Insider Threats in Law Enforcement

Based on the valuable information they have at their disposal, law enforcement agencies are among those that are prime targets for advanced attacks. While network protection can be extensive and sophisticated, the exploitation of insiders poses a serious threat for illegal access to these agencies.
Insider Threats in Law Enforcement

A SANS Whitepaper
Written by Dr. Eric Cole
August 2014

Sponsored by
Raytheon
As business functions continue to migrate to electronic forms, the means, methods and approaches adversaries use to break into systems constantly evolve. Even as companies continue to develop advanced tools, the ways in which attackers can target a system also increase (see Figure 1).

Typically, advanced adaptive attacks were reserved for an elite few. Although the exploits these elite attackers unleash can be devastating, their impact is somewhat controlled based on the small sample size of people capable of performing such attacks. However, now that more automated tools are being written, the potential entities that can launch attacks increases to an almost infinite level. As a result, attacks will continue to grow, increase in intensity and target valuable data stores.

One highly valued target that provides a rich source of information is law enforcement agencies. Many people think of law enforcement organizations as tracking down and arresting criminals, not being the target of the criminals. However, based on the valuable information such agencies have at their disposal, they are—and continue to be—a target of attack.

The fact that law enforcement agencies are the target of a range of attacks is not very surprising. So, law enforcement organizations have invested considerable resources into protecting their assets. The problem is that they have invested considerable effort and energy in building a robust, secure network to protect the servers within the environment. Although network protection is critical, because servers contain the information and networks provide access to that information, the network often is not the weakest link. Many adversaries have recognized that breaking into a well-configured and secure server is very difficult. Therefore, they are now targeting an operating system that is hard to control and impossible to patch. That operating system is the human operating system, and the human being, as the target, represents the insider threat.
Based on recent news stories, when many people think about threats to their organizations, they believe the biggest threat is an external threat. Foreign governments, competitors and organized crime groups are all prime examples of external threats that target and cause significant harm to organizations. While such attacks are damaging, it is important to differentiate between the source of the attack and the cause of damage. Even though the source of many attacks is external, the cause of damage, in most cases, especially when dealing with law enforcement organizations, is internal. Instead of trying to break into a server, an external adversary will perform extensive reconnaissance, send a well-crafted email with malicious content and target an insider. Because the insider believes that the attachment is legitimate, he or she will open it, infect the system and thus become the cause of damage. If the security staff ignores this distinction, they may not be addressing the real problem. The insider threat is the most damaging and highest impact component in any organization. Examples of the extent of that impact are shown in Figure 2.

Figure 2. The Impact Insider Threat Can Have on an Organization

An insider threat might be the only way an attacker can compromise the sensitive or classified information law enforcement agencies possess. This information is often protected by air gaps, isolation or other protection methods. These networks are very secure and locked down. The chance of an external adversary being able to access or directly break into a server that contains the sensitive information is very slim. Therefore, for an attacker to break into the network to monitor or access sensitive information, he or she would need to target and compromise an insider.

A perfect example is the case of Robert Hanssen. Hanssen was paid by Russian handlers in exchange for highly classified national security and counterintelligence information. In this case Hanssen used his position to access information and provide it to a foreign government. The source of the attack was external, but the cause of the compromise was an insider. The Russians knew their chance of directly breaking into the Federal Bureau of Investigation (FBI) directly was slim. However, compromising an insider made the attack feasible.

For many organizations that deal with sensitive information, for example those in law enforcement, an insider is going to be the prime target for an external adversary.

1 Information provided by the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering
2 [www.fbi.gov/about-us/history/famous-cases/robert-hanssen](http://www.fbi.gov/about-us/history/famous-cases/robert-hanssen)
Types of Insider Threats

When people hear the words *insider threat*, they conjure up images of Aldrich Ames from the Central Intelligence Agency (CIA), Robert Hanssen (FBI) and Edward Snowden (National Security Agency)—people who maliciously and deliberately used their access to cause harm. While the deliberate or malicious insider is always a concern, the bigger concern for law enforcement agencies is the *accidental insider*—the person who is targeted and manipulated to cause harm without realizing the true intent of their actions. It is far easier for an adversary to target and trick an internal person than it is to break into a server.

As an attack evolves, targeting the accidental insider is a natural progression. Adversaries are always going to exploit the weakest vulnerability. As organizations address and fix one area of their environment, this will naturally create a new weakness. In the beginning, the weakness for law enforcement agencies was in the security of networks and servers. Because the weak protections continued to be targeted, agencies increasingly focused their efforts on fixing and securing this weakest link.

Over the years, as the agencies continued to build robust, secure, defensible networks—including air gaps and isolation—adversaries needed to find new areas to compromise. That point of compromise became targeting an insider and manipulating that individual to provide a point of access to the network.

---

3 www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames
4 www.nextgov.com/defense/2014/03/snowdens-security-breach-could-cost-us-billions-top-general-says/80044
Solution for Addressing Insider Threats

Based on the information that law enforcement agencies have access to and the type of work they perform, there is a high probability that they are going to be targeted. Therefore, it is critical that organizations address this issue proactively. The fundamental components of addressing insider threat need to be based on a mixture of preventive and detective measures. Typically, many organizations address security by looking only at preventive measures, believing they can prevent all attacks. With the current level of sophistication of adversaries, organizations—including law enforcement agencies—need to accept a fundamental fact: Organizations are compromised and will continue to be compromised.

So, prevention is ideal, but detection is a must. Organizations do need to try to prevent and stop the attacks from occurring. But they must recognize that, in many cases, especially when dealing with a persistent adversary, the adversary is going to get in.

In some cases, prevention techniques merely slow down an adversary and postpone the inevitable. Being able to detect an adversary in a timely manner is often a more effective way of controlling and managing the intrusion.

As illustrated in Figure 3, any insider threat program, especially one dealing with a law enforcement agency, must have a mixture of policies, processes and technologies to provide the necessary balance of prevention and detection.

The core components of any program are ensuring that risk is properly addressed and that security efforts are focused on the correct areas. Security efforts need to be focused on reducing the risk of disclosure, alteration or destruction of an organization's critical assets. As any organization builds its insider threat program, it must validate program elements against these risks. This can be done by asking the following questions:

1. What is the risk this measure is targeting?
2. Is it the highest priority risk we currently have?
3. Is the solution the most cost-effective way of reducing the risk?

The answers to these three questions will help guide the program to ensure it is addressing the correct items.
To answer these questions, the security staff needs to understand its environment and gather the correct information. A worksheet for personnel to use to gather this information contains a column for assets, threats and vulnerabilities.

In the first column, the analyst lists the organization’s critical assets and the business processes that support them. The second column provides space to list the threats that have the highest likelihood of causing harm to the critical assets. The third column allows the analyst to list the vulnerabilities that would cause the biggest impact based on the threats to the critical information.

When the analyst completes this worksheet, the final column contains the highest priority vulnerabilities that need to be addressed to reduce the risk to an appropriate level. Many organizations are tempted to increase budgets and throw money at the problem to reduce risk. Although resources are often needed, spending money does not ensure security—especially if it is not focused in the correct areas.

Although risk needs to drive the implementation of an insider threat program for law enforcement agencies, organizations also need to take the following key steps:

1. Determine access
2. Profile user behavior
3. Control administrator access
4. Raise awareness
5. Monitor activity

These steps will allow law enforcement agencies to be able to prevent the low-grade threats from occurring and provide a comprehensive way to detect advanced persistent threats in a timely manner.
Determine Access

It is critical to clearly articulate what a person’s job requirements are and what access he or she needs to perform that job. In many cases, when someone’s account is compromised, information that an adversary steals is not the information the person needed to perform his or her job function. Therefore, by limiting access to what each employee requires access to, the amount of damage caused by an adversary can be greatly reduced.

Figure 4 reflects a compilation of 12 access incidents in which the users had far more access than they needed; the rest was gravy for the adversary. The entire box represents all of the access the user was granted.

In those 12 incidents, only 14 percent of the information that was targeted and stolen by an adversary was needed by the owner of the compromised account. If organizations better control and limit access, the amount of damage caused by the adversary could be reduced by 86 percent. If the involved organizations had given personnel only the access they needed to do their job, when their accounts were compromised, the amount of data that would have been stolen and the resulting damage would have been greatly reduced.
In controlling access, organizations need to take a four-prong approach:

- Least privilege
- Need to know
- Separation of duties
- Rotation of duties

The focus of this comprehensive approach is not only to stop an adversary, but also to slow the attacker down and give the organization more time to detect compromise in a timely manner.

Individuals should be given the least amount of access they need to perform their jobs—least privilege. Some believe conventional wisdom says that it is better to give more access than less if you are not sure what people need access to. Such an approach will always allow workers to access any information they need. Conventional wisdom, however, does not work when it comes to security. Giving someone unneeded access just makes it easier for the adversary and increases the amount of damage that can be caused by a successful attack.

If an organization is not sure whether someone needs access, it is actually better to give them less access and have them request the additional access than to make it easy for the adversary to cause harm. The need to know policy builds on the premise of least privilege and only gives someone access to particular information when that individual needs it.

For example, officers might need access to a database to perform their job. However, they do not need the access 24/7/365. They need the access only when they are working their shift. Need to know would only allow them access during their shift. In a seven-day week there are 168 hours. Of those hours, an average person typically works 40–50 hours. By enforcing need to know, the organization could cut down on the window of opportunity for an adversary by more than a third. It is also important to remember that many attackers break into accounts after hours and are betting on the fact that the organization is not properly implementing need to know access.

Least privilege and need to know focus on providing access only to the information individuals need—when they need it. However, often the minimal access needed still represents too great a risk. In such situations an organization needs to divide the access among multiple people by implementing separation of duties. Separation of duties requires two or more people to coordinate to perform a job function, making it more difficult for an adversary to cause harm. Compromising one account is achievable—compromising two accounts is significantly more difficult.
Separation of duties is an effective way to make it harder for an adversary, but if an adversary does compromise multiple accounts, he or she would have long-term access. Therefore, to control the window of opportunity that an adversary would have, rotation of duties needs to be layered on top of separation of duties. Rotation of duties requires someone to work with different entities at set intervals to minimize the exposure. For example, consider the situation in which every four weeks the two people who work together change. If an adversary does compromise both accounts, access is available only for a limited period of time.

Finally, when it comes to controlling access to information, expiration dates need to be established for the access. Many organizations give individuals more access as their tenure at the organization progresses. They never remove the access. It is important that all access expires after a certain time to control the overall access available to any one individual. Automated tools can ensure this process and check to make sure that policies are in place on every workstation.

**Baseline User Behavior**

There are significant differences in behavior between a normal user and an adversary. By carefully monitoring user activity and building proper profiles, an organization can detect a compromised account and control the damage. Use the following three variables to monitor an account profile:

- Amount of data accessed
- Failed access attempts
- Data copied or sent to external sources

When an account gets compromised, there are significant differences in the data access patterns of a normal user and one that has been compromised. For example, a normal user typically accesses 40–50 files and would have only a handful of failed access attempts. Once the account is compromised, an adversary is going to use that account as a pivot point from which to perform internal reconnaissance. When this occurs, the attacker accesses tens of thousands of files, and the number of failed attempts increases to several thousand. By carefully monitoring access patterns, compromised accounts can be detected very quickly.

In addition, users are creatures of habit, and their behavior is predictable. Careful examination of those behavioral patterns and looking for anomalies can provide early indicators of a compromise.
**Control Administrator Access**

One reason attacks are so devastating is that compromised accounts are often logged in with administrator privileges. The general rule of thumb is if someone is logged in or running a program as administrator, they cannot access any resources from the Internet or have Internet access. Two of the most dangerous activities someone can perform are checking email or surfing the web as administrator. This creates an easy opportunity for an adversary to target a user and get full access to the system.

To control administrator access and make sure that someone logged in as administrator cannot access the Internet, an organization should take the following steps:

1. Always force a user to log in as a normal user. All operating systems can be configured to allow only normal user accounts to login and never allow someone with admin privileges to log directly into the system.

2. Configure any application that needs to run with administrator privileges to either “Run as Administrator” or `sudo` to the appropriate access that is needed.

3. Log and carefully review all privileged access.

4. If an employee needs a system where they have to log in directly as administrator, give that employee a separate system for any access he or she may need to the Internet.

**Raise Awareness**

As mentioned previously, one of the main aspects of compromise for law enforcement organizations is the accidental insider—someone who is tricked or manipulated into doing something they normally would not do if they knew the true intent of the actions. To help decrease this threat vector, making users aware of the threats and the types of attacks that are possible helps increase the overall security.

It is important to note that awareness is part of the solution, not the entire solution. For some advanced attacks, a user’s normal communication and the attacker’s communication look identical, so awareness would not be effective against such attacks. However, if providing users more awareness that they might be targeted and about the way that targeting occurs reduces the number of compromises by 15 percent or so—that is money well spent.

---

5 [www.nsa.gov/ia/_files/factsheets/Final_49635NonInternetsheet91.pdf](www.nsa.gov/ia/_files/factsheets/Final_49635NonInternetsheet91.pdf)
To increase the awareness, it needs to be tied to the biggest problem areas within an organization. Therefore it is important to remember that policy is part of a triad: policy, training and awareness, as illustrated in Figure 5.

![Policy → Tells you what to do](image)

![Training → Provides the skills for doing it](image)

![Awareness → Changes one’s behavior](image)

*Figure 5. The Security Triad*

While general awareness has some value, it is more effective if it is tied to the areas in the policy that users are not following. Every policy statement needs to be specific and measurable to drive the awareness training. An organization should determine the effectiveness of each policy statement on a regular basis. Any policy statement that employees are not following should be verified to ensure employees have the correct skills to perform that particular activity. If they do, then awareness needs to be improved so the users understand why it is important and change their behavior to follow the policy. Organizations often just push out policies without training and awareness. In such cases, the overall effectiveness is reduced.

While awareness is important, removing the vector of attack is even more effective at reducing insider threat. An organization needs to differentiate between required functionality and optional functionality. Optional functionality needs to be blocked or removed. In terms of stopping most cases where an accidental insider is targeted to become an insider threat, blocking traffic from untrusted networks (such as the Internet) is critical. The typical avenues of attack that need to be blocked include the following:

- EXE attachments
- Macros embedded in Office documents
- Active scripting
- HTML-embedded content

Establishing policies in which users are provided proper training and awareness of the dangers of those avenues, tied with proper blocking of access, can help to protect an organization against the accidental insider threat. Automation techniques can provide another layer of defense.
Monitor Activity

The final component to control and manage insider threats is monitoring key activities and looking for anomalies that could be indicative of an attack. Outbound traffic patterns are a valuable data source to monitor. When an account is compromised, the type and frequency of traffic going to the Internet changes drastically. The following are the areas to monitor for outbound traffic and look for signs of a compromised system:

- Number of connections
- Length of the connections
- Amount of data
- Percent of encrypted traffic
- Destination IP address

The insider threat ultimately allows an adversary to access and control an environment. In many cases, because an accidental insider is being targeted, he or she is not even aware of the compromise. There are often no visible indicators of an attack, but there are often observable technical changes, such as the amount of data or type of data the accidental insider is accessing. Host-based forensics that focus on the hard drive are often performed only after an organization knows it has been compromised. Because today’s insider attacks are stealthy, targeted and data focused, everything looks normal from a computer operations perspective. However, network-based forensics can be very valuable for early detection because they provide a visible sign of compromise—if security personnel are looking in the correct areas. But even network-based forensics will miss activities performed at the endpoint, which is why endpoint, host-based monitoring is necessary to truly mitigate the insider threat.

When a system is compromised, one of the key things an adversary does is set up a command and control (C2) channel to allow covert communication back to the host. When this channel is functional, it drastically changes the normal network patterns of activity leaving a computer. If a proper profile of the system is built, personnel would be able to notice a distinct change in the number of connections, length of connection time and other characteristics that indicate a system has been compromised. Deviation from the control profile provides timely detection of potential insider adversaries, who can compromise a system.

Even if a proper profile does not exist, the five indicators of compromise can also be valuable. Organizations can create five independent lists showing the top 20 IP addresses for outbound traffic in each of those five areas. Then, they can see which IP addresses appear on all five lists. Any system that is on all five lists is highly indicative of a compromised system. Although all five items are powerful indicators, the percent of encrypted traffic and the destination IP addresses require tuning to remove false positives. As a result, to simplify the initial implementation, start with the first three variables: number of connections, length of connections and amount of data.
Conclusion

The insider threat in law enforcement organizations is a significant risk because of the confidential information law enforcement personnel can access. Directly breaking into systems is quite difficult because most law enforcement organizations have spent considerable resources building robust perimeters and securing their systems. Because breaching a system is difficult, an advanced adversary is going to rely on the simplest and most effective method of compromise: the insider.

Attacks targeting the accidental insider are a prime source of compromise because the insider has the means, method and access to the information that an adversary desires. In many instances attacks cannot be prevented, so timely detection is essential. To properly protect the critical information that law enforcement agencies have at their disposal, it is critical that they continue to invest considerable effort in detecting, controlling and managing the risks that can come from the insider threat. Several guidelines and tools have been provided to help organizations get started. The bottom line is: Law enforcement agencies are going to be targeted and, in many cases, are already compromised. The sooner organizations can monitor and control the insider threat, the better their overall security.
Dr. Eric Cole, SANS fellow and instructor, is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master’s degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and chief scientist for Lockheed Martin. Dr. Cole is the author of several books, including Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible, 2nd Edition, and Insider Threat. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting, where he provides leading-edge cybersecurity consulting services and expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole was the lone inductee into the InfoSec European Hall of Fame in 2014. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty fellow and course author who works with students, teaches, and develops and maintains courseware.

SANS would like to thank this paper’s sponsor:

Raytheon
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FL</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NIH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>Online TXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>