BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY I EMPLOYEE MANAGEMENT RELATIONS I THREAT ASSESSMENT & MANAGEMENT

FINANCIAL RISK

UNDERSTANDING THE EVOLVING RISK LANDSCAPE

Financial stability and responsibility are integral components of a secure and trustworthy workforce. While personal finances are generally considered a private matter, significant financial vulnerabilities can create a pathway for exploitation, coercion, or compromise, making individuals more susceptible to insider threat (InT). The evolving risk landscape of financial considerations and their potential connection to InT, including indicators, warning behaviors, and mitigation strategies now includes cryptocurrencies (crypto) that further obscure detection and mitigation. The classic red flags of employees experiencing severe financial stress or who have sudden unexplained wealth still apply but can now be more concealed. The emergence of cryptocurrency amplifies and complicates detection of this risk by offering new, less traceable, avenues for insiders to exploit for personal gain.

$5.6B

In 2023, losses related to cryptocurrency fraud rose by 45% over the prior year to more than $5.6 billion[1].

FINANCIAL STRESS → MOTIVATION → FACILITATION → INSIDER THREAT

Unmitigated stressors can motivate individuals towards concerning behaviors. Financial concerns are one of the common stressors in our current environment that can push an individual along the pathway of InT, closer to an identified InT incident.

Employees facing serious debt, bankruptcy, or other financial stresses may be tempted to misuse their access to sensitive information or assets. While this temptation can act as a ***motivator***, most individuals find appropriate ways to manage financial vulnerabilities.

Cryptocurrencies provide a way to quickly and pseudo-anonymously transfer stolen funds or sell confidential data, bypassing traditional banking oversight, and making detection more difficult. While crypto trading is neither illegal nor prohibited by the DoD, it provides a method for motivated individuals to carry out concerning behavior in a way that obscures their actions, ***facilitating*** malicious acts and rising as a new potential risk indicator meriting InT professionals' awareness.

DETECTING FINANCIAL RISK *(Potential Risk Indicators)*

Excessive Debt:
Signs of significant and unmanageable debt, include but are not limited to: *high credit card balances; payday loans; delinquent accounts; garnishments; and foreclosure notices.*

Gambling Issues:
Signs of problematic gambling behavior, online or in person, may be indicated by: *frequent visits to casinos or online gambling platforms; borrowing money to gamble; and concealing gambling activities.*

Stressful Events:
Significant life events that can cause financial strain may include: *medical emergencies; divorce; family changes (death, birth, eldercare); investment/crypto losses; home repair; educational expenses; and job loss or transition.*

Crypto Activity:
Significant or unusual cryptocurrency activity includes: *large or frequent transactions; use of foreign state-backed or hosted crypto exchanges or wallets; and investment in obscure or high-risk crypto.*

MITIGATING FINANCIAL RISK WITH INDIVIDUALS & ORGANIZATIONS

Enhanced Monitoring:
Combine monitoring of employee financial risk with network monitoring for unauthorized crypto transactions or wallet usage on company networks.

Awareness Training:
Provide regular training to employees on the risks associated with financial vulnerabilities, including fraud schemes, debt, crypto, and gambling. Emphasize reporting channels and requirements.

Financial Counseling:
Promote confidential financial counseling services to employees to help them manage debt and improve their financial literacy.

Proactive Planning:
Develop a response plan to address potential insider threat indicators and mitigate stressors related to financial vulnerabilities before they arise.

InT NEXUS WITH FINANCIAL VULNERABILITIES[2]

- $ **Intellectual Property Theft:** Compromised individuals may steal sensitive information or assets to alleviate financial pressure.
- $ **Extortion:** Financial debts or indiscretions can be used by malicious actors to blackmail individuals into compromising their organization.
- $ **Fraud:** Individuals may engage in fraudulent activities, both within and outside the organization, to improve their financial situation.
- $ **UD & Espionage:** Individuals may sell sensitive information to foreign adversaries or other malicious domestic actors in exchange for money.

1. Internet Crime Complaint Center (September 9, 2024) 2023 Cryptocurrency Fraud Report, FBI. 2. FTC (2023) Cryptocurrency deposits with no returns.