



The most costly security incidents do not rush in from the perimeter as a single blind speed exploit. Threats from the outside tend to probe and test, to map and plan. Threats from the inside similarly tend to test the system in small ways before executing a full scale attack. Predictive analytics allow security practitioners to intercede in time to change outcomes; eliminating risks as they emerge and interrupting attacks before substantial damage is done.

The Insider Threat

by Lenny Holden

Page 1 of 4

Most of our customers have layers of security to control the potential threats posed by outsiders; however (and unfortunately) more often the real threats come from the inside – from your own employees.

It is a bit more difficult to identify an Insider Threat - an employee of potential concern.



For the purpose of this article an “Insider Threat” is any employee or person with legitimate access to your property who may steal Company property from your premises or from others who work or visit your premises, or who may cause damage to your business or brand through the spreading of rumours, innuendos, or business-related information to unauthorized persons (to include on social networks) – whether true or not.

Company Property includes assets, items, goods (perishable and non-perishable) and business-related information, to include knowledge of a personal nature of fellow employees.

There are indicators though that all managers and honest employees should be aware of to alert on a potential insider threat.

An Insider Threat to your business can go unnoticed for months, even years. The best way to defend against Insider Threats is to 1) educate your employees on the signs (indicators) of a potential Insider Threat, and 2) encourage your employees to report any suspicions of possible Insider Threats to management – such as through a Whistle Blower program on even an anonymous suggestion box.



Indicators of Potential Insider Threats

Personal Factors. Employees who display:

- Greed: A belief that money can fix anything.
- Financial Need: Excessive debt or overwhelming expenses.
- Anger/Revenge: Disgruntlement to the point of retaliating against the Company.
- Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, or perhaps a pending layoff.
- Divided Loyalty: Allegiance to another person/company who can be seen as a competitor.
- Adventure/Thrill: Want to add excitement to their life, intrigued by criminal or clandestine activity, "James Bond Wannabe."
- Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.
- Ego/Self-image: An "above the rules" attitude.
- Ingratiation: A desire to please or win the approval of another who could benefit with the expectation of returned favors.
- Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors.
- Family problems: Marital conflicts or separation from loved ones.

Page 2 of 4

Behavioral Factors. Behaviors that may be an indicator an employee is already stealing:

- Observed taking (or trying to take) Company property home.
- Seen in, or trying to access, areas not part of the employee's job responsibilities.
- Interested in Company matters not related to their work duties.
- Disregards Company policies.
- Seen on the premises after work hours or working odd hours not consistent with their work duties.
- Unexplained affluence; buys things they cannot afford on their income.
- Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.
- Overwhelmed by life crises or career disappointments.
- Asks inappropriate questions.
- Concern that they are being investigated.

Organizational Factors. A Company's lax security program may be a fertile environment for Insider Threats:

- The lack of access controls for employees – including employees departing from uncontrolled access points, no searching of staff, etc...
- No restrictions of sensitive areas to only those employees requiring access.
- Lack of CCTV coverage.
- Property not properly labelled.
- Undefined policies for the removal of property (to include taking work home).
- Perception that consequences of theft are minimal or non-existent.
- Employees are not trained on how to properly secure and protect the property they control or have access to.



Now that you know the indicators, you can make a difference and stop the Insider Threat(s)

- Educate and regularly train employees on security or other protocols. Remind employees that reporting security concerns is vital to protecting your company's well-being and its future. They are protecting their own jobs. Remind them that if they see something, to say something.
- Use appropriate screening processes to select new employees to include Police Checks and former employer checks. Be alert to (suspicious of) gaps in employment – this is perhaps an employment from which the new hire candidate was terminated from or had a bad experience at.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Ensure that proper security safeguards are in place.
- Report to the police and prosecute any employee(s) caught attempting to steal Company Property.

Insider Threat identified; now what?

Page 3 of 4

If your employees identify or you believe one or more of your staff are potential Insider Threats, you have several options:

- Request the employee to resign (with proper severance)
- Terminate the employee
- Report the employee to the local police
- Confront the employee
- Bring in outside security investigative service expertise
- Consult with your local security provider

Most companies given the options above will request the potential Insider Threat to resign quietly – make the problem go away. Given the employment situation in Cambodia most likely the Insider Threat will merely go to another similar Company and gain new employment straight away. This option not only encourages the Insider Threat to continue, but passes on a potential identified criminal to another company, and worse sends a “green light” to all other remaining staff that there are no real repercussions if they steal from your Company.

Terminating the Employee or reporting the employee to the police will only be successful if you have real evidence – not just suspicions. Both actions may eventually require a court hearing (either Labor or Civil) where hard evidence will need to be produced. Evidence can include catching the thief red-handed, CCTV footage, or perhaps credible witness statements. Without proper evidence selecting one of these two options will only result in additional costs above and beyond the cost to replace / repair the damage caused by the Insider Threat.

Confronting an employee is an option some Companies will select. If you select this option it is important to have all available facts (above and beyond suspicions) to include fellow employee statements, investigative actions, and then to prepare a proper list of questions prior to the interview / interrogation. The results of the confrontation will obviously result in selecting another option afterwards.



Bringing in an outside security investigative service may be the way forward but you run the risk of again possibly incurring additional costs on top of the losses already incurred.

A prudent measure would be not making the decision on which option to initially select unilaterally; first consult with your local security provider. They can bring in a fresh set of eyes, an outside perspective, and most likely have experience in similar situations. Based on a joint review and a joint internal investigation, the prudent option can be selected. Usually the best (ultimate) option is to terminate the employee and report the matter to the police for prosecution. This will send a message to all employees that employee theft will not be tolerated. But first investigate and get the evidence.

If you identify an Insider Threat and that person has already committed property theft, it is also important to review your current security program to see what measures need to be improved to prevent a similar act. When reviewing your security program consider all aspects to include:

- Physical Security
- System Security
- Guarding
- Personnel Security
- Security Procedures
- Security Education

Page 4 of 4

Again your security provider should be able to assist, consult, and recommend positive adjustments in your security program to mitigate, or hopefully negate, future similar incidents.