instrumentation can be put in place and tested by end of this phase.
3. Monthly live online remote sessions of approximately 60 minutes with Cognitive Defense's CCIOP Lead will be used to:
   - Track and maintain progress against identified objectives.
   - Provide specific advice on specific critical human risk management topics you may be facing at that time.
   - Access to technologies in support of these efforts that include our SaaS service used to perform the CCIOP assessment.

For more information, contact doug@cogdef.com at Cognitive Defense

A Thoughtful Approach to Human Risk Management