Combating the Insider Threat
Protecting Your Network from Advanced Attacks
“It’s not about the 98% you catch, it’s about the 2% you miss.”
– NSS Labs: Analyst Brief
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter One</th>
<th>4</th>
<th>WHO IS ATTACKING YOUR NETWORK?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter Two</td>
<td>10</td>
<td>INSIDER THREAT MOTIVES AND METHODS</td>
</tr>
<tr>
<td>Chapter Three</td>
<td>17</td>
<td>DETERRING INSIDER THREATS WITH TECHNOLOGY</td>
</tr>
<tr>
<td>Chapter Four</td>
<td>22</td>
<td>USING NETWORK LOGS TO THWART INSIDER THREATS</td>
</tr>
<tr>
<td>Chapter Five</td>
<td>30</td>
<td>BEYOND TECHNOLOGY</td>
</tr>
<tr>
<td>Chapter Six</td>
<td>37</td>
<td>SUMMARY &amp; TOP 10 WAYS TO COMBAT INSIDER THREATS</td>
</tr>
</tbody>
</table>
CHAPTER ONE

Who is attacking your network?
Many organizations today are drowning in fears and concerns surrounding sophisticated cyber-attacks such as Advanced Persistent Threats (APTs), DDoS, ransomware and zero-day exploits. While this constant onslaught of attacks can be difficult to keep up with, businesses and government organizations also need to be mindful of perhaps the most alarming type of attack out there – the insider threat.

According to a report by Forrester Research, insiders are the top source of data breaches, with 36 percent of breaches stemming from the inadvertent misuse of data by employees. Additionally, 25 percent of respondents in the Forrester report said that abuse by a malicious insider was the most common way in which a breach occurred over the course of one year.
“The inadvertent misuse of data by insiders was responsible for 36% of breaches in 2013. Abuse by malicious insiders made up 25%.”

– Forrester Research, Understand the State of Data Security and Privacy
What does insider threat mean?

While the insider threat can take on several different forms, the main component is that the attack is initiated from inside your network versus outside where most security technologies are focused. The insider attacker is already on your network, so traditional defenses such as firewalls, antivirus and IDS/IPS will not be able to detect his or her actions. According to a recent survey by SpectorSoft, 61 percent of IT professionals said they could not deter insider attacks, and 59 percent said they were unable to even detect one.

So who is attacking your network? There are three main types of insider threats:

- **Negligent Insiders** – Insiders who accidentally expose data – such as an employee who forgets their laptop on an airplane
- **Malicious Insiders** – Insiders who intentionally steal data or destroy systems – such as a disgruntled employee who deletes some records on his last day of work
- **Compromised Insiders** – Insiders whose access credentials and/or computer have been compromised by an outside attacker

Each of these types of insider attackers has his/her own motives, methods and means of being thwarted. In order to develop an effective insider threat management program, it is critical to understand each type.
Various Business and IT Trends Have Increased the Likelihood of Insider Attacks for Today's Enterprises

**Bring Your Own Device (BYOD)**
Now that it has become commonplace for employees to bring smartphones and laptops/tablets in and out of the office, using them for both work and pleasure, opportunities for said employees to steal sensitive data are greater. As a result of BYOD, the likelihood of employees having their devices, and therefore corporate data, stolen by malicious outsiders has also risen.

**More Open Networks**
In today’s fast-paced business environment, the use of outsourcing, contractors, third-party technology platforms and cloud computing has exploded as a means of fostering greater business agility. However, this dramatically opens up our corporate networks and sensitive data to countless other parties who may not be as trustworthy or careful with our information as we would expect.

**Social Engineering**
In an era of APTs, today’s attackers know that the best way to infiltrate an organization without getting caught is through its trusted insiders. Crafty and patient attackers are creating designer attacks for specific organizations and individuals, and they do not mind taking the time to trick or bribe employees into divulging the confidential details they need to carry out their attacks.

In fact, according to a report by Mandiant, 100 percent of the attacks it investigated used stolen credentials, while only 54 percent of the compromised machines it investigated contained malware. Through a new type of attack known as muleware, attackers are now even paying end users to help them with their attacks.
What is muleware?

Unlike malware, muleware solicits the participation of the user and offers incentives to play a small role in the attack campaign. "Up until this point, cybercriminals have attained their resources by exploiting and compromising devices," said Lancope CTO, TK Keanini. "But wouldn’t it be more efficient and much more profitable to pay for these resources and turn thousands of would-be victims into part of the attacker’s supply chain? I envision that this new form of muleware will be based on the anonymity of Tor networking, and commerce conducted via cryptocurrency such as Bitcoin. Marketplaces will connect the demand with the supply, and cybercrime will rise to an entirely new level, a level that we are not prepared to defend against."
CHAPTER TWO

Insider Threat
Motives & Methods
Negligent Insiders

Negligent insiders are insiders who accidentally expose data. They don’t mean to do anything wrong – they are just employees who have access to sensitive data and inadvertently lose control of it. A large number of security incidents and data breaches fit this description.

Also fitting into this category are insiders who take IT shortcuts or ignore security policies simply to make their jobs easier – for example, downloading unauthorized software, using unsecured wireless networks, or the developer who decides to set up a test site on the Internet with real data.

Malicious Insiders

Malicious insiders are employees who intentionally set out to harm the organization either by stealing data or damaging systems.
“Only 3% of U.S. organizations feel safe from insider attacks.”
– ESG, The Ominous State of Insider Threats
Research by the CERT Insider Threat Center at Carnegie Mellon University surrounding hundreds of real-world cases of attack by malicious insiders has shown that most incidents fit into one of three categories:

- **IT Sabotage** - Someone destroys data or systems on the network
- **Fraud** - Someone is stealing confidential data from the network for financial gain
- **Theft of Intellectual Property** - Someone is stealing intellectual property for competitive advantage or business gain

**Motivations for Betrayal**

The motivations that turn insiders against their organizations are diverse, and can include:

**Job/Career Dissatisfaction**
When someone is extremely dissatisfied with their current work or career situation, they may attempt to harm their employer by destroying or stealing data.

**Monetary Gain**
When exposed to valuable data that could make them money on the black market, some employees will be unable to resist the temptation to steal and sell it. Others will be coerced to do so by malicious outsiders.
Espionage
Both nations and corporations have been known to plant insiders within organizations for the sole purpose of stealing trade secrets and intellectual property for espionage.

Activism
Activists are associated with a particular ideological movement, and can use the theft and exposure of confidential data to bring attention to their cause. The cases of Bradley Manning and Edward Snowden likely fall into this realm.

Compromised Insiders
A compromised insider is an employee whose access credentials or computer have been compromised by an outside attacker. According to the Cisco 2014 Annual Security Report, “Threats designed to take advantage of users’ trust in systems, applications, and the people and businesses they know are now permanent fixtures in the cyber world.” And according to the Verizon 2014 Data Breach Investigations Report, two out of three breaches exploit weak or stolen passwords.

A compromised insider is really an outsider – it is someone who has access to your network as an authorized user, but they aren’t who they are supposed to be. Today’s attackers are frequently employing social engineering tactics to infiltrate corporate networks and execute attacks under the radar, posing as legitimate users.
“Two out of three breaches exploit weak or stolen passwords.”
- Verizon, 2014 Data Breach Investigations Report
Lessons Learned From Manning and Snowden

Security breaches surrounding Bradley Manning and WikiLeaks, as well as Edward Snowden and the NSA, have made it painfully obvious that even the most seemingly impenetrable networks can fall victim to insider threats. If nothing else, these two major incidents have finally brought the issue of the insider threat to the foreground for many businesses.

However, it is important to realize that for every Snowden or Manning out there looking to expose confidential secrets in the name of hacktivism, there are literally hundreds of others planning to steal data from their employer’s network simply for revenge or to make a buck.

It is not enough to think, “Well, our company isn’t doing anything wrong, so we don’t have to worry about insiders exposing our data,” or “We are just a small company so no one is after our information.” The truth is, any company’s data can be valuable when put in the right hands – whether it’s PII, credit card data, medical records or even just intellectual property – and you better believe that the attackers know this!
CHAPTER THREE

Deterring Insider Threats with Technology
Thankfully there are technologies that can help organizations deter or thwart insider threats. Here’s a look at which types of technologies are effective against each kind of insider threat.

**Negligent Insiders**

Various measures can be used to deter negligent activity and "keep honest people honest."

**Access Controls**
Access controls can prevent people from obtaining sensitive data that they do not need in order to do their jobs. According to a December 2014 report by the Ponemon Institute, seventy-one percent of end users say that they have access to company data they should not be able to see.

**Encryption of Data at Rest**
Encryption of data at rest can also help prevent data loss by negligent insiders in the event that they lose their laptops or other equipment.
“Almost 95% of all cybercrime is triggered by a user clicking on a malicious link disguised as a good one.”

- Intel, #ClickSmart campaign


Malicious Insiders

Access Controls
Access controls can also help prevent damage done by malicious insiders. Making it harder to access sensitive data can keep honest people honest, but also put a wrench in the plans of malicious attackers.

Checks and Balances
Checks and balances are also extremely important in this arena. There should never be just one individual who has administrative access to a system, as this could essentially leave the person free to do whatever they want with the data or device – or even hold it hostage after leaving the company. Shared usernames/passwords should also be avoided as they do not hold the individual users accountable, and could still be used by people who have since left the organization.

Logs from Endpoint Systems and Network Devices
Logs from endpoint systems and network devices can also be used to identify and investigate cases of insider malice. For example, a case of financial fraud might be detected by examining database logs from a credit card processing system, whereas a case of data theft might be noticed through monitoring of network traffic.

Compromised Insiders
Compromised insiders are a much more challenging type of insider threat to combat since the real attacker is on the outside, with a much lower risk of being identified. Typically, no amount of deterrence will discourage them from carrying out their attack. Furthermore, traditional security solutions that focus on catching malware and exploits cannot identify the unauthorized use of legitimate accounts. In fact, studies have shown that advanced attackers are on the network for a median of 243 days before being detected. The use of network logs is really the only way to uncover and shut down this type of threat.
“Only 9% of European organizations feel safe from insider attacks, and more than a quarter feel vulnerable.”

CHAPTER FOUR

Using Network Logs to Thwart Insider Threats
While each type of insider threat requires a different combination of security measures, one technique that can help across the board is the monitoring of network activity through various logs. According to Lancope CTO TK Keanini, “In all cases of insider threat, early detection of the activities should be the dominant strategy because no one, no matter how diligent, is going to be able to prevent these threats 100% of the time.”

In order to effectively combat threats, organizations need a way to find out the **who, what, when, where, why and how** of specific attacks. By leveraging network activity logs from technologies such as firewalls, IPS systems, SIEMs, packet capture and NetFlow, organizations can **turn the entire network into a security sensor** and more easily be aware of and shut down insider attack attempts.

All of these technologies have their strengths and weaknesses in terms of expense, level of network visibility provided, and privacy concerns, but should all be evaluated as part of an effective insider security strategy.
“In all cases of insider threat, early detection of the activities should be the dominant strategy because no one, no matter how diligent, is going to be able to prevent these threats 100% of the time.”

– TK Keanini, CTO, Lancope
NetFlow for Combating Insider Threats

By collecting and analyzing metadata from throughout the entire network, NetFlow in particular provides a wide breadth of visibility at a reasonable cost and without the privacy concerns associated with full packet capture.

NetFlow is a protocol developed by Cisco that enables organizations to collect and analyze network traffic from existing infrastructure components including routers, switches, firewalls and others. Because it allows for the collection of network data from virtually anywhere in the network, NetFlow is an extremely valuable technology when it comes to finding and identifying insider threat actors.

Providing a 24/7 pervasive look at everything happening on a corporate network, NetFlow can be leveraged for both real-time threat detection, as well as to create a network audit trail of previous transactions for use in forensic investigations. Since it delivers visibility across the entire network environment, NetFlow can help organizations identify network activity associated with a wide range of cyber-attacks, such as unusually large file transfers or attempts to access restricted areas, for example.

In the case of the insider threat, excessive amounts of network traffic flowing from one user’s computer to the printer could signify an attempted theft of intellectual property. Or, if a user is frequently communicating with an unfamiliar IP address in another country, it could indicate that the user’s computer has been compromised. These are just a couple of examples of how the collection and analysis of NetFlow can help identify insider threats on the network.

NetFlow is also valuable for baselining network assets so that administrators know where the organization’s sensitive data assets reside and how they are being used. After all, IT and security professionals cannot take the appropriate steps to secure critical assets and minimize risk if they do not know that the assets exist, or where they are located.
Detecting Suspicious Network Behaviors

According to TK Keanini, CTO of Lancope, “There is a difference between 'bad' and 'not good.' The insider threat requires you to have tools that can detect 'not good.'” Collecting and analyzing NetFlow data with the right tools can help organizations detect a plethora of suspicious network behaviors that can indicate that an insider attack is taking place. These include:

**Unauthorized Access**
When a user attempts to access resources on the network that are prohibited

**Policy Violations**
When employees begin using services that are in direct violation of company policy, and may be intended to bypass company monitoring

**Internal Reconnaissance**
Before insiders can extract data, they must first inventory it. Organizations can use NetFlow to identify associated internal scanning activities.

**Suspect Data Loss**
When privileged users send abnormal amounts of information out of the network

**Suspect Data Hoarding**
When a user is downloading and collecting a large amount of data, which may indicate an attempt to package and exfiltrate sensitive information
Target Data Hoarding
When large amounts of data are being extracted from a specific host on the network

Detecting these behaviors early on can mean the difference between thwarting a potentially catastrophic insider attack and becoming the victim of one. If you have the appropriate situational awareness and can identify anomalous network activity in a timely fashion, you may just be able to shut down an attack before a privileged user makes off with your data. Unfortunately, however, it still takes more than just technology to adequately protect your business from insider threats.
“There is a difference between ‘bad’ and ‘not good.’ The insider threat requires you to have tools that can detect ‘not good.’”

– TK Keanini, CTO, Lancope
Gaining Security Context with Lancope’s StealthWatch® System

While NetFlow provides a plethora of valuable information for combating network attacks, organizations need a feasible means of collecting, storing and analyzing all of the data to turn it into actionable intelligence for fending off advanced threats. With massive scalability and sophisticated security analytics, Lancope’s StealthWatch® System enables organizations to make sense of all the information available on their networks, as well as quickly act on it.

By collecting and analyzing mass quantities of NetFlow and other types of data from across an organization’s entire network, the StealthWatch System can quickly identify anomalous behaviors that could be indicative of an attack. The system can also store months or even years’ worth of NetFlow to facilitate more comprehensive forensic investigations into previous security incidents.

According to a May 2014 Ponemon Institute Study, the biggest hurdle to determining if insider actions pose a threat is a lack of contextual information from security tools. That is why the StealthWatch System provides additional layers of security context to help administrators make more informed decisions for threat mitigation, including: user identity, device awareness, application-level visibility and threat feed data.
CHAPTER FIVE

Beyond Technology
A 2014 survey by the Ponemon Institute uncovered that only 26 percent of respondents had a multi-disciplinary insider threat management program in place within their organization. It is important to recognize that technology alone cannot prevent insider threats. It has to be a cross-organizational effort that also involves other groups such as HR, Management and Legal.

For example, if HR alerts IT about a disgruntled employee, their network activity can be monitored so that anomalous behaviors such as logging on at unusual hours of the day can be swiftly investigated. And without the involvement of other groups within the company, malicious behaviors discovered by IT cannot be properly addressed.

Specifically, companies that wish to adequately address the insider threat problem should consider the following:

**Background Checks and Screening**
First and foremost, it is important that your company conducts thorough background checks before hiring employees, contractors or third-party vendors so you will know exactly who you are working with.

**Partner Evaluation**
According to the 2014 U.S. State of Cybercrime Survey, “Recent contractor data leaks and payment card heists have proved that adversaries can and will infiltrate systems via third parties, but most organizations do not address third-party security.” Also according to the survey, only 44 percent of respondents have a process for evaluating third parties before the launch of business operations, and only 31 percent include security provisions in contracts with external vendors and suppliers. No matter how strong your security program is, if you are working with insecure partners, it won’t take long for the attackers to find them and use them to infiltrate your network.
“Only 44% of organizations have a process for evaluating third parties before the launch of business operations.”

- PwC, 2014 U.S. State of Cybercrime Survey
Comprehensive Employee Exit Strategies
Research by the CERT Insider Threat Center has shown that malicious insiders typically conduct their unsavory activities within 30 days of giving their resignation. It sounds obvious, but thorough measures need to be taken to revoke employee and contractor access to your company’s systems upon resignation. Also pay particular attention to the person’s active sessions at the time they leave, as they may still be logged in somewhere and able to do damage if they wish.

Management Training
Also according to the CERT Insider Threat Center, insiders who commit crimes often engage in certain behaviors prior to or in the course of committing that crime, such as threatening the organization or bragging publicly about how much damage they could do. If managers are trained to recognize and report these kinds of behaviors, they may identify a potential problem before it becomes a serious security incident.

Employee Assistance
In some cases, personal and financial stress may motivate people to commit crimes at work. There are a number of steps that organizations can take to help employees find constructive approaches to handling difficult personal circumstances, such as establishing a confidential Employee Assistance Program that can provide counseling and advice.
“Only 26% of respondents have a multi-disciplinary insider threat management program in place.”

– Ponemon Institute, Cyber Security Incident Response: Are we as prepared as we think?
User Education
According to a study by Forrester Research of information workers in North America and Europe, only 57 percent said they were aware of their organization’s current security policies and only 42 percent said they received training on how to stay secure at work. User education can go a long way in helping to protect against insider threats. It is a lot easier for employees to abide by best practices for security if they are aware of them, and if they are educated on the serious impact and dramatic consequences that their careless actions could have on the organization. This is especially important in light of new forms of attack such as ransomware.

Users can also be educated about helping to detect potential insider attacks by others. According to the Verizon 2014 Data Breach Investigations Report, the most common way organizations detected insider crimes was when employees reported them.
“The most common way organizations detected insider crimes was when employees reported them.”

- Verizon, 2014 Data Breach Investigations Report
CHAPTER SIX

Summary & Top 10 Ways to Combat Insider Threats
In conclusion, it is critical to recognize that insider threats come in different forms, and technologies that stop one type of insider attack may not necessarily be effective against others. Nonetheless, it is important to adopt a comprehensive range of solutions such as access control and encryption technologies, which can play a big role in deterring insider attacks.

And don’t forget about the use of network logs, particularly NetFlow, for continuously monitoring user activity. Advanced technologies can take the capabilities of NetFlow even further by providing additional security context and helping organizations make sense of the plethora of data available on the network.

In the end, however, insider threat prevention is about more than just technology. Other key groups within the organization, including HR, Management and Legal, for example, also need to join IT in the fight against insider threats.

Please refer to the following Top 10 List for a comprehensive recap of insider threat prevention methods.
Top 10 Ways to Combat Insider Threats

1. First and foremost, it is important that your company conducts thorough background checks before hiring employees, contractors or third-party vendors.

2. Once employees are hired and given access to sensitive systems, establishing appropriate checks and balances for access to confidential data is key.

3. Thorough measures must also be taken to revoke previous employee and contractor access to your company’s systems.

4. Understand the different types and characteristics of insider threats – negligent, malicious and compromised – so that you can better detect and protect against them.

5. Remember that access controls can serve as a key deterrent for both negligent and malicious insiders.

6. Additionally, encryption of data at rest is crucial for minimizing the impact should a negligent employee lose his/her laptop or other equipment.

7. Of course, user education should not be overlooked. It is a lot easier for employees to abide by best practices if they are aware of them.

8. The collection, analysis and storage of various types of network logs should be a critical component of any insider threat security program.

9. Remember that some monitoring solutions provide additional security context, such as identity awareness, which can be invaluable for quickly tracking down the source of insider attacks.

10. Last but not least, it is important to realize that the IT department alone cannot adequately protect a company from its own insiders. Insider threat programs must also involve Management, HR and Legal.
For More Information

Listen to this complimentary webinar for more information on combating insider threats.

Additional Resources

**Insider Threats Infographic**  
Download your free copy today!

**Lancope Video**  
*Insider Threat – Fighting Authorized Evil with StealthWatch*

**Ponemon Institute**  
*Cyber Security Incident Response: Are we as prepared as we think?*

**Lancope White Paper**  
*Internal Network Visibility for APTs and Insider Threats*

**CERT Insider Threat Center**  
Protect Your Network
Combat insider threats and other advanced attacks with Lancope’s StealthWatch® System.

Learn More