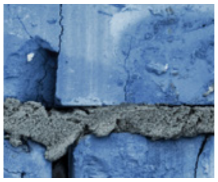
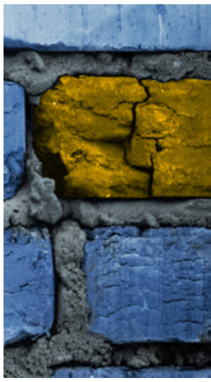
INSIDER THREAT PROGRAM DATA SHEET

Your People Can be Your Worst Enemy – or Your Best Defense.



Insider threats, both malicious and accidental, have become too common to ignore. In fact, **25% of all system breaches involve internal threat actors,** according to the Verizon 2017 Data Breach Investigations Report. Insider threat programs, designed to balance both tech and human vulnerabilities, are key to preventing these hidden threats from harming your business.



A comprehensive Insider Threat Program (ITP) can effectively, and proactively minimize damage from internal threats.

An Insider Threat Program affords a human layer of security that is becoming a practical requirement in today's world. As access to information becomes easier to obtain, and the vulnerabilities to compromise more numerous, protecting a company from fraud, blackmail, intellectual property theft and sabotage is a necessity — for the company's brand, reputation, stockholders and customers.

Unlike other firms that provide 'insider threat advisement', GRA Quantum places an emphasis on the human dimension of the problem rather than focusing chiefly on technical monitoring capabilities. The human and technical components of an Insider Threat Program are two sides of the same coin; and an effective program should focus on both.

Examples of ITP successes are rare when the mark of an effective program is that nothing of a damaging or criminal nature happens. Nevertheless, working recently with a client that was in the midst of updating his cyber security operation — and seeking to discover the source of damaging information leaks — GRA was able to discover through interviews and technical monitoring that several mid-level company executives, working with outside actors, were planning a hostile takeover of the company.

GRA QUANTUM

graquantum.com | info@graquantum.com

Our programs are tailored to the unique needs of our clients, but typically include:

- **Establishment and Adoption advisement**

  Guidance in developing an insider threat board, defining and allocating roles and responsibilities

- **Technology assessment**

  Analyze an organization's cyber architecture and installing the most effective technical tools to combat cyber threat

- **Workforce Training Program**

  Educate employees on how to avoid being victimized by cyber criminals, how to spot the signs of insider threats and how to address concerns without negatively effecting employee sense of well-being

- **Employee onboarding and off-boarding practices**

  Establish best practices and instruction for company leadership on the adoption of an ITP

- **Thorough new hire screening**

  Create recommendations based on specific job functions and organization's data sensitivity

- **Special Investigation Readiness**

  Pre-establish protocols and procedures to investigate the damage when hours and minutes really matter, so you're prepared to deal with the effects of a real-time insider threat scenario

Sample of Content from Our ITP Training Program:

WARNING SIGNS

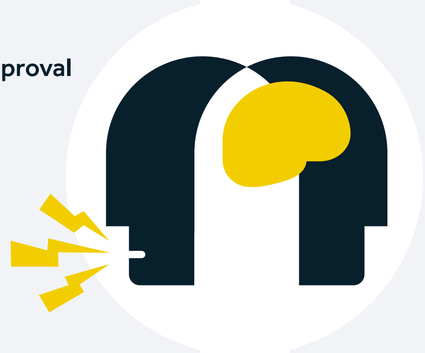
Changes in work and/or personal habits
(e.g., working weekends or outside normal working hours without authorization)

Initiation or escalation of vocal disapproval to company policy or goals

Tardiness or absences

On-the-job carelessness or diminished focus

Arguments with, or isolation from, family, friends and coworkers



MOTIVATIONS

Disgruntlement based on status
(e.g., lack of recognition, promotion or bonuses)

Greed, financial distress, or fear of job disruption including termination

Personal issues involving political or social change, family, religion, physical health, addictions or mental illness

Disagreement over company policies

Outside influences
(e.g., organized crime or foreign government intimidation)

GRA QUANTUM

graquantum.com | info@graquantum.com