Agent Surefire: Insider Threat Learning Objectives

I. Training Description:

Agent Surefire: Insider Threat is an immersive Information Assurance training simulation in Serious Games format raising employee awareness and "buy-in" on information security best practices. It is designed to effortlessly bridge daily practices with the most common cyber security threats and vulnerabilities. The engaging immersive content delivery allows learning by trial and error, situational awareness, immersed decision making, by way of identifying violations in a realistic work environment and real-world threat scenario.

II. Value Proposition

- Information Security Awareness training and skill development
- Broad awareness of cyber threats as well as proactively recognizing most common threats
- Turning knowledge into informed decision and targeted action
- Higher level mistakes demonstrated to raise awareness around complex attacks
- Hands-on practice of identifying threats as a follow-up to existing cybersec training
- Observing and experiencing cybersec threats from an inspector's vantage point
- Empowering the individual as the first defense against malicious threats against sensitive information

III. Training Objectives

A. Develop attention to detail

- Actively seek information
- Use your environment to recognize cyber security threats and vulnerabilities

B. Identify and distinguish between threats and vulnerabilities

- Physical environment
    - Dumpster Diving
    - Unauthorized privilege escalation
    - Unattended hardware
    - Unlocked storage
    - Traps set by hackers
- Computer Environment
    - Unauthorized privilege escalation
    - Spam and Phishing
    - Malicious Software

- Password security
- Abuse of Internet access

C. Develop critical thinking skills & ability to take proactive action

- Connect the dots between daily activities and information security vulnerabilities
- Be aware of potential adverse effects of small mistakes upon the very survival of the organization
- Recognize hard-to-notice dependencies between daily activities and security best practices
- Learn how Hackers think. (Path of least resistance)

IV. Results

A. Greater employee involvement in cyber security best practices (a culture of security)
   - Security-conscious employees
     - Making it difficult for attackers to trick employees in order to bypass cybersecurity technology
     - Employees carry security best practices into their personal environment, broadening the defense against complex attacks.

B. Prevention of considerable financial losses and legal hassles

C. Increased competitive advantage by reduced leakage of intellectual property

D. Greater confidence in the organization by clients, partners and employees

E. Reinforced employee loyalty by way of demonstrating company's commitment to protecting staff and client assets by investing on cutting-edge training technologies

V. Threats and Vulnerabilities Covered

The training/simulation contains more 120 cases of information security violations that are categorized under 12 main threat categories distributed around the virtual environment:

- Office cabinets and drawers security
- Improper disposal of sensitive documents
- Improper handling of sensitive documents
- Information used in social engineering
- Using predictable PINs
- Unauthorized access
- Malware infection
- Phishing messages
- Instant messaging abuse
- Insider abuse of internet access
- Lost laptop or lost portable devices

- Theft of Personally Identifiable Information (PII) and ePHI via lost portable devices

VI. Target Employees

Non-technical, general employee profile

All employees who handle sensitive information such as research & development, critical and strategic projects, marketing materials and accounting data, competitive services and confidential methodology, customer and business partner information, confidential employee information, etc.

VII. Training Duration

Completing the required training and identifying a minimum number of violations for a passing score takes 20-30 minutes.

The trainees have the option to spend additional time on the engaging storyline. This entertaining element increases interest in the subject matter, generating greater repetition resulting in better retention and broader awareness of more complex risks.

Administrators can place optional restrictions on game time during office hours. (See Technical Document)