INSIDER THREAT PROTECTION FRAMEWORK

Steve Higdon

Contents

Acknowledgments

This framework was reviewed by Jason Hoenich, Robert Beverly, Richard Morrison, and Brian Woodall, all of whom provided substantial feedback and contributions. They were instrumental in the framework's completion and quality.

Introduction

Insider Threat is an information security problem that has led to numerous breaches of data in organizations. It has been attributed as the leading contributor for a large percentage of overall information security incidents and continues to cause concern for organizations attempting to avoid data loss, ransomware, phishing, and other similar attacks.

> The definition of Insider Threat, according to the National Insider Threat Task Force (NITTF) in the National Insider Threat Policy is the threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

For the sake of this framework and so that it may be used by organizations of all types and in all industries, Insider Threat can be defined as any decision or action taken by someone within an organization that can cause harm to that organization. Insider Threats can be classified into three primary categories – accidental, negligent, and malicious. Several previous philosophies pertaining to Insider Threat were focused solely on malicious insiders. More recently and especially with increased attention drawn to phishing and other social engineering techniques, individuals and organizations have also included unintentional insiders, where the likelihood of incidents is significantly higher.

According to the National Insider Threat Policy referenced above, Insider Threat incidents can be categorized as leaks, spills, espionage, sabotage, and targeted violence. The most common of these categories are leaks and spills, where sensitive information for an organization or its customers is copied or moved from within organizationally-controlled assets to a location controlled by the attacker or to publicly accessible storage space. Espionage, sabotage, and targeted violence are categories of Insider Threat incidents conducted by malicious insiders, where intent is to cause harm to the organization or individuals within an organization. Insider Threat is not a problem exclusive to information technology or information security. Industrial/physical security, legal, and human resources teams, as well as senior management should also be involved in working toward reducing Insider Threat risk.

Framework Basics

The Insider Threat Protection Framework is a tool that organizations can use to measure their preparedness and effectiveness in responding to Insider Threat incidents. Many of the controls outlined in the framework can also be used as a deterrent against such incidents, especially through training and culture improvements.

These controls are not intended to be used for compliance purposes, but to assist organizations in improving their security posture against Insider Threat. Most organizations will find that several Insider Threat protection controls also align with other frameworks and regulations, of which they already comply.

Another key point of understanding is that the Insider Threat Protection Framework is not a tool to be used only once or by itself. The Insider Threat program must work in coordination with other areas of the information security program to achieve success. This is especially important for larger organizations with established security operations centers (SOCs), policy departments, and legal teams. SOCs specialize in the ability to detect and respond to suspected incidents and events quickly, and they can recognize insider trends and individuals or teams who exhibit behaviors that increase overall risk to the environment.

Many organizations still focus their Insider Threat programs on data loss prevention (DLP). The industry has more recently found that insiders can increase risk to other important areas as well, such as organizational capabilities and business processes. The need to identify data, capabilities, and processes that require increased security can help when forecasting budgets, allocating resources, and developing improvement plans. Risk, in all applications, must take several factors into account. A common equation for risk is impact multiplied by probability, and all divided by cost. Sometimes a set of data or system can be highly vulnerable, yet its sensitivity to the organization or business is so low that resources could be better spent on higher priorities. Those priorities will not be known however, unless the organization first identifies them through a risk assessment.

There are three primary elements that administratively cover all areas of an effective Insider Threat program: support from senior management, inclusion of Insider Threat into the organizational security budget, and the primary goal of cultivating positive security culture within the organization. Even though culture is the last area covered in the framework controls, it represents both the culmination of all other Insider Threat protection efforts and the measurement of success for Insider Threat programs. While improved security culture is the perceived destination, the journey must include improvements in the other three control categories.

How to Use the Framework

A list of security controls is included in the framework to assist organizations in their efforts to measure the effectiveness of their Insider Threat programs. To assess the level of preparedness for Insider Threat incidents, organizations should start with the Administration controls for each of the four control categories (Policy, Technology, Awareness and Training, and Culture) as a baseline to determine maturity of current programs. To take a more granular view, they can then move through the Quality, Implementation, and Maintenance controls.

The number of controls that are not met can be used to measure overall preparedness and level of maturity for Insider Threat protection. Organizations are encouraged to develop a plan of actions for each of the control gaps to achieve stronger security postures and protect against Insider Threat incidents.

Framework Controls

Policy

Policy Administration (PA)
Policy Quality (PQ)
Policy Implementation (PI)
Policy Maintenance (PM)

PA-1	The organization has policies in place to help reduce Insider Threat risk
PA-2	Policies are easily accessible by employees
PA-3	Employees formally acknowledge understanding and intent to comply with organizational policy
PQ-1	Policy includes a summary that highlights key requirements and associated explanations of what they entail
PQ-2	Policy is written in a manner of which the end user is the target audience
PQ-3	Policy identifies acceptable use of IT equipment and information
PQ-4	Policies outline reporting process for suspicious activities
PQ-5	Responsibilities are clearly defined and specific

PQ-6	Policy compliance requirements match the organization's culture, IT environment, and employee base
PI-1	Policies are referenced in periodic communications
PI-2	Applicable stakeholders are included in policy development and modification
PI-3	Support and compliance with policy is consistent at all levels of the organization
PI-4	Enforcement strategy for policy compliance is developed and followed
PM-1	The organization regularly performs maintenance on its policies
PM-2	The organization has policy review/update procedures
PM-3	The organization has a policy review/update schedule
PM-4	The organization reviews/updates policies according to a predefined schedule
PM-5	The organization performs policy reviews/updates according to predefined procedures

Technology

Technology Administration (TA)
Technology Quality (TQ)
Technology Implementation (TI)
Technology Maintenance (TM)

TA-1	The organization uses technology support policy and training
TQ-1	The organization implements technologies aimed at reducing Insider Threat risk
TQ-2	The organization consistently uses Insider Threat technologies as a primary part of its Insider Threat program
TQ-3	Access controls are implemented by the organization to protect sensitive data
TQ-4	Access is controlled by the organization to ensure least privilege
TQ-5	Access is based on individual roles in the organization
TQ-6	Privileged access is controlled by the organization to ensure least privilege
TQ-7	Alerts generated by technology solutions are filtered in order to reduce false positives

TI-1	Technologies are implemented in a manner intended to avoid production impacts
TI-2	Change management procedures are used to avoid unauthorized changes to systems
TI-3	Security and event logs are gathered and stored for systems
TI-4	Security and event logs are analysed with a security incident and event management solution
TI-5	Security incident and event management solution generates alerts
TI-6	The organization responds to security alerts generated by technology solutions
TI-7	The organization has implemented a technical reporting solution or methodology
TM-1	The organization regularly performs maintenance on its technological solutions
TM-2	The organization has technology review/update procedures
TM-3	The organization has a technology review/update schedule
TM-4	The organization reviews/updates technology according to its predefined schedule
TM-5	The organization performs technology reviews/updates according to predefined procedures
TM-6	Data and system access is regularly reviewed to reduce the likelihood of unauthorized access to sensitive data

Awareness and Training

Awareness and Training Administration (AA)
Awareness and Training Quality (AQ)
Awareness and Training Implementation (AI)
Awareness and Training Maintenance (AM)

AA-1	The organization has an awareness and training program
AA-2	The awareness and training program has support from senior management
AA-3	The organization has a method for measuring success of the awareness and training program
AA-4	The organization has an established training program for personnel responsible for Insider Threat protection
AQ-1	The awareness and training program supports organizational security policy
AQ-2	Training is role-specific to maximize effectiveness

AQ-3	Training parallels the organization's current operating environment
AQ-4	Training curriculum includes current industry trends and recent threats
AQ-5	Training includes identifiers of common Insider Threat behaviors and attack methods, to include social engineering
AQ-6	The organization has established reporting procedures
AQ-7	Training includes the organization's reporting procedures, including supporting technical solutions or methods
AQ-8	Formal training includes all key topics of the awareness and training program
AQ-9	Informal training includes at least one key topic of the awareness and training program
AQ-10	Insider Threat program personnel have defined roles and training is role-specific
AI-1	Formal training is conducted at the frequency required by compliance at a minimum
AI-2	Informal training is conducted at least monthly
AI-3	Training is conducted either in-person or virtually
AI-4	The organization uses a variety of training methods
AI-5	Training topics are enforceable
AI-6	Physical penetration tests are regularly conducted to enhance training and measure effectiveness
AM-1	The organization regularly performs maintenance on its awareness and training
AM-2	The organization has awareness and training review/update procedures
AM-3	The organization has a awareness and training review/update schedule
AM-4	The organization reviews/updates awareness and training according to its predefined schedule
AM-5	The organization performs awareness and training reviews/updates according to predefined procedures
AM-6	Insider Threat program personnel have both informal and formal training requirements that include practical exercises and updated adversary tactics, techniques, and procedures

Culture

Culture Administration (CA)
Culture Quality (CQ)
Culture Implementation (CI)
Culture Maintenance (CM)

CA-1	The organization has a security culture improvement program
CA-2	The security culture improvement program has support from senior management
CA-3	The organization has a method for measuring success of its security culture improvement program
CQ-1	The organization identifies weaknesses in security culture
CQ-2	The organization focuses improvement efforts to address weaknesses
CQ-3	The organization's employees understand that security is everyone's responsibility
CI-1	Organizational leadership regularly communicates key security concepts
CI-2	Planning and implementation of the security culture improvement program includes employees with a variety of roles, skills, backgrounds, and seniority levels
CI-3	Rewards and/or incentives are used by the organization to support positive actions and behavior
CM-1	The organization regularly performs maintenance on its security culture improvement program
CM-2	The organization has security culture improvement program review/update procedures
CM-3	The organization has a security culture improvement program review/update schedule
CM-4	The organization reviews/updates security culture improvement program according to its predefined schedule
CM-5	The organization performs security culture improvement program reviews/updates according to predefined procedures

References

Collins, Matthew., Theis, Michael., Trzeciak, Randall., Strozer, Jeremy., Clark, Jason., Costa, Daniel., Cassidy, Tracy., Albrethsen, Michael., & Moore, Andrew. (2016). *Common Sense Guide to Mitigating Insider Threats, Fifth Edition* (CMU/SEI-2016-TR-015), https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.

National Insider Threat Task Force. (2012). *National Insider Threat Policy*. Issued by President Barack Obama, https://www.dni.gov/files/NCSC/documents/nittf/ National_Insider_Threat_Policy.pdf