January 10, 2015

Insider Threat Report:

The Ten Steps to Thwarting the Insider Threat

By Kevin McPeak, CISSP, ITILv3

Technical Architect, Security

Public Sector Strategic Programs

Symantec Corporation

www.symantec.com

EC-Council

http://ciso.eccouncil.org/

Insider Threat Report:

The Ten Steps to Thwarting the Insider Threat

INTRODUCTION:

The damage caused by Insider Threats has been a recurring news topic, capturing headlines around the world. The Office of the Director of National Intelligence (ODNI) offered this perspective:

"Over the past century, the most damaging U.S. counterintelligence failures were perpetrated by a trusted insider with ulterior motives. In each case, the compromised individual exhibited the identifiable signs of a traitor – but the signs went unreported for years due to the unwillingness or inability of colleagues to accept the possibility of treason."

Insider Threats should be analyzed holistically. Some believe that thwarting the Insider Threat is exclusively about data loss prevention, but it's actually far more complex. It's both a data lifecycle management challenge as well as cybersecurity challenge. Organizations that value the protection and preservation of their financial, personnel, and customer data, as well as their Intellectual Property (IP) and other forms of proprietary information, should employ a comprehensive approach to battle Insider Threats. A robust, defense in depth Insider Threat program is typically built on four core processes:

- Defuse the Threat – businesses must proactively understand, manage, and monitor their data, which reduces the risk of Insider Threats even attempting exploitation.
- Deter the Threat – organizations must develop "right for them," tailored, best security practices, which makes the secure process the friendliest process throughout the data lifecycle. Informed users are less likely to bring harm to their organization's cyber posture.
- Detect the Threat – security teams should detect threats earlier and more accurately, using multiple data sources – including from inside your business, the cloud, and both technical and non-technical social network sources.
- Defend Against the Threat – Should an Insider Threat choose to act, the net effect of an organization's technical and process solutions should protect both their systems and their data by using their infrastructure in the most efficient possible way.

[1] "Insider Threat," National Counterintelligence and Security Center. http://www.ncix.gov/issues/ithreat/

The Insider Threat concern is essentially a subset of the overall cyber threat landscape. The threat landscape facing large enterprise data owners has fundamentally shifted over the years. In an era long gone, hackers simply demonstrated their technical prowess by defacing corporate or government websites. Cyber-attacks then evolved into more malicious cyber-crime just as such attacks became increasingly lucrative to carry out. Cyber espionage also exploded onto the stage and has recently escalated into cyber warfare, as nation-states battle each other not only on land, sea, and in the air, but increasingly within the cyber realm. Well placed malicious insiders can facilitate destructive cyber events with cataclysmic potential for damage.

An effective breach and subsequent large scale exploitation can be carried out more successfully with the help of one or more Insiders. According to the ODNI, "Malicious insiders can inflict incalculable damage. They enable the enemy to plant boots behind our lines and can compromise our nation's most important endeavors."

However, destructive Insider Threat activities are not only performed by malevolent actors. It's actually been determined that 64% of data loss caused by insiders, are caused by insiders who meant well. In other words, the majority of Insider Threat events are not caused by insiders seeking to bring harm to their employer, but by insiders who either meant well but nonetheless did not follow proper data handling policies, or by those who did not even know what the proper procedures were for their respective companies.

The total dollar cost of breaches perpetrated by insiders should never only be calculated in terms of the raw value of the compromised systems or data, but also by factoring in the burden of legal and compliance penalties along with loss of market share as customers, employees, and investors lose faith in the compromised business entity.

An Insider Threat can harm an organization by negatively impacting what is known as the "CIA triad," which consists of the confidentiality, integrity, and availability of an organization's data. While many businesses do an effective job of managing external cybersecurity threats that attempt to attack the organization's IT infrastructure from the outside, fewer businesses have also effectively tackled the Insider Threat. With the Insider Threat, the concern is that important or sensitive data located within the inside is being compromised, modified, or made unavailable by employees of the company or those given access to the inside IT infrastructure of the company.

Each business should carefully assess its goals for thwarting the Insider Threat. Each industry will have different priorities in defining their goals, but regardless of industry, such strategy sessions frequently converge on the following goals:

- Safeguard the lives, safety, and reputation of your organization by safeguarding your operation's most sensitive data Government agencies, corporations, and academic institutions can suffer an enormous reputation hit after even one embarrassing public disclosure.
- Discover sensitive data wherever it resides and identify those endpoints with the highest risk.
- Actively monitor the many ways that sensitive data can be used on the endpoint and flag all abnormal activities.
- Utilize the most efficient and unobtrusive methods possible.

[2] Ibid

A business can pursue the previously mentioned goals through the following ten steps:

STEP ONE

Identify the appropriate data owners (operating units, specialized teams, task forces, specific individuals).

a. Work with these Data Owners to further identify additional priority data types.

b. Over a senior management agreed upon cycle of time, perform this as an iterative process for reigning in the organization's overall risk posture.

STEP TWO

Locate all of the places where sensitive data resides.

a. Consider data at rest, data in use, data in motion, archived data, and encrypted data.

b. Consider standard locations such as network devices, storage, databases, file servers, web portals and other applications, laptops, e-mail servers (MTA or Proxy), and PST files.

c. Also consider non-traditional locations such mobile devices, printers, scanners, fax machines, copiers, file sharing apps, USB drives, CD/DVDs, paper copies, IM, "free" webmail services, university webmail for students and alumni (who may be working within your corporate offices and using your network to access encrypted mail systems that your company does not control), and FTP puts.

STEP THREE

Tag your sensitive data.

STEP FOUR

Monitor and learn how sensitive data is typically generated by and then used by your workforce.

STEP FIVE

Determine where your sensitive data goes once it is created or modified.

STEP SIX

Implement automatic “real-time” methods to enforce your CISO approved data security policies (visibility, remediation, notification & prevention).

a. Visibility: The first step is to understand where your data is stored and how it is used across your enterprise.

b. Remediation: Once you’ve identified broken business processes and high-risk users, then you can improve processes, clean up misplaced data, and provide specialized training to high-risk users.

c. Notification: Next, turn on automated e-mail and onscreen pop-up notifications to educate users about data loss policies. This alone can dramatically cut down the number of repeat offenses.

d. Prevention: Lastly, stop users from accidentally or maliciously leaking information by quarantining, encrypting, or blocking inappropriate outbound communications.

STEP SEVEN

7. Educate your sys admins as well as your end users about sensitive data security.

a. Sys admins may not realize CISO approved policies exist for certain data types. Educating them and winning them over towards a mindset of thwarting the Insider Threat is a key component towards success.

b. Sys admins (as well as end users) may be more receptive than you would initially think most sys admins will welcome the opportunity to participate in promoting proper cyber hygiene across the enterprise.

STEP EIGHT

De-escalate excessive sys admin privileges.

a. Most sys admins don't want admin rights beyond what they need to do their assigned job functions.

b. Separation of duties is a cybersecurity best practice for thwarting the sys admin "Insider Threat."

STEP NINE

Wrap additional security around sensitive data.

a. Deploy creative and technically rigorous security around each aspect of your data at rest, data in motion, and data in use, realizing that the best and also the least expensive Incident Response (IR) is for the incident to have been prevented in the first place, long before it even became an incident.

b. Constantly review file permissions. Those who no longer maintain an operational need to access sensitive data should have their rights to those data sets revoked.

c. Consider using additional encryption for sensitive data as part of your defense in depth posture.

STEP TEN

Halt data leaks before spillage occurs.

a. An ideal Insider Threat program will be highly automated to provide resolution, enforcement, and notification when a potential data loss is occurring. This is when the loss can be halted, rather than only assessing the damage in hindsight much later on.

b. The right team member(s) need rapid notification when such events occur, so that they can respond quickly.

c. High severity incidents should receive the highest alert notifications.

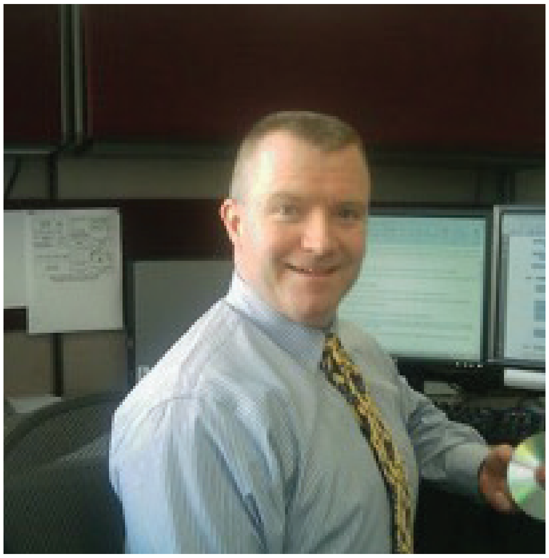
d. The "five second test" occurs when it can be demonstrated that information indicating that an Insider Threat event is in progress is identified, routed to security personnel, and thwarted via automation, all in less than five seconds.

e. Automated systems that allow for one-click responses to shut down Insider Threat events in real-time are ideal.

f. Organizational leaders need access to the right metrics, in order for the security team to prove the value of their Insider Threat prevention program

In conclusion, businesses must not only concern themselves with external cybersecurity threats. They must also anticipate and understand the myriad ways that Insider Threats, which consist of both well-meaning and malicious personnel, can gravely harm the confidentiality, integrity, and availability of their most valuable and sensitive data and systems. By developing strategic goals for thwarting Insider Threats, an organization can then develop a rigorous step by step process for applying both technical and non-technical means to prevent and reduce the damage that Insider Threats can cause.

ABOUT THE AUTHOR



Kevin McPeak is a Symantec Security & Mobility Architect who is focused on supporting US Government customers. In this capacity, he serves as a technical SME for reputation based malware filtering, endpoint management, endpoint security, data loss prevention, encryption, mobile device management, mobile app management, secure mobile content delivery, and new defensive technologies.

Kevin has two Masters of Science degrees, with one being earned at Johns Hopkins University and the other being earned at Virginia Tech. He is also currently a part-time PhD candidate at Virginia Tech's northern Virginia extension campus.

Prior to working for Symantec, Kevin worked for several systems integrators to include CACI, Lockheed Martin, and AlphaInsight. Additionally, Kevin is currently an Army Reserve warrant officer [CW3] (with over 22 years of continuous service) and in that military capacity he is a veteran of both Operation Enduring Freedom (2003) and Operation Iraqi Freedom (2010 – 2011).

COMPANY INFORMATION

Symantec Corporation
www.symantec.com