Insite
ADVANCED SECURITY MANAGEMENT

THE INSIDER THREAT

Red Flags and Risk Management Solutions for a Different Breed of Criminal

A white paper by:

Christopher Falkenberg | cfalkenberg@insitesecurity.com

Founder & President, Insite Security

One of the major responsibilities of many family office executives is hiring personnel to whom they entrust their clients' assets. Deficiencies in the background investigation processes commonly used to pre-screen employees may be putting those clients at serious risk for insider attacks.

This white paper examines key aspects of a threat that family offices are increasingly vulnerable to: insider attacks by employees. It identifies red-flag psychological traits of the insider-threat mentality by examining four high-profile national security breakdowns with serious implications for the family office. It also highlights the link between flawed government background investigation processes and hiring practices typically used by family office executives. And finally, it advocates that executives take immediate steps to adopt more advanced pre-employment screening processes and put in place systems to regularly monitor both new and veteran employees with access to valuable assets and sensitive information.

What's at Stake

James Bond movies and Tom Clancy thrillers may provide amusing family entertainment, but the rogue operatives they often portray are far from fictional. As the recent espionage activities of Edward Snowden prove, the insider threat posed by those with access to sensitive information is all too real -- and it is intensifying. Far from just a government problem, this type of criminal is also of urgent concern to the family office.

Snowden's act of espionage, the largest breach of classified information in U.S. history, has focused attention on deficiencies in the federal government's background investigation process. These deficiencies and the enormous vulnerability they revealed have triggered intense scrutiny.

One inevitable conclusion: federal background screening techniques are dangerously flawed and inadequate in their capacity to identify rogue employees likely to betray the United States. But why should Edward Snowden's insider attack, while clearly of national importance, be an issue of urgency for family office executives?

There's a simple, but troubling, answer: The pre-screening procedures that family offices currently employ in the hiring process are derived entirely from government security clearance systems. What's more, many private-sector screening techniques are only mediocre imitations of their public counterparts. The bottom line: If the hiring process is broken for the federal government, then it's broken for the family office as well.

In fact, the systems routinely used today by family office executives — and by the security firms they may employ to screen new hires — are subject to precisely the same weaknesses and problems that allowed Edward Snowden to gain access to classified information and then release it.

The result? Insider threats that poorly screened but highly placed employees pose for family office clients are virtually identical to the threat Snowden posed for U.S. national security. This points to massive vulnerabilities at every stage of the hiring process.

When it comes to background investigation, what should hiring screeners look for? What behaviors point to problems with prospective employees? Exploring the psychological mindset underlying potential insider threats offers valuable takeaways. Equally important, the recent espionage activities of Edward Snowden, Bradley Manning, and two earlier cases displaying similar patterns, highlight two imperatives for family office executives.

The first area of concern: identifying red-flag issues likely to emerge during the pre-employment screening process that may signal an insider threat. These red flags often involve personality traits, some subtle and easily masked, that indicate potential problems with prospective employees, especially those in sensitive, high-impact positions.

The second area of concern is the widespread lack of post-employment monitoring by family offices. This paper makes the case that operational security does not end when someone is hired: it must be an ongoing process. Rigorous, timely security procedures must be in place to identify significant threats that both new and veteran employees pose by virtue of the information they acquire as insiders. The paper also offers basic guidelines for post-employment security procedures.

The Insider Threat: Psychological Red Flags

Over the years, the intelligence community has made significant strides in analyzing the psychological underpinnings of people who commit espionage. Experts have identified a constellation of psychological traits and attitudes toward authority that tend to be shared by people who betray their loyalties. Some of these traits and behaviors can be summed up in "Psychology 101" profiles of three major personality disorders:

Narcissism: This is best described as unmerited feelings of self-importance and entitlement. Narcissists harbor grandiose views of their abilities and values — they are vain and arrogant. A narcissistic personality can be difficult to identify because its hallmark traits also appear in individuals with high levels of self-esteem and self-confidence. As a result, many successful people exhibit some degree of narcissism — and, on the surface, many narcissists appear to have healthy reservoirs of self-esteem and confidence.

In general, psychologists distinguish people who exhibit the pathology of a narcissistic personality from those who have strong self-confidence by identifying the degree to which a particular individual believes that the normal views of society do not apply to his/her actions.

Histrionic personality disorder: People diagnosed by psychologists with this disorder exhibit distorted self images and intense, unstable emotional behaviors. In general, they have an overwhelming desire and pathological need to be noticed. As a result, they often behave dramatically or inappropriately to capture attention. They are also highly suggestible.

Anti-social personality disorder: Also known as sociopathy, this disorder is marked by persistent failure to conform to social norms. Individuals exhibiting it are unconcerned with the rights of others; they are also indifferent to societal moral and legal standards. Characteristic behaviors include excessive drinking, fighting, and irresponsibility. A hallmark of this disorder: long-standing manipulative and exploitive behaviors that consistently and determinedly ignore others' rights and views.

People with this disorder frequently make a good first impression and manage interviews well. However, deeper research into their behavioral histories often raises red flags. For example, they tend to be effective at creating short-term relationships, but are unable to sustain long-term emotional connections.

Another warning sign: They disregard rules. This behavior may manifest itself in seemingly insignificant violations, such as lateness and/or absences. While these forms of rule breaking seem innocuous and incidental, they can indicate deep-seated antipathy toward authority. Patterns detected in these types of actions often point to insider-threat potential.

To see these disorders at work, let's turn to a rogues' gallery of insiders turned traitors. A brief review of four high-profile cases of espionage underscores some of the practical lessons that can be applied to pre-employment and post-employment investigative procedures.

From Insider Threat to Insider Attack

Each of the individuals profiled here outmaneuvered the experts assessing him. Each managed to gain access to valuable, highly sensitive information. And each chose to release that information, with far-reaching implications.

While Edward Snowden remains at large and may continue to wreak national security havoc from somewhere in Russia, we have the benefit of hindsight in the cases of Private Bradley Manning, Aldrich Ames, and Robert Hanssen — all of whom underwent intensive psychological assessments after being apprehended and imprisoned.

Edward Snowden

Oceans of ink have been spilled in efforts by armchair psychologists and the intelligence community to trace the behavioral trajectory and security lapses that contributed to Edward Snowden's insider betrayal. The jury is still out as to whether his potential as an insider threat could have been detected if more stringent employment review procedures had been in place.

Nevertheless, few would deny his stunning impact: Snowden is responsible for the largest breach of classified information in U.S. history. In analyzing his insider threat-turned-reality, we have access only to his actions, behavioral indicators, and his public statements made from afar. Taken together, these point to a high degree of narcissism and a reckless disregard for authority.

Clearly, Snowden wanted to be noticed and to attract widespread attention. His public statements also indicate that he believed that by acting as he did he could be an agent for good. Based on his self-proclaimed motives, Snowden exhibits significant and revealing rigidity in his views on what constitutes right and wrong. His moral stance is worth noting: He believes that his views on morality trump those of U.S. authorities: He has a greater loyalty to his own ethical compass and beliefs than he does to the American government.

Along with a high degree of narcissism, Snowden's statements reveal the presence of paranoia. One of his justifications for betraying the U.S. government is that he believes that it is out to "destroy privacy and basic liberties around the world."

Finally, Snowden has exhibited reckless behavior on several fronts: 1) the enormous volume of data he stole; 2) his decision to reveal his identity by conducting interviews so soon after he left the United States; and 3) the fact that some of the interviews he gave were conducted in close proximity to a CIA facility in Asia.

Even a cursory assessment of the background investigation process used to screen Edward Snowden raises red flags. Signs of dishonesty are readily apparent: In all, there are at least three significant misrepresentations in Snowden's CV. Background investigators could and should have flagged these during his security clearance process. And they should have been assessed prior to giving him access to high levels of classified information.

For example, the way in which Snowden reported his peripatetic educational background is an obvious warning signal. He claimed that he studied at John Hopkins University when, in fact, he attended a trade school only loosely affiliated with the university. He also exaggerated his course work in the United Kingdom. Another potential alert: Snowden failed to finish high school, obtaining a GED instead — an unusual trajectory in a candidate for high-level computer work and top-secret security clearance.

In retrospect, a question arises: Were Edward Snowden's misrepresentations, which should have been apparent to a talented background investigator, serious enough to indicate a small degree of sociopathy? And if so, was the pattern of his lies clear enough to warrant an initial determination that he was untrustworthy? As this case develops, it will be critical to analyze how and why his narcissism escalated to the point that he felt entitled to release sensitive public information and to pursue public attention for his actions.

Private Bradley Manning

Our second subject is Bradley Manning, now known as Chelsea Manning. After he was convicted of stealing government secrets, Manning identified himself as female and is currently seeking a gender reassignment surgery from the brig in Leavenworth, Kansas. Manning is the product of what has been characterized as an emotionally impoverished upbringing and struggled his whole life with issues of sexual identity and gender dysmorphia.

What is most amazing about Manning is that *after* he entered the army, he exhibited numerous signs that he was not worthy of trust and confidence. Despite this, he was pushed forward and eventually obtained a top secret SCI clearance — one of the highest clearance levels granted by the government.

Manning enlisted in the U.S. Army hoping that military discipline would resolve his gender confusion, but struggled in basic training and was scheduled to be discharged. Somehow, his discharge order was reversed and he was sent back to basic training, which he ultimately completed.

Bright and apparently capable, Manning was assigned to an intelligence unit where, despite almost being discharged from the military, he was granted a top-secret security clearance. Upon gaining this clearance, Manning was reprimanded for a serious security violation: posting YouTube videos within a SCIF (the acronym for a "secure compartmentalized facility") — an area in which cell phones and cameras are banned.

Manning struggled with emotional problems and was referred to military psychiatrists, who provided counseling to him. As he was undergoing counseling within his military unit, he was issued orders to deploy to Iraq. His commanding officer did not want to deploy Manning to Iraq because he thought that he would be a danger to himself and to others.

Yet, despite multiple warning signs: Manning's initial failure to complete basic training, his apparent psychological issues, his security violation, and his commanding officer's reluctance to deploy him, he was sent to Iraq. Once there, he was placed alone in an unsupervised area and granted access to reams and reams of highly classified information. While he was in this sensitive position, Private Manning's psychiatric problems continued to mount. In fact, the day before he committed his first security breach, he complained on his Facebook page of feeling *hopeless* and *totally alone.*

Aldrich Ames

Aldrich Ames was a senior CIA operative who provided information to the KGB between 1985 and 1991. Throughout his career, he was known to have significant problems with alcohol addiction. But even more revealing is the evidence of reckless and sociopathic behavior he showed early in his life. He was unable to finish college and recklessly stole a bike as a young person.

Throughout his career, Ames ignored basic rules by being chronically late in submitting work. In addition to his rampant procrastination, he was known in the CIA for being willfully inattentive to detail. On two separate occasions, he failed to fulfill critical security responsibilities and endangered a number of important intelligence operations.

One interesting aspect of the Ames case, revealed in interviews conducted in prison is his statement that, when he started spying for the KGB, he was initially motivated by money. Ultimately, however, he also came to see espionage as a game that he could win. He thought he was clever enough to come up with a plan by which he could reveal enough sensitive CIA data to induce the KGB to pay him a large sum of money without actually revealing any important information. Ames thought himself such a master of espionage that he could play the two parties off one another while profiting himself.

Robert Hanssen

Robert Philip Hanssen was an FBI mole who spied for the KGB and GRU (the Soviet military intelligence agency) for more than 20 years. A thorough assessment of his background revealed evidence of sociopathy. What came to the fore in post-imprisonment investigations was his degree of callousness and lack of remorse for his actions. He was also found to be impulsive, although evidence of this emerged only after his espionage was uncovered, when childhood friends revealed the reckless driving and other dangerous and thoughtless behaviors that Hanssen exhibited in as a young man.

Later in life he was extremely reckless in his sexual relations, cheating on his wife within two days of their marriage and engaging in voyeuristic activities. At one point, he released sexually explicit material about his marital relations that was detailed enough to easily identify both him and his wife.

National Security Meltdowns: Key Takeaways

So what is there about the U.S. government's background investigation process that failed in these cases, which span a total of 35 years? While a full assessment of America's national security lapses isn't possible here, a number of weaknesses are glaringly apparent from an investigative perspective. Chief among them:

1) *The system is entirely retrospective in nature*: Screening is limited to past actions rather than affect and patterns that point to future behavioral problems. As a result, it focuses on early warning signs as a pre-employment screen but virtually ignores post-employment signs of recklessness, deep-seated behavioral anomalies, and/or sudden behavioral changes.

2) *Screening programs lack a psychological component*: While the individuals profiled above exhibited identifiable signs of narcissism, sociopathy, and gender confusion — all these warning signals went unrecognized or were disregarded, with disastrous consequences.

3) *Screening programs focus on major life events*: As a result, they pay little or no attention to subtle but significant indicators of some of the psychological disorders described earlier. Investigators screen for criminal convictions without seeking to uncover information on objectionable "signpost" behaviors that did not result in arrest. Similarly, screeners look for litigation against former employers but don't analyze disputes that did not lead to public filings.

4) *Current screening systems take a narrow view on references*: National background investigations limit their interviewing process to references selected by employment candidates, but do not seek out other, often more relevant, people to interview. As a result, investigators do not gain a well-rounded view of prospective candidates or have access to information about behaviors that could signal future problems.

5) *Post-employment reviews are minimal or nonexistent*: Post-employment relaxation of standards and lack of monitoring have emerged as persistent problems for the U.S. national security program. Private Bradley Manning's obvious and well-documented struggles with his sexual identity and the psychological turmoil they caused *after* he joined the army is a case in point.

As noted earlier, the same inadequacies noted above are found in the screening practices widely used by family offices. What steps can family office executives take when hiring employees at all levels to decrease their clients' vulnerability to insider attacks?

The Imperative: A Comprehensive Screening Program

First and foremost, a hiring program should identify for positive traits that a family office values and wants to encourage, including the ability to work well with others, compassion, a willingness to take criticism, and the capacity to deal well with frustration.

On the preventive front, my firm has moved aggressively to develop a sophisticated two-pronged investigative strategy for our clients in order to forestall insider attacks: 1) a rigorous and comprehensive pre-employment screening process, and 2) ongoing post-employment monitoring. Here are some of the warning signals our system is designed to flag that family office executives should be alert to:

Look for early warning signs of misrepresentation: Dishonesty in applying for a job may take the form of inflating credentials — not necessarily a sign of psychological disorder. On the other hand, CV misrepresentations can be danger signs and signify future problems. They may indicate that, if hired, employees will not follow rules and regulations at work because they intentionally disregarded the rules of the application process.

In extreme cases, dishonesty in the application process can be an indicator of the psychopathology of narcissism or anti-social tendencies. Candidates who exhibit such tendencies may reflexively feel that rules do not apply to them and will therefore have little compunction about abusing positions of trust.

Look for lack of long-term stability and connection: Frequent turnover, as reflected in professional and personal life, is a warning sign that an individual has difficulty sustaining long-term commitments. Pay close attention to the length of time that employment references are commenting on. Someone

who doesn't get along well with others is unlikely to stay in the same employment situation for very long. Be very suspicious if every reference that a candidate gives indicates a short-term relationship. Even in cases where long-term employment relationships do exist, be on the alert for vague references in contrast to those that indicate long-standing social or business intimacy.

Look for red-flag personality traits: People who betray information acquired as insiders often have long-standing attitudes toward rules and people in positions of authority. As a result, people who dislike supervision, who resist suggestions, who hold grudges, and who have conflict-prone relationships with co-workers and bosses — are high-risk hires. So are people who can't release the anger and/or frustration that arise in daily life.

How do you determine if a potential employee exhibits these kinds of tendencies and behaviors? One strategy is to go beyond the traditional reference approach. In addition to requesting regular references, a hiring interviewer can require a candidate to provide a reference for someone with whom they didn't get along particularly well or didn't enjoy working with.

Note the applicant's response carefully. If applicants in their early twenties suggest that all their interactions with co-workers have been perfect — this may be acceptable. However, anyone who's applying for a senior position will have experienced problematic relationships at work.

If a prospective senior-level employee insists that all his/her relationships with supervisors, co-workers, and subordinates have been conflict-free — this should be viewed as a red flag. If the candidate does volunteer such a reference, then this person should be interviewed about how the candidate handled difficult situations and adverse decisions, and how flexible they are.

Look very carefully at litigation: In the best examples of due diligence investigations, meticulous research can uncover small claims cases. These may involve disputes that end up in court even though most people would have settled them through negotiation. These minor court cases have been helpful in establishing an individual's lack of suitability as an employee because their decision to litigate points to an inability to deal with conflict and/or to use accepted channels of conflict resolution.

The practices outlined above are vital in helping identify insider threats in the pre-employment hiring phase. However, as our rogues' gallery demonstrates all too well, once hired, seemingly trustworthy employees can commit acts of betrayal: Insiders can turn into betrayers over time. What steps should be taken to help ensure that people in positions to acquire insider information don't go rogue and put family office clients at risk?

Look for the sudden appearance of stressors: People turn from once-trusted employees into insider threats because of stressors that occur at work or as a result of outside stressors that profoundly affect their view towards work. While issues of employee privacy are an important concern, skilled post-employment monitoring can reveal the presence of new stressors that could conceivably lead to insider attacks.

Look for sudden behavioral changes: One example is hours worked, both from a schedule and duration standpoint. Another major warning sign: psycholinguistic changes — ways in which people change the methods and style by which they communicate. Using more "I's," "me's," and "my's" may be one sign of such a shift; the use of more negative words is another. There are programs designed to detect these changes in email transmissions.

Look for signs of financial problems: Both Aldrich Ames and Robert Hannsen claimed that they initially began spying in response to financial pressures. Stress in this area can be a potent trigger for insider attacks. Regular reassessments of employees' litigation and criminal histories, along with periodic credit checks, can help pinpoint emerging problems.

Conclusion

Hiring personnel is an extremely sensitive and high-risk responsibility. This is especially true given the inescapable fact that family offices, like most organizations, are increasingly vulnerable to insider attacks. Over time, employees at all levels can change. They can shift from being trustworthy to being a threat — and their access to valuable assets and privileged information can put clients at risk.

Yet most family offices — and the security firms they depend on — are using dangerously inadequate pre-employment screening techniques. What's more, it's highly likely that family offices have no rigorous post-employment process in place to provide regular re-assessment of current employees.

Given the growing threat of insider attacks, it is imperative that family office executives entrusted with hiring responsibilities take immediate steps to put in place comprehensive hiring programs with two major components: 1) a rigorous, sophisticated pre-screening process that features psychological assessments; and 2) ongoing post-employment reassessment to determine the risks that employees at all levels may pose for insider attacks.

About the Author

Christopher Falkenberg is the Founder and President of Insite Security, fulfilling his vision of providing world-class security and risk management solutions to corporations and affluent families.

Mr. Falkenberg is a former Special Agent of the U.S. Secret Service and an attorney. While with the Secret Service, Mr. Falkenberg conducted numerous protective advances for the President and other government officials both here and abroad as well as for visiting dignitaries. He led investigations of major fraud cases and participated in the successful prosecution and sentencing of the perpetrators.

Among his awards and citations, he received the Treasury Department's Special Service Award and was recognized for heroism following the 1993 World Trade Center bombing. As a litigator with Davis Polk & Wardwell, a large New York law firm, Mr. Falkenberg conducted corporate internal investigations and was involved in a variety of civil and criminal matters. Prior to that, Mr. Falkenberg clerked for a judge of the U.S. District Court for the Southern District of New York. He holds a Bachelor's degree from Kenyon College and a J.D. from Columbia University, both with honors. He is the former president of the northeast chapter of the Association of Threat Assessment Professionals.