Position Paper

Irene Schwarting, Panelist

Pacific Northwest National Laboratory

Irene.Schwarting@pnl.gov

ABSTRACT

The insider threat is considered by many security experts to be the biggest threat to corporate and national security today. Although the number of security incidents involving insiders is far smaller than that of incidents involving attempted intrusions from outsiders, the success rate of insiders is much higher, and the damage that they can cause is incalculably higher.

For purposes of this discussion, the insider threat is defined as any situation in which an individual takes advantage of information or access accorded to his/her position within an organization to betray the organization's trust. This is certainly not a new problem: it is one that has plagued organizations large and small for centuries. One of the earliest documented military strategists, Sun Tzu, wrote eloquently on the risk of trusted insiders betraying the mission, either by giving away information (espionage) or by destructive acts (sabotage). For the most part, the risk of espionage is far higher, because it is both easier, and less risky, than sabotage. As both are risks, though, from trusted insiders, we will address each in turn.

1 UNAUTHORIZED DISSEMINATION OF INFORMATION ACCOMPLISHED THROUGH INSIDER ACCESS: AKA, ESPIONAGE.

Espionage is normally defined on a national level: when an individual betrays national secrets to a competing nation, but the principles of insider betrayal are the same regardless of the scale of the organization or the activity.

Four preconditions are required for espionage (insider betrayal) to occur:[i]

- A motive or need to be satisfied through the crime.
- An ability to overcome natural inhibitions to criminal behavior, such as moral values, loyalty to employer or co-workers, or fear of being caught.
- An opportunity to commit the crime.
- A trigger that sets the betrayal in motion.

Traditionally, the MICE model is used to describe the four motives for committing espionage.[ii]

NSPW 2005 Lake Arrowhead CA USA

- **Money**: Some spies betray secrets in order to get paid for them. Aldrich Ames is one modern example of this motivation. This is probably the most common motivation in modern-day America.

- **Ideology**: Agents may be recruited by their ideological support for the recruiting nation. This is believed to have been the motivation behind Klaus Fuchs and the Rosenburgs. Although less common currently than it was during the heyday of Communism in the 50s, it is still a very effective motivator for individuals from certain cultures. Ana Montes, for instance, is believed to have been ideologically motivated to spy for Cuba.

- **Coercion**: On occasion agents may be recruited by blackmail or by overt threats, such as to their family or friends. This is a relatively uncommon motivation as it is less reliable than other motivators: the agents are more likely to be "doubled," i.e., recruited by the target organization, or the coercion factor may escape the recruiters' control. This is most effective in situations where family ties are very strong, or where certain cultural taboos can be exploited. Homosexuality was often used to coerce agents, although it is less effective currently than in decades past, at least, in the United States.

- **Ego**: In some cases the agents may be recruited through appeals to their egos. This works best in situations where the agent feels underappreciated or unrecognized for his contributions. The recruiter can appeal to the agent through flattery, crediting his contributions. Sexual recruitment often also appeals to the ego.[iii] Espionage as an act of spite, where the agent betrays insider information to get revenge or retaliation against the parent organization, is a relatively common subset of this category. Robert Hanssen, who is often described as the most dangerous spy in the history of the FBI, was recruited by appeals to his ego: he felt unappreciated by his employers and is said to have committed his espionage as a sort of retaliation.

Two types of opportunity are required for an insider threat to become realized:

- **Access** to information or material that can be sold or used to achieve some other goal.

- **Access** to persons expected to be willing to pay, or at least interested in having, such information or material.

Two further issues may influence the ability to overcome the cultural inhibitions to betrayal. One is the relatively faceless (and often, seemingly victimless) aspect of cyber espionage. There may be a perception that giving away digital information assets is not "really" bad, because of a subconscious distinction between "real" (i.e., paper) documents and digital documents. Secondarily, it may be easier to overcome the inhibitions against betraying trust by e-mail than it would be to deliver the documents in person to the outside entity. Some evidence indicates that people are more willing to communicate via an electronic medium than they would be in person, such as in e-mail or in "blogs." [iv] There is an extensive and rapidly growing literature on the similarities and differences between cyber social interactions and physical interactions; it remains to be determined whether this virtual freedom is related to psychologically easing betrayal.[v]

Regardless of the anonymity of the Internet, there have been no major shifts in the human psyche that would change the basic motivations for espionage. The one thing that has changed recently, and that most profoundly increases the insider threat, is that the opportunities have increased. Information stored electronically is far more transportable than information in paper copies. Through networked data systems, it has become far easier for insiders to find and access information of value that they would not otherwise be able to access. The wired world has also made it far easier to find and discreetly contact buyers for that information.

To reduce insider threat, we must approach it as an espionage problem, and treat it accordingly. We must identify those who may have the motivation to betray information, and minimize their opportunities to do so. Indicators of espionage risk are well known. They include, but are not limited to:

- Unexplained affluence
- Unreported or concealed travel or contacts outside of normal spheres, such as with adversary organizations
- Showing unusual interest in information outside the job scope.
- Keeping unusual work hours.
- Taking sensitive material home, onto a personal communication system, or otherwise external to normal business channels
- Attempting to gain new accesses without the need to know.
- Unexplained absences.

The more difficult challenge that must be addressed to reduce insider threat is to minimize the opportunities for betrayal. This is a challenge, for trusted insiders are the most difficult to monitor or restrict access. In a free society, there is a limit to the amount of restriction that can be put on employee communications. Restricting their access to the information of value, on the other hand, is more feasible.

Encryption, restricting information to those with "need to know," requiring authentication for access to sensitive information, limiting privileges and authorities, are all simple techniques that are already used to protect sensitive information in the physical world and that can be implemented in the cyber arena. More advanced techniques, such as digital watermarks, read-once files, and copy-proofing, also reduce opportunities for betrayal. Technological advances in information security should be considered in terms of their ability to protect sensitive information both from external, and internal, threats.[vi]

2 MALICIOUS AND DESTRUCTIVE ACTIVITY ACCOMPLISHED THROUGH INSIDER ACCESS: AKA, SABOTAGE

One very large concern in the software industry, which includes any business that uses or develops its own software, is malicious code insertion. Viruses, worms, are all generic types of malicious software, 'malware', that is deliberately designed to do something it should not. Most often, this malware is not actively destructive, it may do no more than leave open doors, providing access to systems that would be otherwise secured. This is no different than someone who jams open the door to the office as he leaves one evening, allowing burglars or industrial competitors free access to the facility. However, it is equally possible to introduce malware that has any number of destructive effects, including but not limited to; denying access to systems or networks, destroying or modifying data, physical damage of computer hardware, and even more catastrophic physical consequences. All of these actions are varieties of sabotage, and should be considered as such.

The motivations for sabotage are much the same as for espionage, the drivers are often the same. The risk, of course, is somewhat different: sabotage can result in direct (as opposed to indirect) economic costs, up to and including human injury or death.

It's not good. It's just not new

The risks of political, economic, and physical damage due to malicious code insertion, unauthorized access, and information exfiltration are indeed extremely significant. Economic losses are already calculated to be in the billions of dollars, and the political ramifications play out across the world media stage regularly. These threats must be taken seriously, and they must be interpreted in their global and historical context. The insider threat has influenced every significant political and corporate decision in human history, and the fact that in this age they play out in bits and bytes does not change their import. By understanding the insider threat in this greater context, and capitalizing on lessons learned from generations of counter-espionage experts, researchers and developers in the cyber arena can jump-start the process to defending their and preventing damage and loss.

3 REFERENCES

[1] Research on Mitigating the Insider Threat to Information Systems - #2: Proceedings of a Workshop Held August, 2000, Robert H. Anderson, Thomas Bozek, Tom Longstaff, Wayne Meitzler, Michael Skroch, Ken Van Wyk, CF-163-DARPA, 2000, http://www.rand.org/publications/CF/CF163/

[i] *Your role in combating the insider threat,* Office of the National Counterintelligence Executive, http://www.nacic.gov/archives/docs/Your_Role_in_Combating_the_Insider_Threat.pdf

[ii] *Espionage by the Numbers: A Statistical Overview* Richards J. Heuer, Jr. Defense Personnel Security Research Center Katherine Herbig TRW Systems , http://rf-web.tamu.edu/security/secguide/Treason/Numbers.htm

[iii] *Sexual Behavior Text 1*: http://www.dss.mil/nf/adr/sexbeh/sexT1.htm

[iv] *The Psychology of Cyberspace,* John Suler, Ph.D. Rider University http://www.rider.edu/~suler/psycyber/psycyber.html

[v] *How Real is Communication in the Virtual World of Cyberspace?* Rick Dietrich, Jill Grear, & Amber Ruth , http://www.units.muohio.edu/psybersite/cyberspace/cmcreal/index.shtml

[vi] *The Insider Threat To Information Systems* Eric D. Shaw, Ph.D., Keven G. Ruby, M.A. and Jerrold M. Post, M.D. Political Psychology Associates, Ltd. http://rf-web.tamu.edu/security/secguide/Treason/Infosys.htm#infosys