

Insider Threat Management

Lions Gate Investigations Group



Prepared By:

Scot Filer
Managing Partner
Lions Gate Investigations Group

Phone: 604-684-7753
Cell: 604-375-1669
Email: scotfiler@lgig.ca



Organized criminal enterprises target employees to obtain corporate information.....



.....regarding security practices, schedules, loads, routes, staffing levels, etc.



Corporate information is utilized by criminals to perpetrate highly organized thefts and robberies, resulting in a significant loss of money.

Introduction

This document is respectfully offered as information only. It is intended to provide the reader with a general understanding of the “insider threat” concern and how it could apply to their business. Although the term often refers to cyber threats, the writer is applying the term here, because it is a functional term for the other aspect of a business environment.

This document contains a definition of the “insider threat phenomenon, information about malicious employees including some psycho-social indicators of potential persons of interest and management strategies.

Definition of “Insider Threat”

The term “*insider threat*” is most commonly used when referring to current and past employees, contractors and vendors who possess sensitive information about a company’s corporate internal systems, data and operating procedures. These persons then sell or utilize their knowledge for an inappropriate or illegal purpose. This mis-use of information causes some form of damage to the company in the form of financial loss, loss of productivity, damage to reputation or may have some form of legal implication.

These individuals may act alone or in concert with others to perpetrate a variety of crimes against the company. The motivation for the act could be revenge, dissatisfaction with company management, financial gain, in response to duress or simply the excitement of the challenge.

The Issue

Insider threats are more difficult to detect than external threats. From a psychological perspective, it is more common, and easier to fear and mistrust outsiders than those entrenched within your own organization.

Employees have a significant advantage over others who may want to attack or victimize an organization. They can bypass physical and technical security measures designed to prevent unauthorized access. Mechanisms such as firewalls, intrusion-detection systems, and electronic building access systems are implemented primarily to defend against external threats. The problem is, employees are not only aware of the policies, procedures, and technology used in their organizations, they are often aware of the vulnerabilities in protocols and exploitable technical flaws.

Employees have access to and knowledge of, sensitive corporate information and procedures as a routine part of their work. Those employees with malicious or criminal intent are well placed and informed to cause damage to the company. It is difficult to identify an individual who is misusing corporate information. Unlike external threats where the indicators are often overt, internal threats are discreet and detection is challenging.

Company "A" - The Problem

The intelligence report submitted by Scot Filer documents a series of crimes against Company "A". These crimes have caused Company "A" millions of dollars in lost revenue and probably other issues that are unknown to the writer.

This problem is made more complicated by the following:

1. The crimes against Company "A" are being organized and perpetrated by individuals who are members of, or are associated to, organized criminal enterprises.
2. Reliable information from a confidential source implicates unidentified employees of Company "A" and their transportation arm, Company "B", are providing information to, or cooperating with, member(s) of the criminal enterprise.

Honest Mistake or Malicious Employee?

An analysis of these incidents should determine if one or more of these crimes resulted from unintentional mistakes, careless behaviour or malicious behaviour.

The nature of these crimes, even without the source information alleging that employees are involved, raises many investigative questions about how the crimes were committed. From a corporate, more global perspective, the following are a few questions that require consideration:

- What is the potential for another similar crime to occur?
- What will be the cost to the company?
- What other information is being stolen and for what purpose?
- Is this information being passed to the criminal group electronically or by other means?
- What specific information is being passed on?
- Are there risks to other aspects of the business as a result of these employees?
- Is there any relationship between the criminal groups responsible for these thefts and the cigarette smuggling and counterfeiting problem?
- Is there any link or relationship from the crimes in BC to similar thefts occurring elsewhere (southern Ontario)?
- Where do we stand civilly with potential liability issues?

Malicious Insider

Based on my experience analyzing and investigating crimes, I am confident that some, if not all of these crimes were aided and abetted by one or more employees of xxxxxxxx. What can be done about it?

This "insider threat" component requires immediate attention by the Corporate Security Department:

- To analyze each of the crimes and how they were perpetrated in an effort to identify vulnerabilities and patterns
- To identify the employees involved
- To determine the role they played in the crimes
- To identify the vulnerabilities in the processes and protocols that allowed them to operate undetected
- To recommend changes and improvements to any processes and protocols where vulnerabilities are identified
- To recommend any other operational and security related changes that will reduce the risk of similar crimes occurring in the future

An article written by has Dr. Jerrod Post, Kevin Ruby and Eric Shaw has identified six psycho-social characteristics of malicious insiders. The following personal characteristics are said to have direct implications for risk.

- Sense of entitlement
- History of personal and social frustrations
- Computer dependency
- Ethical flexibility
- Reduced loyalty
- Lack of empathy

An awareness of these indicators may be useful to line supervisors, managers and human resources personnel. These behavioural cues may be useful if attendance, discipline or performance issues arise with an employee. Employee interviews and investigation of these areas could provide corroborative evidence linking an employee to a related action or the specific criminal event.

From an investigative perspective the traditional goal to establish the employee's motivation and means to commit the crime remains the most reliable path to the source of the problem.

A thorough analysis of the crime details, a critical review of the corporate protocols, cross referenced with the employees actions will on most occasions lead to the identification of the connection between an employee and the action associated to the crime.

Strategies for Managing Insider Threats

Insiders can be stopped, but the task can be complex and time consuming. The challenge is relational to the depth of the problem. The most effective approach is that of a layered security strategy consisting of policies, procedures, technical controls and a seamless relationship between these component parts.

Effective insider threat management requires an organization to remain vigilant regarding the observation and detection of concerning or suspicious employee behaviour, information management, human resource hiring practices and operational protocols.

There are three phases of the insider threat management process:

1. Assessment
2. Prioritization & Review
3. Remediation

Assessment

The organization needs to understand their insider threat situation and exposures. Efforts should be made to audit insider activity through various assessment methods, including a technical exposure assessment, personnel interviews and policy reviews.

An automated technical exposure assessment (EA) using a network monitoring tool can detect activity patterns and user behaviour. This assessment will identify policy violations that may be occurring through electronic or internet-based communications. It may show that corporate information is leaking out through email, instant messaging or other internet-based activities.

EA results can be used to target persons of interest and areas of interest through the personnel interview process. Circumstances permitting, it is sometimes easier and more cost-effective to request that employees self-disclose in a consequence-free situation. The alternative for the security investigator is attempting to discover the threatening or risky behaviour through the investigative process. (i.e. security log reviews, CCTV footage, operational protocol reviews, etc.)

Lastly, a review of paper policy is critical to assessing areas of potential weakness. Policies may include legal or regulatory mandates, employee acceptable use and conduct guidelines and corporate governance requirements. This process, combined with the EA and personnel interviews may expose policies that are poorly defined or don't exist.

- Note: If the EA is to be implemented, it is recommended that it be done covertly to avoid warning employees and risking behavioural pattern changes regarding their use of technology.

Prioritization and Review

Once the assessment phase is completed and an Insider Assessment Report has been prepared, the next step is for a business review and prioritization session. This involves key members of the organization from IT, operations, human resources, legal, security and senior management to meet to review and discuss the results of the assessment.

Their objective is to identify, rank and prioritize the critical areas of concern. A simple ranking or scoring system can be utilized and applied to each item identified. Severity labels such as "low risk", "medium risk", "high risk" or "critical risk" are suggested.

After the prioritization process is completed, a report of the findings should be prepared. As the issues are dealt with, the report can be amended to document the changes.

Remediation

The last phase, after assessing the threats and ranking the critical risk areas, the organization can begin to address and remediate the threats. Decision makers need to keep in mind the need to match the remediation to the size of the threat.

Remediation efforts can take many forms:

- Re-installation or re-configuration of existing security systems both for the physical security and for the IT risk areas
- Purchase and implement new security tools
- Forensic investigations
- Employee awareness training
- Rewriting corporate policies
- Contracting for specialized consulting services
- Ongoing insider threat assessments
- Discharge, where justified and supportable, employees who have proven to be engaged in illegal or highly inappropriate behaviour

Remediation should involve consultation between the managers of affected departments and corporate senior management. This consultative process should strive to make people accountable, respond to budget concerns and assign a timeline and responsibilities for the tasks that follow.

Conclusion

There are no quick fixes for identifying and managing insider threats, be they physical threats, risks to assets or cyber related improprieties. The major obstacles are technical complexity, labour intensive process audits, potential for high costs and securing buy-in from senior management.

Security is not a project, it is a corporate function that continues to improve and evolve over time. The damage and cost to a corporation is potentially so much higher when insider threats go undiscovered or are ignored.

Scot Filer
Managing Partner
Lions gate Investigations Group

Office: 604-684-7753
Direct: 604-375-1669
Email: scotfiler@lgig.ca