UNDERSTANDING THE INSIDER THREAT

For decades, the Federal government and US industry focused on external threats, but now that the Internet has connected the world, espionage and theft are largely anonymous and borderless activities. The government and its contractors now look inward and apply new technologies and counterintelligence strategies to detect and deter criminals, spies, or leakers in their midst. In response to publication of sensitive documents leaked by an Army intelligence analyst to the WikiLeaks website, President Obama issued Executive Order 13587 establishing a National Insider Threat Task Force and mandating that all Federal agencies that handle classified material institute insider threat programs.

- Designate a senior official to oversee classified information sharing and safeguarding, including support to the classified Information Sharing and Safeguarding Office and the Insider Threat Task Force.
- Implement an insider threat and detection program.
- Self-assess compliance with insider threat policies and standards.
- Support independent assessments of compliance with these same policies and standards.

Of the fifteen Cross-Agency Priority (CAP) Goals in the 2015 Federal Budget, Insider Threat and Security Clearance[1] stands out as one of the mission oriented goals. The goal statement for this CAP is to mitigate the inherent risks and vulnerabilities posed by personnel with trusted access to government information, facilities, systems, and other personnel[2]. The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program, intended to provide all Federal departments with real-time situational awareness of threat activity at the boundary and with the network.[3]

The creation of the National Counterintelligence and Security Center (NCSC) in December 2014 was another action taken by the government to address "the destructive growth and complexity of cyber threats, economic espionage, insider threats, and supply-chain threats"[4]. One area of NCSC focus is to counter the surreptitious electronic collection of personally identifiable information (PII) that could be used to identify, target, recruit, or coerce potential insiders in government in industry.[5]

The Federal government has clearly recognized the importance of devoting resources to detect and deter insider threats and has taken concrete steps to put needed programs in place. However, not just the government needs to worry about insider threats. Small businesses, think tanks, non-profits, Non-Governmental Organizations, and scientific organizations are just a few organizations at risk from insider threats. Understanding what constitutes an insider threat is the first step towards recognizing your vulnerabilities and taking corrective action.

Background

History is replete with examples of trusted individuals betraying secrets to outsiders. The WWII generation would cite the names of Burgess and Philby, Soviet spies in the heart of the British government. America in 1980s had Ames, Hanson, and Pitts, who also sold secrets to the Soviets. Each of them was a trusted person who, through years of covert

activity, was able to cause incalculable harm to the counties they ostensibly served…and their allies as well.

With the advent of the Internet, the concept of insider threat has taken on new dimensions. Malicious insiders no longer have to work their way into positions of trust to gain access to the most sensitive information. Nor do they face personal danger in obtaining and turning those secrets over to their handlers. Spy cameras and microdots have been replaced by USBs and global network connectivity.

Manning and Snowden are arguably the most recognized names associated with the modern insider threat. They were able to collect and disseminate significantly more information in much less time than a conventional insider could ever imagine. While this type of insider activity is well publicized, there is another category that is not as well known, but just as dangerous – the unintentional insider. They are well-intentioned people who create vulnerabilities that external actors can exploit. We never learn the names of individuals who compromise their employers' security by clicking on malicious links in social media or falling for a spoofed e-mail, but bet their actions could have the same impact as those of a willful malicious actor.

The explosion in consumer cloud applications such as Gmail and Dropbox makes it easy for insiders to extract vast amounts of data, usually undetected. A recent SpectorSoft Insider Threat Survey Report[6] found that 53 percent of enterprises surveyed discovered that employees were accessing consumer cloud services on company-issued computers to transfer corporate data. Another survey found that 20 percent of respondents used such services to intentionally share data with outsiders.[7] Combine these metrics with the Congressional testimony that nearly 60 percent of small businesses will close within six months of a cyber-attack[8], and it becomes clear that no organization is too small to ignore the insider threat.

About Insider Threats

Combating the insider threat is more than a technology issue. Unlike a hacker who has to gain intelligence about a target over time, the insider threat may have access to sensitive information on the first day on the job, and they go undetected because they happen behind the organization's defenses, which mainly focus externally. That is why firewalls, intrusion detection systems, and intrusion prevention systems do little to solve the insider problem. Defense against the insider threat involves a range of disciplines including operational security (OPSEC), counterintelligence, and behavioral analysis, in addition to technology, to detect and deter insiders.

Insiders have the advantage of knowing where the sensitive information is and how it is protected. They also know the policies and procedures intended to protect it. That gives them the time to plan how to exploit weaknesses in policy and technical defenses without attracting attention. While both intentional and unintentional insider threats create conditions where an external player can move or change data or inflict damage on the target's IT infrastructure, their motives and methods differ. The sections that follow explain how.

Unintentional Insider Threat

An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) uses harm or

substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.[9]

COMMON EXAMPLES OF UNINTENTIONAL INSIDER THREATS	
Lost or stolen laptop, USB, CD, hard drive, data tape, or cell phone	Providing access through social engineering (e.g., phishing[11] e-mail attack, planted or unauthorized USB drive) and carried out via malicious code[12] or spyware[13]
Accessing data/records without a legitimate need to know	Accidental disclosure (e.g., posted publicly on a website, mishandled, sent to the wrong party via e-mail, fax, mail)
Improper control and disposal of electronic devices and physical documents	Opening malicious files or links when instructed to by someone with an apparently legitimate reason
Providing sensitive information to a person posing as someone in authority	Failure to properly use or configure security controls
Misconfiguration of devices and equipment	Failure to apply timely software patches
Possessing access rights in excess of job requirements	Improper or accidental disposal of physical records
Unwarranted elevation of access rights	Failure to properly remove sensitive data before reassigning or decommissioning computers
Running unsupported software	Careless use of wireless networks (especially public)
Exposing sensitive files to unintended sharing on peer-to-peer (P2P) networks[10]	

The Intentional Insider

The intentional insider conducts reconnaissance from within, and access to information technology (IT) infrastructure provides many opportunities for malicious insiders. Due to the requirements of their jobs, programmers and system administrators usually have privileges to network assets that contain data for which they have no legitimate need. They may be able to disable or circumvent security measures and leave no trail of their actions, or they may create backdoors in critical systems that provide them access even after they leave the organization. These persons may also neglect to implement proper security controls to gain unwarranted access and avoid detection, such as test accounts or fictional user accounts.

Analysis of the CERT insider threat database of more than 700 cases revealed four classes of malicious insider activity[14]:

- IT Sabotage — Use of IT to direct specific harm at an organization or an individual.
- Theft of Intellectual Property (IP) — Use of IT to steal IP from the organization, including industrial espionage involving outsiders.
- Fraud — Use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain or theft of information that leads to an identity crime (e.g., identity theft, credit card fraud).
- Miscellaneous — Cases in which the activity was not for IP theft, fraud, or IT sabotage.

Detect and Deter the Threat

Both technical and non-technical means are required to address the insider threat. The insider is a person, and ideally, people are motivated to align with the best interests of their organization. Predicting an insider who will consciously decide to harm an organization is quite difficult with technology alone. Fortunately, there is a body of research on the behavioral aspects of what might motivate somebody to switch from being a loyal employee to someone working against the employer's interests. By feeding data from across the organization (Human Resources, Legal, Security, Lines of Business,

IT) into the appropriate algorithms, risk scores for these behaviors could be calculated for every employee. For example, the system could alert on an employee with access to sensitive information who just received a poor performance review or disciplinary action and is trying to download large amounts of data. A high risk score could trigger scrutiny by Security, such as real-time keystroke monitoring, to detect and act against a malicious insider at a very early stage. However, a thorough analysis of the impact on employee privacy must be conducted before such a program is contemplated.

Regardless of its size, purpose, or budget, any organization is at risk of an insider threat, but the application of best practices to address patterns and activities observed in hundreds of reported cases can minimize the impact.[15] These best practices should be embraced by every organization or business regardless of whether it has the resources or practical need to do so.

BEST PRACTICES FOR AVERTING INSIDER THREATS	
1. Consider threats from insiders and business partners in enterprise-wide risk assessments.	10. Institute stringent access controls and monitoring policies on privileged users.
2. Clearly document and consistently enforce policies and controls.	11. Institutionalize system change controls.
3. Incorporate insider threat awareness into periodic security training for all employees.	12. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	13. Monitor and control remote access from all endpoints, including mobile devices.
5. Anticipate and manage negative issues in the work environment.	14. Develop a comprehensive employee termination procedure.
6. Know your assets.	15. Implement secure backup and recovery processes.
7. Implement strict password and account management policies and practices.	16. Develop a formalized insider threat program.
8. Enforce separation of duties and least privilege.	17. Establish a baseline of normal network device behavior.
9. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	18. Be especially vigilant regarding social media.
	19. Close the doors to unauthorized data exfiltration

Guidance

Organizations that deny or ignore the insider threat do so at their own peril. There is a growing body of evidence that more and more sensitive information is being exposed externally by the intentional or unwitting actions of trusted individuals. Regardless of the actors' intent, the legal, reputational, and financial impact can be substantial, so an organization must take practical steps to minimize the likelihood and consequences of negative insider activity. We recommend the following measures:

Involve senior management, IT, human resources, legal counsel, security, and operations in the planning and implementation of your insider threat program. Indicators of negative insider activity can be observed by both coworkers and technical means. A successful program involves coordination of all departments so that information from across the organization can be pieced together to identify suspicious activity. The plan must balance the requirement to protect users' privacy with the ability to collect information to support a criminal prosecution.

Know your data and how to protect it. Do you know what your sensitive information is? Do you know where it is? Do you know who has access to it? If the answer to these questions is no, you have the perfect environment for an insider threat.

There are two principles to follow when determining who has access to what. First, 'need to know' dictates that people be granted access to only those subsets of available data that are required to carry out their duties. Second, the related concept of 'least privilege' states that users should have access to only those resources necessary to perform their job functions.

- Every organization should categorize your data by type and sensitivity and ensure that proper controls are in place based on this categorization. PII, medical information, personnel records, intellectual property, and financial data are common categories that have specific sets of required controls.
- Regular review of IT staff access rights is an important way to verify that least privilege is in effect.
- Organizations often focus on protecting electronic data and overlook securing physical representations of the same data. Designs copied from a whiteboard or strategic plans pilfered from a printer are just as valuable as electronic versions.
- A clean desk policy will ensure that physical documents are also properly controlled and secured.

Train your people. The more common type educates your staff on the impacts of spam, phishing, social engineering, social media, and the proper handling and destruction of sensitive data and equipment. This training should occur frequently and be reinforced in newsletters and other in-house communications. As you update your anti-virus on a daily basis to address new threats, you should also update your staff about the changes in their threat environment.

We are all familiar with the "If you see something, say something" campaign to involve the public in recognizing and reporting suspicious behavior. People tend to be reluctant to confront or report a fellow employee, but studies have documented that malicious insiders make statements or engage in activities that concern coworkers. Organizations should train their employees on how to handle these concerns appropriately.

- Establish a formal and confidential mechanism for employees to discuss their observations about suspicious activity.
- Work with legal counsel to develop protocols to investigate these activities and determine proper action, if any.
- Develop coordinated plans so that all departments can act quickly and in unison to minimize the impact of removing the malicious insider.

The process must assume innocence until proven otherwise and be structured so that it cannot be used to harass employees. In the event that initial stages warrant further investigation, the surveillance mechanisms must not violate the individual's privacy.

Review the program quarterly. Technological advances provide new opportunities for both the insiders and the teams seeking to thwart them. Scientific studies and analyses of actual events provide new insights into how insiders operate. You should review your insider threat programs to reflect these developments. It is a dynamic environment, and you cannot be successful in protecting your organization by fighting yesterday's battles.

[1] http://www.performance.gov/cap-goals-list

[2] http://www.performance.gov/node/3407/view?view=public#overview

[3] http://www.whitehouse.gov/blog/2014/10/03/taking-steps-improve-Federal-information-security

[4] http://www.wtop.com/807/3753574/New-intelligence-agency-established

[5] http://www.wtop.com/807/3753574/New-intelligence-agency-established

[6] http://downloads.spectorsoft.com/resources/infographic/spectorsoft-2014-insider-threat-survey.pdf

[7] SailPoint 2014 Market Pulse Report https://www.sailpoint.com/news/2014-market-pulse-survey

[8] http://smallbusiness.house.gov/uploadedfiles/3-21-13_chris_collins_opening_statement.pdf

[9] Unintentional Insider Threats: A Foundational Study. The CERT® Insider Threat Team, Software Engineering Institute, August 2013

[10] Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server. [http://searchnetworking.techtarget.com/definition/peer-to-peer]

[11] Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. [CNSS Instruction No. 4009, National Information Assurance (IA) Glossary, 26 April 2010, p. 54]

[12] Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [ibid p. 45]

[13] Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. [ibid p. 70]

[14] Common Sense Guide to Mitigating Insider Threats 4th Edition SEI December 2012 , pp. 4-5

[15] Common Sense Guide to Mitigating Insider Threats 4th Edition SEI December 2012 , p. xiv