



CLEARFORCE



Soft Targets & Insider Threat

SOFT TARGETS

Today's public venues, stadiums and amusement parks are acutely aware they present an inviting target for malicious actors to inflict great harm and casualty to our nation's unsuspecting public. Evidenced by the recent attacks overseas, international terrorist organizations, their affiliates, and "lone wolf" sympathizers view public events and venues as vulnerable, "soft targets" of opportunity. It is not coincidental that our nation's security apparatus also formally categorizes these same locations and events as "soft targets" that require planning, training and a reactive response should one become the target of terrorism.

PERIMETER AND PHYSICAL SECURITY

The majority of domestic security efforts and investment have focused on external threats, deploying perimeter based physical security measures to combat and deter threats.

Many of our public forums and workplaces have adopted layered defenses that employ the latest in physical security, electronic monitoring/surveillance and network based technologies. While these measures remain critical to ensuring public safety, the threat continues to evolve and a security strategy must now include an inward facing component to be considered comprehensive and effective.

INSIDER THREAT

One of the less obvious and most challenging of threats are the many employees and contractors who have internal access inside the organizational perimeter. Those within the trusted workforce who, for one reason or another, take actions or engage in behavior that negatively impacts the safety and security of the very organization they work for. Commonly referred to as “insider threats”, these employees and contractors become vulnerable to exploitation, susceptible to commit bad acts or, at a minimum, are distracted in the performance and execution of their jobs. This is the human side of insider threat, and regrettably, most organizations do not address this rising concern within their layered security approach. Surprisingly, many simply rely on a background investigation prior to hiring employees and contractors, then assume a level of trust for the tenure of employment. This practice has proved catastrophic across public and private sectors alike.

BEHAVIORAL ALERTS

ClearForce addresses the human element of this institutional security vulnerability in a manner that protects privacy, promotes transparency between an organization and its workforce, and mitigates risk. ClearForce leverages data, analytics and technology to identify early indicators of personal and financial stress through real-time, event-based alerts of criminal arrest, material and unusual changes in financials and other high-risk behavioral alerts based on organizational requirements and risk. ClearForce is configurable and operates as a Credit Reporting Agency with full employee consent and an FCRA and EEOC, legally compliant workflow while enabling consistent and appropriate action. As the only solution of its kind, ClearForce protects the workforce, the company and the venue 24 hours a day/365 days a year.

***ClearForce delivers
workforce assurance and
insider risk management***

For more information,
Contact ClearForce at
888-870-5773



CLEARFORCE