Insider Threat

Protecting U.S. Business Secrets and Sensitive Information*

Jarrellann Filsinger, National Archives and Records Administration
Barbara Fast, CGI Federal
Daniel G. Wolf, Cyber Pack Ventures, Inc.
Charles H.Brown, C H Brown Consulting, LLC

June 2013

Introduction

Executive Order 13587 established the need for every agency and department in the U.S. Executive Branch to develop an insider threat program to protect national security (classified) information. It is our assumption that Federal insider threat programs would closely resemble those implemented in industry to protect trade secrets, intellectual property, or sensitive information. Both seek to deter, detect, and mitigate the exploitation, compromise, or other unauthorized disclosure of sensitive information. Many U.S. businesses are aware of such threats. The AFCEA Cyber Committee is interested in learning how these businesses are implementing the core elements of their insider threat programs. The objective of this paper is to identify the successful elements of insider threat programs established by U.S. businesses and to use this knowledge to advance information protection efforts for those businesses that are just become aware of the problem.

This paper on insider threat is intended to raise awareness of the risks, to highlight current issues surrounding insider threat, and to put forth continuing challenges to promote actionable results.

Approach

As a means of creating a greater understanding of the issue, the AFCEA Cyber Committee formed a subcommittee on Insider Threat. This subcommittee is composed of members with both public and private sector experience. To address awareness and progress in this area, the subcommittee invited a broad range of subject matter experts to discuss frankly how their companies are addressing the issue. The organizations participating in these interviews came from retail, financial, U.S. Government contractors, telecommunications, and manufacturing. In an effort to foster candid responses, none of those interviewees will be mentioned by name in this paper.

*The views or opinions presented in this paper are solely those of the authors and do not necessarily represent those of the organizations with which they may be affiliated. .

Trade Secret Theft Incident

The following incident reveals the extent of damage possible from theft of a trade secret as well as the millions of dollars lost to an American business. Although incidents like the one below are in the news, awareness of the increasing problem is just beginning to be recognized by a broader audience.

> "On January 2012, Wen Chyu Liu, aka David W. Liou, a former research scientist at Dow Chemical Company in Louisiana, was sentenced in the Middle District of Louisiana to 60 months in prison; two years supervised release, a $25,000 fine and was ordered to forfeit $600,000. Liu was convicted on Feb. 7, 2011 of one count of conspiracy to commit trade secret theft for stealing trade secrets from Dow and selling them to companies in China, and he was also convicted of one count of perjury. According to the evidence presented in court, Liu came to the United States from China for graduate work. He began working for Dow in 1965 and retired in 1992. While employed at DOW, Liu worked as a research scientist on various aspects of the development and manufacture of Dow elastomers, including Tyrin CPE. The evidence at trial established that Liu conspired with at least four current and former employees of Dow facilities in Plaquemine, Louisiana, and Stade, Germany, who had worked on Tyrin CPE production to misappropriate those trade secrets in an effort to develop and market CPE process design packages to Chinese companies. Liu traveled throughout China to market stolen information. In one instance, Liu bribed a then-employee at the Plaquemine facility for $50,000 in cash to provide Dow's process manual and other CPE-related information. The investigation was conducted by the FBI.
>
> *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, 2013*

Insider Threat Key Findings

The section summarizes the dominant issues discovered through the interview with U.S. industry representatives.

Corporate Organizational Structure

Most commercial organization had some form of insider threat deterrence, detection, and mitigation activity, some even formalized as programs. Virtually every organization had an identified a responsible individual for such activity, but sometimes without any subordinate structure or resources and sometimes as an additional duty. The placement of the insider threat program within the various corporate structures also varied widely. Some organizations treated their insider threat activity as a subsidiary component of the corporate security or the physical security organization. Others made it an aspect of their corporate Information Technology (IT) organization. Still others included it in human resources (HR) on in legal departments. Some treated their insider threat program as an independent corporate activity and a peer to their corporate activities including legal, chief information officer, HR, and finance. While specific

placement within the corporate structure may seem inconsequential, we believe it is critical for an organization's insider threat program to possess a separate identity at the corporate level. This separate identify provides the program with the independence required to perform the analytical work of detection.

We are concerned about organizations which treat insider threats as just another form of abuse to the corporate IT system and thus solely a technology problem for which the IT department is responsible. Such organizations are operating at unnecessary risk. The insider threat vulnerability involves the people, not the IT system storing the information they want to steal. While it is tempting to assign this effort to information technology staff, have them buy monitoring software, and have them monitor for abnormal activity as a component of their normal network operations, neither the people conducting the monitoring nor the technology may be adequate for this task. Similarly, to place the program solely within HR, legal, information assurance, or physical security does not pull together the appropriate skills required to mitigate the vulnerability. The threat is a corporate level issue that crosses functional areas and should be addressed as such.

The corporate information systems are the means, not the threat. We believe that most of the successful programs we reviewed were a combination of technology, legal, policy, physical security, awareness and training, plus counterintelligence resources where program personnel had a deep appreciation, if not a thorough understanding, of the role each of these disciplines contributes. We know that having "top-level management" support is a necessity for addressing insider threat problems. And we maintain that such support being visible through both word and deed is essential to the insider threat program success given the interdisciplinary approach required to comprehensively address insider threat issues.

It is perfectly reasonable, in our view, for an organization to perform a risk assessment to determine what corporate assets need to be protected. In fact, this is an essential part of the protection process if an organization finds itself in a legal situation and must defend its program protection policy and mechanisms. A risk assessment might also govern resources needed to be dedicated to the insider threat mitigation program. The costs of an insider threat program to deter, detect, and mitigate and are not inconsequential. If it is not practical to house the program at the corporate level, then we recommend that as an absolute minimum the program manager should have direct operational reporting responsibilities and ready access to top management, even if the resources are administratively subordinated elsewhere.

Doctrine, Principles, and Policy

During the course of our interviews, we looked for comparison and contrast between the policy development and the implementation of insider threat programs in industry to those found in the U.S. Federal government. Not surprisingly, with a long cultural history of having to develop, store, exchange, protect, and destroy classified national security information, we believe

corporations can and should learn much from the Federal government. Not everything in the national security area translates to a best commercial practice. But some things do. Simple steps such as analyzing what are critical data and information for an organization's reputation and competitive success is a foundation for an insider threat program. The information that is guarded with particular methods and tools need not be just the trade secrets but can also be computer configurations diagrams, salary details, and even organizational charts. Information of corporate value is dependent on the organization's risk assessment and the ability to direct the policy and program to protect it.

Effective insider threat policy development requires a corporate governance perspective over the information deemed as valuable. There are conflicting priorities between the need to protect data valuable to the corporation by restricting access and the need to share data within the corporation and with vendors, customers, and partners – some international, where the reach may not readily or easily extend. The "need to know" and "need to share" debate is an enduring one within government and is complicated by public debate and emotion, conflicting or ambiguous Federal legislation, and political factors. We recommend that this "need to" tension be thoughtfully examined at the corporate level so that individual data use policies have a consistent framework derived from common agreement. In our research we saw much individual interpretation applied to data protection/data sharing policies across large organizations. While there is nothing wrong with allocating these policy matters out to various operating functions, fundamental guidelines should exist with common definitions and wide promulgation so that, given identical situations, individuals throughout each corporation or operating unity would come to similar determinations on the need to protect and handle data.

One area that is particularly challenging is marking of data clearly as to the level of corporate sensitivity. Although we did see a few organizations with a marking policy, we believe having a common marking scheme, uniformly applied across all media, hardcopy, and softcopy, is essential to an effective insider threat program. How else are people to know precisely what to protect? To expect each individual, including customer, vendors, employees, consultants, partners, etc. to know the standard to which a given data set should be protected is both inefficient and unreasonable to implement practically. However, a common set of markings, included in common formats, both hard and soft copy, will serve as a training and awareness aid to help people remember what the corporation considers sensitive. Data marking also enables better detection of inadvertent disclosures via a compromise. The insider threat policy determinations and marking of sensitive data, particularly legacy data, may pose enormous challenges. But we consider both practices to be essential to an effective insider threat mitigation program. Over time, we believe each to be cost effective to the corporate bottom line.

Automation, Monitoring and Tools.

Most of the organizations interviewed indicated that they had established policies and strategies for implementing monitoring of the enterprise, specifically for insider threat. These policies or triggers might be as simple as alerting on large file transfers outside the enterprise or on unauthorized users accessing data repositories. These automated monitoring tools implement triggers that activate an alert for the insider threat program personnel to begin an inquiry. Ideally, the insider threat program staff consists of experienced counterintelligence (CI) professionals. The more mature programs reviewed had a combination of experienced CI individuals and security professionals performing this work. In most if not all cases, organizations implemented the standard practice of presenting a warning banner alerting users as to the ongoing monitoring for violations of policies and procedures.

One of the most common triggers implemented by automated tools is the monitoring of personal computer and network activity by employees who have given notice of resignation from the organization. Once notified of an individual's intent to leave the organization, some of the organizations interviewed indicated that they start monitoring email, file transfers, printer traffic, web accesses, and other activity starting 45-60 days before the final departure date. Organizations can use this approach to detect potential unauthorized removal of company information by a departing employee. Another approach mentioned by a global entity employed internal marking of company sensitive documents, which enabled them to limit access to information by workgroups of employees. It was also viewed as a useful mechanism to detect misuse of information. For the international organizations we spoke with, this approach also enabled better control of technical information that had export control restrictions.

Encryption was also mentioned as a preventative solution that makes theft of IP or insider threat more difficult to accomplish. This is a double-edged sword. It protects data in the networks from unauthorized users and secures email from prying eyes, but it also reduces the ability of monitoring systems to evaluate content of data in motion.

Many of the popular monitoring tools emerged from the finance community. These focus on protecting personal information, i.e., Social Security numbers, date of birth, and other personal identifiable information. These tools have limited use in protecting IP or detecting insider threat. Their use might potentially provide a false sense of security since they only address part of the challenge of detecting malicious activity. The consensus opinion by most of the respondents to our interviews indicated that many of them rely heavily on computer monitoring tools, but these are not enough. Global organizations have legal complications when implementing monitoring tools due to the differences in individual country's privacy laws. Organizations with rigorous protection programs do not depend solely on these tools. A professional security staff with CI training and experience is needed to be truly effective.

Counterintelligence Staff

Among those organizations we spoke with, an overwhelming majority believed the skills held by former U.S Government counterintelligence personnel were the most valuable part of the insider threat team core skills. As noted earlier, skilled staff members are in a better position to assess the contributions of technology, policy, legal, physical, and personnel security, awareness and training, and IT to the overall program than to assess any of those elements individually. This skill set consists of knowing how to conduct an inquiry of a potential incident, restricting the details of an inquiry to the smallest set of staff, using analysis skills to validate the facts, and knowing when to call law enforcement to elevate the incident to an investigation. U.S. Government counterintelligence personnel are also trained in foreign counterintelligence detection of collection threats and collection techniques, which provide incredible insight to organizations operating under economic espionage threat. This counterintelligence expertise is typically not found in industrial training programs. It is part of military or law enforcement training to pursue national security crimes such as espionage. The more successful programs tended to hire professionals from this career talent pool.

The *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* outlines "Voluntary Best Practices by Private Companies to Protect Trade Secrets" which include:

- Research and development compartmentalization;
- Information security policies;
- Physical security policies; and
- Human resource policies.

However, this list is silent as to a sufficient skill set to deter, detect, and mitigate potential incidents or crimes. With insider threat programs now developing in the commercial space to guard against economic espionage, counterintelligence training should likewise develop within industry. This represents another opportunity for government-industry collaboration. Effective counterintelligence personnel with background and inclination trained to think like counterintelligence officers are critical to an insider threat program's success.

Education and Awareness

The organizations we interviewed stressed the need for awareness as a first step. Sometimes there is a tendency to think only about the employee, but actually there are several layers of awareness required concerning the individual user. Who takes the interest in your company – the chief information officer (CIO) or the chief executive officer (CEO)? As one executive put it, this is "an A+ corporate level" issue. This executive believes that buy-in from the most senior levels in the company is essential. It is a leadership issue that requires the CEO's attention.

In addition to the CEO and CIO, a sound insider threat program also requires the attention of the Chief Operating Officer, Human Resources Officer, the head of counterintelligence (if there is one), and the Senior Legal Counsel. It is this team that must work together to put a realistic program in place and execute it. Step one, of course is to recognize the potential that exists for insider threat within your own organization. This is the dilemma for many savvy CIOs, as the have to sell it to the leadership. Educating the leadership and convincing them to spend money and time often requires the assistance of an outside firm or individual. Some of the leaders we interviewed stressed the importance of working with other industry partners and with federal agencies. Ultimately the CEO wants to understand the nature of the problem and also the return on investment. Sometimes organizations are also helped by their Board of Directors, who increasingly are becoming more aware of the problem and who want to understand from management how they are dealing with the risks.

Once leaders understand the potential that exists for insider threat, the natural next step is to know what to do about it. There is a tendency to think about tools that are available to ferret out malicious behavior, but in fact all of the interviewees stressed instead the importance of the human factor. The first step in ”planning awareness” is to identify key risks to the organization, critical assets, and the people who have access. One company said that education and awareness was his number one priority. Awareness and education is necessary for leaders, for those who are the "watchers," and for the employee. It starts when an employee walks in the door and in the first 72 hours receives training. Each employee signs a code of conduct annually as a refresher.

The purpose of education is to prevent, monitor, detect, and respond. All interviewees believe that the employee has a key role to play in all four of these elements. We encountered a wide range of approaches as to how organizations deal with training. A few had no training program that addressed insider threats. For those companies that did, their methods varied from externally provided training to internally conducted training. Some training was in a classroom setting; others used online training programs. While most organizations conducted annual training, one or two organizations used ongoing and sometimes unannounced training. The most aggressive program we encountered was a company that actually conducted "phishing" and other activities that required an employee to be on their toes all the time. Interviewees all stressed the need for positive, not punitive training. Some sought to protect and even reward employees who came forward.

It is important to note that some insider threat activity is not always a deliberate malicious act. A sound training program helps users understand how they can become an unwitting "threat" to the company, for example, by sending emails or briefings to their home computer in order to work from home. The employee thinks he is helping the company by working during downtime, when in fact his motives may be misconstrued. Another example is the spotty use of encryption. Not always cheap or easy to use, some employees choose to send unencrypted messages because "it's hard or takes too much time," not realizing the potentially

serious outcome of their action. Such inadvertent acts, although done with no malicious intent, exposes potentially sensitive information. Introducing this type of threat awareness to employees within an annual training program reduces corporate exposure.

Interviewees stated that the best program is one that is embraced by employees. How leaders communicate the importance of awareness and action is very important. Beyond prevention, the goal of education is to have employees recognize bad behavior and report it. Employees should be trained on what and how to report. They need to feel safe about reporting—that there will be anonymity and not retribution from either the company or from the reported employee. Some organizations have set up an Ethics Hotline; others have an office, person, and phone number where employees can go to report activity.

And, what about the "watchers?" These professionals need to be trained as well. Whether an organization chooses to get help from an outside firm or train internally, those who are monitoring employee traffic must be trained in how to optimally use monitoring tools and what to look for. Several of the interviewees stated that they have profiles of when an employee is at the greatest risk of stealing information or damaging the company through malicious activity. The most sophisticated insider threat Programs have tools that monitor employees during these periods of heightened risk. They have trained their people not just on the automated tools, but on the human factors associated with behavior.

Finally, who's watching the watchers? Monitors are high risk employees. They have access to critical company information and to employee communication. Not only do they need education, but leaders must be aware that the monitors themselves need to be watched. The most effective programs that we saw have counterintelligence staff. This person completes the awareness of company officers on threats, provides training, and often conducts investigations.

In summary, awareness and training is perhaps the most important tool in the toolkit. Interviewees stated that buy-in, through effective security and ethics training, coupled with signed acknowledgements, are cost effective and key to the success of a company's program.

Continuing Challenges

> *Detection of the malicious insider is one of the biggest challenges—Privacy and security are tradeoffs in this equation. Determining what is the acceptable balance remains an open question.*
>
> *Some organizations do not take legal action against an individual or competitor when sensitive information is stolen, preferring informal agreements rather than legal actions through the court. To what extent are we addressing the problem of trade secrets and intellectual property theft when a "gentlemen's" agreement instead of a more transparent court action is sought?*

Should the U.S. Government take a stronger role in protecting the private intellectual property of U. S. industry?

With regard to insider threat, is economic security equivalent to national security?

Summary

The theft of trade secrets, intellectual property and other types of sensitive information from U.S. organizations is becoming increasingly common in the headlines. The American public is becoming more aware of the economic and security impacts of these activities. Insider Threats are an important matter for AFCEA member companies and the economy at large. The intent of this paper was to discover how companies are addressing the insider threat: how the insider threat program is structured; where it resides in the organization; who has oversight authority; what are the tools and techniques deployed for detection and monitoring; and whether the sensitive information is marked and protected? We found varying levels of insider threat program maturity in these organizations, reliance on automated tools, many different approaches to the organizational components of the program and a variety of marking and protection policies. One of the more surprising results of the research is that education and awareness of the insider threat seemed to be a top priority of the organizations we interviewed. The second common element in successful programs was the employment of trained and experienced counterintelligence staff as a key part of their program.

Understandably, the implementation of a specific insider threat program needs to be tailored to each individual organizational situation.. Each organization must assess the risk that malicious or inadvertent behavior by insiders poses. These risks can be mitigated by organizations that plan an insider threat program that will include senior management, stand up a program incrementally, conduct a valuation of assets, recruit experience staff, select automated tools wisely, and continue to educate the staff on the consequences of insider threats.

Insider Threat Best Practices and Current Initiatives

Through the course of our research, we found much thoughtful and current work germane to the Insider Threat problem. We have included a number of useful references below:

1. U.S. Department of Defense, Defense Security Service. *Counterintelligence and Security Countermeasures*. www.dss.mil/isp/count_intell/count_n_sec_count_meas.html

2. Insider Threat Research. www.cert.org/insider_threat/

3. Joel Brenner. *America the Vulnerable Inside the New Threat Matrix of Digital Espionage, Crime and Warfare*. The Penguin Press, NY. 2011.

4. Office of Management and Budget. *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets.* February 2013.

5. The FBI – The Insider Threat. www.fbi/gov/about-us/investigate/counterintelligence/the-insider-threat

6. Insider Threat – Office of the National Counterintelligence Executive. www.ncix.gov/issues/ithreat/

7. Eric Chabrow. *Mitigating Insider Threat From the Cloud, Part 1: Relying on Provider to Keep Its Employees in Check*. www.bankinfosecurity.com/interviews/mitigating-insider0threat-from-cloud-i-1917

8. Dennis C. Blair and Jon M. Huntsman. *The IP Commission Report* The Commission on the Theft of American Intellectual Property. The National Bureau of Asian Research. May 2013. http://www.ipcommission.org/