The Case for Monitoring Unclassified Systems: Public Mask vs. Private Behavior

ManTech Insider Threat
M. Troy Bye | Brian Kruppenbacker | Philip Brooks
team-insider-threat-campaign@mantech.com

Research in social psychology has consistently shown that people tend to underestimate the extent to which their peers engage in undesirable behaviors, while overestimating positive ones. This misperception can lead individuals to publicly conform to perceived norms while privately holding different beliefs or engaging in contrasting behaviors. Studies in behavioral economics further illustrate this disparity, demonstrating how people often make choices in private that contradict their publicly stated preferences or values.
(Prentice, D. A., & Miller, D. T. (1993). Pluralistic ignorance and alcohol use on campus: Some consequences of misperceiving the social norm. Journal of Personality and Social Psychology, 64(2), 243-256.)

Employees may outwardly agree with security policies while privately engaging in actions that compromise organizational safety. This disconnect between stated values and actual behavior emphasizes the need for comprehensive monitoring systems that can detect anomalies and potential threats.

By implementing advanced insider threat detection tools on unclassified systems, organizations can:

- Identify discrepancies between an employee's public persona and private actions
- Detect patterns of behavior that may indicate a growing risk
- Intervene early to address potential issues before they escalate
- Create a more accurate picture of the actual security landscape within the organization

By acknowledging the potential gap between perception and reality, organizations can create a more resilient defense against insider threats, protecting both their assets and their employees from the consequences of misperceived norms and hidden behaviors.

Case Study:
John Doe, a systems administrator with a Secret clearance, had been employed by a defense contractor for five years. Known for his technical prowess, John's primary responsibilities involved classified systems. However, he also had access to the government unclassified network via a Contractor Wide Area Network (CWAN) for routine administrative tasks.

Unbeknownst to his colleagues, John had developed a severe gambling addiction, accumulating substantial debt.

One evening, while working late, John used his CWAN access to visit several online gambling sites. Desperate to recoup his losses, he began exploring sports betting, hoping for a windfall to settle his debts.

The company's User Activity Monitoring (UAM) system on the unclassified network flagged John's unusual behavior. Insider Threat algorithms identified the change in John’s baseline behavior:

1. Significant increase in after-hours network activity
2. Attempted access to unauthorized cloud storage services
3. Accessing documents unrelated to his current projects
4. Unusual patterns in external communications

The security team launched an investigation, uncovering a complex web of financial troubles and desperate actions. They discovered John's communications with individuals from competing companies, some with known foreign intelligence connections. These interactions were primarily centered around John's attempts to sell company information to alleviate his crushing debt. In one particularly alarming exchange, John had discussed the possibility of providing sensitive (though unclassified) customer project data in exchange for a substantial sum of money that would cover his mounting gambling losses and overdue mortgage payments.

While no classified information was compromised, John's actions violated company policy and potentially threatened national security by exposing sensitive corporate data. He was immediately suspended, his clearance was revoked, and legal proceedings were initiated.

Overlooked Early Warning Signs:
1. Gradual shift in login patterns: Over several months, John's access times increasingly occurred during evenings and weekends.

2. Expanded document access: John began opening files from departments unrelated to his responsibilities, a change that occurred incrementally.

3. Attempted use of unauthorized cloud services: There was a noticeable uptick in John's attempts to access free cloud storage sites.

4. Changes in email behavior: John's communication with external entities increased, including more frequent use of personal email accounts from work computers.

5. Unusual printing activity: A slight increase in printing jobs, often for documents outside his usual work scope, was observed.

Organizations should:

- Recognize that trusted employees can become insider threats
- Invest in automated systems that can aid in detecting unusual behavior patterns
- Take a continuous monitoring approach of analyzing subtle behavioral changes over time for each employee
- Provide regular security awareness training for all employees
- Implement and enforce strict policies on personal use of work systems

This case underscores the importance of:

Comprehensive monitoring of unclassified systems
The vast majority of our critical technology is often compromised through unclassified networks. Many technologies are initially developed in unclassified environments because their inherent nature isn’t sensitive—it's the specific applications, targeting, and employment that render them classified.

Unfortunately, by the time these technologies transition to classified status, they have often already been exposed or compromised through vulnerabilities in unclassified networks. This is particularly concerning as Controlled Unclassified Information (CUI), For Official Use Only (FOUO) data, export-controlled information, ITAR-regulated content, and proprietary information are routinely removed from unclassified networks, reflecting the constant struggle to protect sensitive technology from potential threats.

The indicators noted above, while seemingly minor in isolation, collectively painted a picture of changing behavior and potential risk. The case highlights the need for holistic analysis of user activities across all systems, particularly those considered less critical. It also emphasizes the importance of correlating data from various sources to identify patterns that may indicate evolving insider threats.

By addressing these aspects with a robust Insider Threat program organizations can better protect against insider threats risks and potential data loss.

Analysis and Fusion on High Side
Data Stored in Isolated/Protected SAN

How To Do it: