ALION
SCIENCE AND TECHNOLOGY

WHITE PAPER

Fighting the Insider Threat

Six Steps to Mitigate Security Vulnerabilities within Your Organization

William (Bill) Senich
Global Cyber Solutions
wsenich@alionscience.com

 08/15

Fighting the Insider Threat

Six Steps to Mitigate Security Vulnerabilities within Your Organization

EXECUTIVE SUMMARY

In this paper, you will learn how to keep pace with the evolving nature of internal threats, develop the toolkit to lock down a broad range of internal security gaps and stay secure even as threats shift over time.

TOPICS INCLUDE:

- The current state of the threat environment
- How to define and identify an insider threat
- How to prioritize risk and apply the right protection resources at the right time
- How to harness the power of analytics to gain visibility and control over your threat universe
- How to develop a formal response plan to ensure continuity of operations

"A third of workers admit they'd leak sensitive biz data for peanuts. And three per cent of employees would consider offers as low as £100"[1]

STATE OF UN-READINESS: CURRENT EFFORTS TO STOP INSIDER THREATS

A recent study within the information security community found that 62% of respondents feel that insider threats have become more frequent in the last 12 months. This study estimates that the overall average cost of remediating a successful insider attack is approximately $445,000. With an average estimated risk of 3.8 insider attacks per year, the total remediation cost of insider attacks can escalate into millions of dollars.

With such a significant risk, where does the services industry stand on insider threat mitigation? The same study cites that only 34% of security professionals expect to receive additional budget to address this growing risk to global business. And while 62% of the study's respondents admit that insider attacks are more challenging to detect and prevent than external threats:

- 21% of respondents said they continuously monitor user behavior.
- 26% monitor access logging only.
- 25% of organizations monitor user behavior within the cloud.

The bottom line is that with the current limited efforts to address insider threats, only 45% of respondents could even answer conclusively as to whether their enterprise had experienced an inside attack in the last 12 months.[2]

OPM BREACH REWRITES THE RULEBOOK

The recent security breach at the Office of Personnel Management exponentially increases a traditionally rare insider threat: the "coerced threat."

With the personal information stolen from 19.7 million security clearance applications,[3] previously trustworthy individuals could be coerced into becoming an insider threat—attacking from unforeseen corners across all sectors of government.

The possibility that this breach was sponsored by a foreign state actor launches the insider threat to a frighteningly unknown level. The impact will be felt for several decades.

The reality is that most organizations are not ready to deal with insider threats, and the potential risk—both physical and financial—is dire. So what can you do about it?

SIX STEPS TO CONTROL THE INSIDER THREAT

Step 1: Define the Threat

The first step is to identify what constitutes an insider threat. The Department of Defense (DoD) defines an "insider" as someone with authorized access to one of their systems, including members of the military, civilian employees, contractors, other vendors/suppliers, educational institutions, and foreign partners.[4]

The "threat" takes the form of an individual or organization abusing their access, granted authority and trust. This is combined with their superior

knowledge of asset value compared to an outside threat.[5] Not all threats are malicious. In many cases the threat vector includes an unwitting insider who is either cleverly exploited by an outsider and either coerced or pressured into compromising the enterprise.

In the private sector, industry experts surveyed feel that the largest insider threat (59% of responses) comes from privileged users, such as managers with access to sensitive information, followed by contractors/consultants/temporary workers at 48% and regular employees at 46%. In their opinion, in addition to removable media, the most vulnerable applications in use today include:

- Collaboration and communication applications, such as email: 45%
- Cloud storage and file sharing applications: 43%
- Finance and accounting applications: 38%
- Social media applications: 33%[6]

Highly-privileged users with broad data access permissions can expose companies to significant risk through either fraud, sabotage or theft of the company's data or through negligent or inadvertent introduction of vulnerabilities that a skilled actor can use to compromise the integrity of the company's data systems.

Step 2: Prioritize the Risk

It's not enough to simply identify threats. You must also identify the 'crown jewels' of an organization. What assets are critical to the continuity of business? These need the most protection. Three locations where data is most at risk in volume are: databases, file servers, cloud.

But, no organization has unlimited resources, making it impossible to assign threat protection to every conceivable risk. Security resources need to be proportionately applied to maximize overall protection.

An effective formula to allocate security resources is:

Risk = Threat * Vulnerability * Impact

To prioritize protection levels in each area, the probability of an attack must be balanced with the potential negative impact of the attack. Risk also needs to be recognized across all threat avenues. As an example: Many organizations deploy advanced security tools to protect their network and other technology assets, but ignore the internal policies and procedures that identify insider threat behavior and enable the threat to go undetected.

Step 3: Detect the Threat

The National Insider Threat Policy, derived from Presidential Executive Order 13587, includes the following as part of its directive to Federal Departments and Agencies:

"Establish an integrated capability to monitor and audit information for insider threat detection and mitigation. Critical program requirements include but are not limited to: (1) monitoring user activity on classified computer networks controlled by the Federal Government; (2) evaluation of personnel security information; (3) employee awareness training of the insider threat and employees' reporting responsibilities; and (4) gathering information for a centralized analysis, reporting, and response capability."[7]

There is widespread agreement that in the fight against insider threats, predictive analytics are essential. The ability to build a holistic database of observation data, including behavioral and technical metrics, enhances the ability to identify trends that match threat profiles. But there are several prerequisites to deploying predictive analytics effectively:

- The ability to integrate behavioral and technical data into one comprehensive view. The gathering of data must be in real-time, valid, reliable and able to continuously yield actionable conclusions
- The ability to build this visibility while adhering to privacy and employee protections
- The ability to effectively use social media—open source intelligence, such as social channels, offers new data collection opportunities, while recognizing it may also be part of the enabling factors in threat development

One size solutions do not fit all. To be effective, predictive threat analytics must build on a pre-

established understanding of the personalities and behavioral norms of the insider population as a whole, then rapidly and accurately identify deviations from these norms.[8] The Department of Homeland Security defines the following characteristics of insiders at risk of becoming threats:

CHARACTERISTICS OF INSIDERS AT RISK OF BECOMING THREATS

Introversion
Greed/financial need
Vulnerability to blackmail
Compulsive and destructive behavior
Rebellious, passive aggressive
Ethical "flexibility"
Reduced loyalty
Entitlement – narcissism (ego/self-image)
Minimizing mistakes or faults
Inability to assume responsibility for actions
Intolerance to criticism
Self-perceived value exceeds performance
Lack of empathy
Predisposition towards law enforcement
Pattern of frustration and disappointment
History of managing crises ineffectively

In most instances, the best defense is to train employees to recognize and report certain behavioral indicators in peers or business partners, specifically:

- Remotely accesses the network while on vacation, sick or at odd times
- Works odd hours without authorization
- Notable enthusiasm for overtime, weekend or unusual work schedules
- Unnecessarily copies material, especially if proprietary
- Interest in matters outside the scope of their duties
- Signs of vulnerability, substance abuse, financial problems, gambling, illegal activities, hostility or poor mental health

Considering the challenges associated with effectively deploying predictive analytics, the use of a third-party vendor is highly recommended. Security analytics is one of the largest areas of investment in the technology sector, and it is a rapidly evolving field. An organization must gather and analyze actionable data in a relevant timeframe to achieve the meaningful protection. Many firms retain analytics vendors who bring specialized tools and deep domain expertise to bear.

Step 4: Supercharge Your Data Security

While the topic of data security can yield volumes of recommendations, some strategies are essential for the technical component of any insider threat protection plan.

AN EXPONENTIAL PROBLEM

This fall, the DoD is launching its Defense Insider Threat Management and Analysis Center (DITMAC), with full operational capacity planned for 2018-2019. The center's goal is to analyze and fuse insider threat data from various sources.[9]

The task ahead is massive. According to the Defense Advanced Research Projects Agency (DARPA), at the time of the Fort Hood Shooting, there were approximately 65,000 personnel stationed at base. Every piece of electronic communication between those soldiers and their contacts equals 14,950,000 different nodes, including people, devices and other communication points. There were up to 4,680,000,000 electronic messages in total.[10] To prevent an attack, this volume of messages needs to be scanned, "normal" communications need to be defined and unusual activity identified.

Identity Management

The proper management of privileged access accounts is critical, as these identities typically have access to the most sensitive corporate information. Strict identity management is necessary to enforce accountability for insiders, and also to limit the damage from an external hacker if they manage to pirate an administrative account.

"The most dangerous insiders have privileged access."
— Edward Snowden

Proper control starts with user privileges. Access rights can be improperly assigned or fail to be revoked when an insider moves on to a new position. Process

and policy should always be in place to evaluate user credentials on an ongoing basis in order to review and, if needed, modify access, as new insider issues are identified.

An effective method to limit abuse of privileged accounts is to require authorization from more than one person for important duties, such as changes to transaction logs or the deletion of backup files.

Network Security Design

A network should be developed at its core with the ability to detect inappropriate activity and notify the right resources to form a response. Normal network activity should be documented for an extended period of time to develop a baseline to compare with potentially suspicious activity.

To create a powerful enterprise security solution, consider adding robust security technologies such as Identity Access Management (dual factor authentication), intrusion detection, file encryption and data loss prevention (DLP) software, traffic monitoring, log analysis (SIEM), network segmentation by user level of access and social media controls. The user and the data should be tagged and data access granted only to authorized users who have a need to know.

Training on the proper use of technology can be as important as the technology itself. Employees should know that their activities are monitored with sophisticated tools. There should be a strong initiative within the organization to educate staff on password control and on the dangers of improper use of social media.

Step 5: Formalize Your Strategy

An insider threat mitigation plan is not something to be done casually. A formal insider threat team should be assembled to develop the strategy. The team should include representatives from executive management, legal, HR, security and IT. The team should have a leader with broad authority to establish an insider threat response policy and plan. Vulnerabilities should be identified and prioritized with resources allocated to meet the unique needs of the organization. One-size-fits-all is not an effective strategy to overcome the insider threat.

In building this strategy, organizational culture must be taken into strong consideration. Strong, positive corporate cultures can work continuously to reduce the threat surface, while negative or ineffective cultures can make defenses weaker and breed new threats. Formal training to build awareness on insider threat issues is key. Members of the organizational culture need to feel that they are part of something special—something valuable and worth protecting. They should understand and appreciate their responsibility to look after their organization and team.

Step 6: Plan Your Response

An insider threat materializes and an incident occurs—now what? You should develop a response plan with a formalized structure and a level of detail similar to your prevention plans. A sound Incident Response Plan includes detailed plans for data breach reporting and includes human resources leadership and legal counsel. The Insider Threat Task Force recommends the following as part of your Incident Response Plan:

- Instead of simply terminating an employee, which pushes them to another vulnerable organization, consider the full range of disciplinary actions against malicious insiders, including legal action.
- Weight the program response towards staff that exhibit suspicious technical or nontechnical behavior. Monitor their outgoing email and use of removable media to ensure they are not removing sensitive information.
- Document and track each insider event with reporting through the Legal Counsel to provide a record of incidents, strengthen insider threat defenses and preserve the company's integrity.[11]

THE INSIDER THREAT TASK FORCE

The Insider Threat Task Force comprises current and former executives from public, private and academic sectors with expertise in cyber security. It was formed to engage with Intelligence Community, DoD thought leaders and private sector to examine best practices in regards to cyber security and insider threats.[12]

BUILD YOUR OWN INSIDER THREAT PROGRAM

For more information on how to deploy these six steps for the protection of your own organization, contact an Alion representative. We can show you how to hone these measures into a specific program with the dedicated agility to meet the evolving threats of the 21st century.

Please contact:
William (Bill) Senich: wsenich@alionscience.com

POINTS TO REMEMBER:

1. No industry sector is immune
2. Less than 50% of organizations have appropriate controls to prevent insider attacks[13]
3. Defense Contractors will soon be required to establish insider threat programs due to the DSS/NISPOM Conforming Change 2
4. Understand your network: what's going out is as important as what's coming in
5. Endpoint protection must address USB use and printers

BIBLIOGRAPHY

1 "A Third of Workers Admit They'd Leak Sensitive Biz Data for Peanuts," *The Register*, (July 29, 2015)

2 "Insider Threat Spotlight Report," Crowd Research Partners, SpectorSoft, developed with cooperation of LinkedIn Group Partner: Information Security, (2015)

3 Jim Sciutto, "OPM Government Data Breach Impacted 21.5 Million," CNN, (July 10, 2015)

4 "DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team," Department of Defense, United States of America

5 "DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team," Department of Defense, United States of America

6 "Insider Threat Spotlight Report," Crowd Research Partners, SpectorSoft, developed with cooperation of LinkedIn Group Partner: Information Security, (2015)

7 "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," White House Memo, (November 21, 2012)

8 "Combating the Insider Threat," Department of Homeland Security, National Cyber Security and Communications Integration Center, (May 1, 2014)

9 Patrick Tucker, "To Prevent Insider Threats, DOD Must First Define 'Normal,'" Defense One, (July 19, 2015)

10 "Anomaly Detection at Multiple Scales (ADAMS): Broad Agency Announcement, (October 22nd, 2010)

11 "A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector," Intelligence and National Security Alliance, Cyber Council: Insider Threat Task Force, (September, 2013)

12 "A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector," Intelligence and National Security Alliance, Cyber Council: Insider Threat Task Force, (September, 2013)

13 "Insider Threat Spotlight Report," Crowd Research Partners, SpectorSoft, developed with cooperation of LinkedIn Group Partner: Information Security, (2015)