NSA CYBERSECURITY & CRIME WORK GROUP

Sheriff David A. Goad (Ret.), Chair

Dennis Kelly, Esq., Vice Chair

WORK GROUP REPORT:

IMPLEMENTING CRITICAL AGGRESSION PREVENTION TO DEFEAT THE INSIDER THREAT WITH SCIENCE-BASED PREVENTION:

Strategies To Overcome The Cybersecurity Insider Threat Based On Human Psychology-Based Personnel-Management Measures Rather Than Machine-Driven Measures

JULY, 2024

IMPLEMENTING CRITICAL AGGRESSION PREVENTION TO DEFEAT THE INSIDER THREAT WITH SCIENCE-BASED PREVENTION:

Strategies To Overcome The Cybersecurity Insider Threat Based On Human Psychology-Based Personnel-Management Measures Rather Than Machine-Driven Measures

Introduction

Most generally-accepted efforts employed by cybersecurity programs to address the cyberthreat are technical, machine-driven, measures. Typically, these machine-driven measures either a) identify and remediate device breaches that have already occurred or b) overcome or bypass barriers to device functionality that are already in place, or c) prevent those device breaches from occurring in the first place.[1] In the series of meetings that have occurred in this Group's deliberations since 2018, too little attention has been given to addressing and effectively overcoming the human threat, especially the insider threat, that, by definition, must be addressed by human and psychologically-driven measures.[2]

Many U.S. law enforcement leaders and managers have experienced cyber breaches or attacks that are the product of the Insider Threat, rather than technical cybersecurity gaps, and, like many other kinds of crime, can be identified through human precursors that reflect negative human intent needing personnel management attention, rather than more and better machine-driven measures.

This Report of the NSA Cybersecurity and Crime Work Group ("Work Group") outlines the recommendation that law enforcement leaders and data system managers, as well as others responsible for data system defense, response and recovery, robustly implement human psychology-based personnel management measures, as well as technical, machine-driven measures, to perform their mission. This recommendation also reflects that, to achieve this outcome, Mission Critical Law Enforcement and Emergency Service Sector Agencies be trained in leading edge Critical Aggression Prevention Strategies (CAPS) as the foundation for these personnel management measures.

Summary Statement

[1] See, e.g., this discussion of the global cybersecurity threat addressing only machine-driven technologies. **Washington Post, A fatal program update: How CrowdStrike crashed global computer systems (July 19, 2024),** https://www.washingtonpost.com/technology/2024/07/19/bosd-outage-microsoft-crowdstrike/.

[2] It is too common for human/personnel management issues to be somewhat overlooked in analyzing the Cyberthreat, and to favor technical, machine-driven, issues. See, e.g., the following description of how Cyber Information Security Officers (CISOs) think, which contains extensive discussions of technical issues like "Antivirus Software", "Attack Surfaces", "Penetration Testing" and "Closing the Skills Gap with AI", but not even the mention of "Insider", "Insider Threat", or "personnel management": **bugcrowd, INSIDE THE MIND OF A CISO 2024: The Evolving Roles of Security Leaders** (June 2024), https://www.bugcrowd.com/wp-content/uploads/2024/06/Inside-the-Mind-of-a-CISO.pdf.

Critical Aggression Prevention Strategies (CAPS) support local law enforcement cybercrime investigations by providing law enforcement investigators with the benefit of vetted defensive measures that System owners and operators may implement to defeat the Insider Threat present in many cyber breach and attack scenarios. The Objective of CAPS Training is to deliver to System owners and operators the ability to identify indicators of aggressive behavior well before an incident/crime has occurs, thus preventing the incident/crime.

UAE Law Enforcement: A Case Study For Implementing CAPS

The United Arab Emirates is now one of the world's leading centers of Global Policing and Cybercrime Response, for reasons outlined here.[3]

in support of the UAE's crackdown on cybercrime sweatshops, several strategies can be implemented to enhance identification, prevention, and mitigation efforts. The core principle here is recognizing that "crime" itself is aggressive behavior, often going unnoticed until it occurs. CAPS allows investigative agency personnel to identify the precursors to crime, thus enabling prevention. This does not mean that Law Enforcement does not have "prevention" strategies, but government agencies often consider "prevention" by identifying someone planning or preparing for an attack. This is far too late in the sequence of events. In a CAPS scale which starts at a zero baseline and transitions through nine stages of aggressive behavior (the 9th Stage is the perpetrator of murder/suicide or terrorist), planning or preparing for an attack is Stage seven. CAPS has the ability to identify indicators of aggressive behavior well before an incident/crime has occurs, thus preventing the incident/crime.

1. Identification of Human Precursors to Cybercrime Involvement

A CAPS Program can train law enforcement and cybercrime task forces to recognize aggression precursors in individuals transitioning from trusted insiders to cybercriminals. According to CISA, up to 60% of successful breaches are perpetrated by insiders. This includes:

- **Cognitive Aggression Analysis:** Training officers to identify signs of insiders transitioning to cybercrime, such as manipulative or coercive behaviors common in cybercrime sweatshops.
- **Primal Aggression Indicators:** Recognizing precursor signs of individuals under duress, which can lead to errors of omission, a common issue in cybercrime vulnerability.

2. Proactive Monitoring and Surveillance

Agency authorities can implement a CAPS System to enhance monitoring and analysis in environments prone to cybercrime activities:

- **Predictive Analytics:** Utilizing CAPS's predictive tools to identify potential hotspots for cybercrime activities based on data trends and behavioral patterns.
- **Surveillance Training:** Improving surveillance techniques to detect suspicious CAPS precursor activities indicating cybercrime operations, such as unusual online behavior or unregistered workspaces.

[3] See https://img1.wsimg.com/blobby/go/6754d4ea-d143-490a-a31b-1d2bf066d416/3%20240720%20ESSCC%20Recent%20Developments%20Cybersecuri.pdf.

3. Law Enforcement Training Programs

Law Enforcement is notorious for their responding/reacting to incidents, not preventing them. This does mean that Law Enforcement does not have prevention strategies they simply are not reliable in part because they are based upon methods that are, like mental health assessments, far too subjective and notoriously inaccurate or their strategies require levels of sophistication that are well beyond law enforcement officers who are required to use them. CAPS instead uses measurable precursor-indicators of human-based aggressive behaviors that are scientifically reliable and do not violate privacy regulations. CAPS uses intuitive based indicators that most every Law Enforcement Officer can relate to, thus it is easy to understand, learn and utilize.

CAPS can be integrated into law enforcement training programs to address the unique challenges of cybercrime and human exploitation:

- **Scalable Online Training:** Providing CAPS online courses that are easily accessible for UAE law enforcement, enhancing their ability to prevent cybercrime.

4. Collaboration with International Bodies

Leverage the UAE's sponsorship of UNCOPS 2024 and other international law enforcement summits to promote CAPS as a global standard:

- **Global Training Standards:** Advocating for CAPS protocols in international (global) cybercrime as well as personal crime prevention strategies discussed at these summits.
- **Knowledge Sharing:** Facilitating the exchange of best practices and CAPS-related research among global law enforcement leaders.

5. Establishment of Specialized Units and Courts

Like the use of Red Flag Laws here in the United States, Law Enforcement has had great difficulties in getting to implementation because these methods of determining the guilt or innocence of an individual are often determined using Mental Health Assessments, which once again to far too subjective and thus notoriously inaccurate. It is too easy to apply punishments to innocent individuals. Support initiatives like the establishment of a special cybercrime court in Dubai with CAPS-informed protocols that are founded in science.

Support initiatives like the establishment of a special cybercrime court in Dubai with CAPS-informed protocols:

- **Specialized Training for Judges and Prosecutors:** Training legal professionals to understand and apply CAPS in cybercrime cases for better decision-making.
- **Integrated Approach:** Combining CAPS with legal and investigative frameworks to comprehensively tackle cybercrime.

6. Community Awareness and Education

Deploy CAPS to create awareness programs aimed at preventing individuals from falling victim to cybercrime employment traps:

- **Public Campaigns:** Launch campaigns educating the public about the precursor signs of cybercrime recruitment and how to report suspicious activities.
- **Victim Support Programs:** Establish support systems for individuals rescued from cybercrime sweatshops, providing psychological aid and reintegration assistance.

7. Enhancing Penalty Frameworks

Work with UAE officials to incorporate CAPS insights into a science-based platform for combating cybercrime:

- **Policy Development:** Using CAPS data to inform policies that address the root causes and impacts of cybercrime.
- **Legislative Advocacy:** Advocating for laws that not only penalize cybercrime but also focus on science-based prevention.

Case Study Conclusion

Implementing CAPS across these initiatives can significantly enhance the UAE's ability to combat cybercrime sweatshops. By focusing on prevention, training, and international collaboration, CAPS can transform reactive measures into proactive strategies, ensuring a safer and more secure digital environment.

Identified Possible Resources

We have listed below several resources that have an "insider threat" capability, and have provided contact information for those firms. As behavioral aspects are outside the scope of most cybersecurity service providers, these organizations operate well outside the scope of services of traditional Cybersecurity Service Providers:

• Center for Aggression Management, Inc., "Critical Aggression Prevention System (CAPS)," 11956, Iselle Drive, Orlando, FL 32827, 407-718-5637, https://aggressionmanagement.com/index.php

• ONITC, "Manage and investigate insider threats," 4009 Marathon Blvd., Austin, TX 78756, 512-572-7400, https://ontic.co/

• AT-RISK International LLC, "Insider Threat Program Development," 14100 Parke Long Ct, Chantilly, VA 20151, (703) 378-2444, https://at-riskinternational.com/

For Additional Information

Sheriff David Goad (Ret.), Work Group Chair, 301-368-2901, dgoad78@gmail.com
Dennis Kelly, Esq., Work Group Vice Chair, 504-251-0240, dkelly@basinstreettech.com
Dr. John Byrnes, Work Group SME, 407-718-5637, johnbyrnes@aggressionmanagement.com