Software Engineering Institute | Carnegie Mellon.

Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls

Andrew P. Moore
William E. Novak
Matthew L. Collins
Randall F. Trzeciak
Michael C. Theis

Abstract

The goals of the initial work described in this paper are to elaborate the potential ways an insider threat program (InTP) could go wrong and to engage the community to discuss its concerns and, ultimately, to define practical strategies for mitigating these consequences. We describe several categories of negative unintended consequences as to whether they involve (1) interference with legitimate whistleblower processes and protections, (2) InTP management/employee relationships, (3) InTP management's lack or loss of interest in the program, or (4) misuse of the InTP by its staff or other employees (accidental or purposeful). We also present a fully-elaborated InTP archetype specification that describes a particular negative unintended consequence in detail with an associated archetypal narrative, a causal loop specification, and a discussion of possible mitigations. By establishing a clear picture of the way things could go wrong when establishing and executing an InTP, we can help organizations understand the need for a balanced approach that has a better chance of reducing insider threats while minimizing the chances or severity of negative unintended consequences. Future work will involve validating (or refuting) the existence of the unintended consequences and mitigations in operation, enumerating other negative unintended consequences that have occurred, and elaborating methods to avoid or mitigate these consequences.

INTRODUCTION

What if an organization chooses methods in developing its InTP that are seen by its employees as being intrusive and micro-managing? Even worse, what if an organization becomes overly aggressive in its insider threat monitoring and investigation, and is seen as Orwellian and adversarial? *Could this spur employee disgruntlement in a way that increases insider threat risk? Could unwanted media attention or even lawsuits by disgruntled insiders harm the organization's reputation and make hiring qualified individuals more difficult?*

What if an organization focuses so exclusively on an established list of indicators that it fails to notice insider threats that have rarely been seen before? At

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

> an enterprise level, suppose an organization spends a large amount of time and resources to establish an InTP only to find that no real threats are found, but instead a large number of false leads. *Would insider threat risk management start to be viewed as a resource sink with little ROI, thus causing management to eventually dismantle the program or merely pay lip service to its existence with minimal actual support?*

These are just a few of the potential negative unintended consequences of attempts by an organization to establish an InTP. We do not have empirical evidence that these consequences have happened to organizations that established or are establishing InTPs. However, their potentiality has been expressed as concerns by organizations with which the CERT Insider Threat Center has been in contact.

The goals of the initial work described in this paper are to elaborate the potential ways an InTP could go wrong and to engage the community to discuss its concerns and, ultimately, to outline practical strategies for mitigating these consequences. By establishing a clear picture of the way things could go wrong when establishing and executing an InTP (many of which may already be lurking in the back of the minds of organizations), we can help organizations understand the need for balance in their approach. We believe that a candid elaboration of how establishing an InTP can be taken too far will help InTP managers avoid misinterpreting the guidance provided by the CERT Division of the Software Engineering Institute and government organizations, and increase buy-in for a balanced approach with a better chance at reducing insider threats while minimizing the chances or severity of negative unintended consequences.

In this paper, we first describe the set of potential negative unintended consequences that we have identified to date. The consequences were identified through internal (CERT Division) brainstorming sessions and a formal discussion at the first offering of the Insider Threat Program Implementation and Operations course (a part of the *CERT Insider Threat Program Manager Certificate Training)*. We describe findings from these sessions as well as an elaboration of a particular negative unintended consequence in the form of a system archetype, originally described by Peter Senge [Senge 1990]. We conclude with a summary of our current status and areas of potential future research.

POTENTIAL NEGATIVE UNINTENDED CONSEQUENCES

In this section, we describe the current set of potential negative unintended consequences of establishing or executing an InTP within an organization. We separate these consequences based on whether they involve

- interference with legitimate whistleblower processes and protections
- InTP management/employee relationships
- InTP management's lack or loss of interest in the InTP
- misuse of the InTP by its staff or other employees (accidental or purposeful)

This breakdown was our first attempt at categorizing the problems that might arise, though it may need to be refined or extended as we identify others, possibly through interactions with organizations in the process of establishing their own programs. We have started to describe a finer grained taxonomy of potential problems, as specified in Appendix A, but are not yet at a point of declaring it complete.

Interference with Legitimate Whistleblower Processes and Protections

Table 1: Unintended Consequences that Interfere with Legitimate Whistleblower Processes and Protections

1a. Unprotected Whistleblowers Bite Back.		
	Behavior	The InTP does not adequately distinguish between legitimate whistleblower programs and the InTP function, possibly treating legitimate whistleblowers as suspects/criminals.
	Consequence	The organization inhibits correction of problematic issues, may encourage illegitimate whistleblowing, and may get bad press and be subject to lawsuits.
	Mitigation Strategies	Clearly delineate the InTP processes and procedures from those of the whistleblower program, and train InTP staff on the distinction between the two programs as well as how to process legitimate whistleblower actions if encountered.

1b. Distrusting Whistleblower Goes Public.		
	Behavior	Employees distrust effective (but misperceived) whistleblower protections.
	Consequence	Employees' use of illegitimate (over legitimate) whistleblowing creates unnecessary problems for the organization.
	Mitigation Strategies	Regularly remind employees (possibly as part of insider threat training) of the distinction between legitimate whistleblowing and insider threat, and the distinct processes and procedures applicable to each.

Table 1 lists two potentially negative unintended consequences of an InTP related to whistleblowing. While they have similar results (the potential for illegitimate whistleblowing and great harm to the organization), the causes and mitigations of the unintended consequence differ. In the first case, the InTP is not treating whistleblowing as a legitimate function with its own processes and procedures. In the second, the InTP respects the role of whistleblowing, but employees do not trust that whistleblowers will be treated fairly.

Mitigation Discussion

Though technical indicators of insider threats are valuable for detection, employee reporting of suspicious behavior or observed insider attacks can provide the missing piece to detect a case of insider threat. InTPs need to provide employees with a clear procedure for reporting observed wrongdoing. This internal reporting can be viewed as a form of internal whistleblowing; organizations should offer similar protections to the employee that a person would receive when they report the matter to an external, independent third party officially charged with rectifying any wrongdoing. This protection comes with the responsibility of investigating reports in an impartial and fair manner, keeping the whistleblower anonymous and protected from retaliation, and, when appropriate, providing feedback to the internal whistleblower about the outcome of the investigation.

The whistleblower might decide to report the perceived wrongdoing to a legitimate third party if the employee believes that he or she will not be afforded adequate protections by the organization or the organization will not change based on the whistleblowing. Also, whistleblowing to a legitimate third party is encourage by financial incentives, such as those provided by the Dodd-Frank Whistleblower Program. If activity related to external whistleblowing is detected (such as providing the government with evidence of wrongdoing), the InTP must be able to correctly identify the activity as legitimate and take care to not interfere with the process. Exfiltrating data to an illegitimate third party is still theft and should be detected and prevented by the organization's InTP monitoring.

To avoid the consequences in Table 1, the InTP should make it clear that internal reporting is encouraged when appropriate, that internal whistleblowers will be protected, and that reports of wrongdoing will be used to improve the organization. The organization should also clearly identify the legitimate external options available to whistleblowers and take care to not interfere with legitimate whistleblowers. The InTP can include clear guidance in policies and insider threat awareness training that explains protected whistleblower rights and procedures and how they are not diminished by the existence of the InTP. They can also provide employees with examples of the positive impact of valid whistleblowers using public examples from other organizations if none are available in the organization's history

InTP/Management/Employee Relationships

Table 2: Unintended Consequences that Involve InTP/Management/Employee Relationships

2a. Aggressive Detection Alienates Employees.		
	Behavior	The InTP is overly aggressive in its detection and response measures.
	Consequence	A high false-positive rate alienates employees, exacerbates threats, reduces morale, repels good employees, inhibits creativity, and/or increases claims of privacy violations and law suits.
	Mitigation Strategies	Maintain minimum thresholds for establishing inquiries and strict confidentiality once inquiries are initiated.
2b. Aggressive Prevention Inhibits Performance.		
	Behavior	The InTP is overly aggressive in its prevention measures.
	Consequence	The InTP inhibits employee productivity/creativity, reduces morale, and repels good employees.
	Mitigation Strategies	Align insider threat prevention measures with the culture of the organization and the extent of the risk to critical assets due to insider threat.
2c. Secretive Surveillance Breeds Distrust.		
	Behavior	InTP measures are overly secretive or deceptive.
	Consequence	The InTP creates an environment of distrust between management and employees.

	Mitigation Strategies	Clearly articulate the following in employee agreements and training: roles and responsibilities of the InTP, the rights of employees, and the limits to how the InTP can use the information collected.
2d. Open Surveillance Promotes Evasion/Subversion.		
	Behavior	InTP measures are overly transparent.
	Consequence	Employees may try to evade or subvert the InTP for their own (possibly malicious) benefit.
	Mitigation Strategies	Maintain confidentiality about the details of detection methods and diversify methods as much as possible.
2e. The InTP Inhibits Employee Reporting.		
	Behavior	The InTP inadequately motivates the need for suspicious behavior reporting.
	Consequence	Employees may resist reporting suspicious behaviors for fear of getting others in trouble for no good reason.
	Mitigation Strategies	Clearly define and exemplify in security awareness training the relationship between the behaviors you are asking employees to report and the threat that may be behind those behaviors.
2f. Early Suspicions Bias Investigations.		
	Behavior	InTP investigations form early false leads on which investigators focus almost exclusively.
	Consequence	The diversion of the investigation wastes resources and prevents identifying the true problem.
	Mitigation Strategies	To the extent possible, perform analysis without knowledge of the specific suspects prior to initiating an inquiry, and use different parties to initiate, investigate, and adjudicate inquiries and incidents.

An InTP has the potential to strain the relationship between managers and the employees that they manage at all levels. Table 1 describes the range of problems associated with the strain that can occur. An organization’s employees may view the InTP staff in an adversarial way—“they are trying to catch us doing something bad!” Employees may start gaming the system, hiding their behavior, or neglecting to report coworker behaviors that the InTP depends on for an effective detection system. Employees, especially those that view the InTP adversarially, may infer the strategy of the InTP from the response that it takes to various behaviors and thus inhibit InTP effectiveness over time.

Mitigation Discussion

To create an atmosphere of trust within the organization, InTPs should clearly articulate both what the InTP is and what it is not as part of Insider Threat Awareness Training. InTPs should also clearly state in employee acknowledgements (logon banners, user accounts, etc.) when and for what purpose the InTP may use information. To ensure preventive measures do not go too far, they should be aligned with the protection of critical assets from empirically measured threat vectors using an established risk management approach. InTPs should establish procedures that ensure confidentiality of inquiries, since the majority of anomalies and allegations will likely be disproved/unsupported. Knowledge of the existence of an inquiry should be kept to the absolute minimum number of individuals necessary to resolve the issue.

Confidentiality also serves to promote unbiased investigations. The InTP should endeavor to analyze as much data as possible without knowledge of the name of the suspect before making a decision to open an inquiry. In this way, bias for or against individuals can be averted. For a notional example, John Doe inserts a USB device and downloads a large amount of sensitive. Immediately knowing that John Doe is the individual that inserted a USB and downloaded data can impart a bias of either “John would never do something questionable so take no action” or “John is pretty shady, so let’s open an inquiry.” However, without knowing the name of the individual and comparing other data sources in the blind might reveal that the download occurred two minutes before the individual logged-off, badged out, and was not seen in the facility or on the system for another 30 days. An impartial decision to open an inquiry subsequently reveals it was John Doe, and John went on vacation in a foreign country right after downloading the sensitive data.

Organizations may also want to separate those who initiate inquiries from those that perform and investigative functions and adjudicators. For example, Alice the analyst verifies the veracity of an alert or allegation with supporting data, initiates an inquiry that is conducted by Bob (who is not a co-worker of Alice) and Bob’s report of findings are adjudicated by Charlie (who is not a co-worker of Bob or Alice). Subsequent to the final disposition of the inquiry, Dan (a managerial, but non-supervisor of Alice, Bob, or Charlie) reviews the entire inquiry process and makes any necessary recommendations for quality control improvements.

Credibility of the InTP is of course of primary concern. Inquiries are the face of the InTP to those being investigated or who are otherwise involved in the investigation. The InTP should carefully establish thresholds for initiating inquiries to ensure the inquiry is truly warranted and the anomaly or allegation could not be resolved through other less intrusive means. It also should finely tune alert rates to avoid unnecessary inquiries.

While the InTP should make it clear that measures are used to protect critical assets, should not openly reveal the exact methods used in InTP processes (identification of hardware, software, inspection schedules, and procedures). In those instances where detection methods and procedures are known by specific individuals, the InTP can use alternative methods and procedures to ensure those with knowledge of the regular methods are not able to employ effective countermeasures. This approach is analogous to law enforcement's use of both regular police cars and unmarked police cars for the enforcement of traffic laws.

To maintain insider threat situational awareness, the InTP can collect and analyze statistical data concerning reporting rates, methods, and types of incidents reported. This information can provide insight into the relative effectiveness of awareness training, confidential reporting methods, and the types of incidents that employees are most likely to recognize and report. Organizations should analyze InTP detections and employee reporting to develop trends and potential future threats that may need to be addressed through enhanced awareness training or more effective protective measures.

Management Lack/Loss of Interest in the InTP

Table 3: Unintended Consequences that Involve Management Lack/Loss of Interest

3a. Costly InTP Work Is Undermined by Perceived Higher Priorities.		
	Behavior	The mandate to have an (expensive) InTP is unfunded.
	Consequence	Management views the InTP as taking funding away from more beneficial work and support erodes.
	Mitigation Strategies	Track InTP operational measures and then use to improve operations over time and justify the organization's investment in the InTP.
3b. An Ineffective Program Loses Steam.		
	Behavior	InTP detection measures do not identify ongoing threat behaviors or identify mostly innocuous behaviors.
	Consequence	Management views the ROI of the InTP as low and support erodes.
	Mitigation Strategies	Learn from InTP failures to improve its operation over time, and remind leadership (perhaps as part of regular insider threat awareness training) that the purpose of the

		InTP is not to “catch bad guys,” but to manage the risk to critical assets.
3c. False Positives Erode Support.		
	Behavior	InTP detection and response exposes high false-positive rates.
	Consequence	Management thinks InTP measures are ineffective and support erodes. Employees think management is incompetent and trust erodes.
	Mitigation Strategies	Define clear procedures for incident response that include how to vet alerts against other data sources with the goal of establishing reasonable suspicion and justifying further inquiry.
3d. Too Much Information Erodes Support.		
	Behavior	The InTP detects peripheral behaviors that the organization prefers not to know.
	Consequence	Management thinks the InTP increases its liability and support erodes.
	Mitigation Strategies	Produce scenarios for leadership to consider, wherein the ignorance of insider threat scenarios would demonstrate an ineffective shield against lawsuits or negative public opinion.
3e. Apparent Success Diminishes the Perceived Need.		
	Behavior	InTP measures apparently eliminate the perceived problem.
	Consequence	Management thinks they have solved (or don’t have a) problem and support erodes.
	Mitigation Strategies	Remind leadership (perhaps as part of regular insider threat awareness training) of the cyclical nature of threats based on new hires, mergers/acquisitions, policy changes, etc.

Support for the InTP from the chief executive through all levels of management is crucial for the continued success of the InTP mission. Table 3 describes various ways that management support may erode. Many organizations are mandated to establish an InTP, but if financial support is inadequate or there are other perceived higher priorities, support may dwindle for anything beyond paying lip service to the need.

The situation may become worse if the InTP appears to be ineffective or if the false-positive rate is higher than expected. On the other hand, if InTP measures seem to solve all insider problems, or no insider incidents actually occur, management may also want to move InTP financial support to other activities. Finally, any way that the InTP appears to increase the liability of the organization, especially with regard to employment law, may discourage the support needed for effective InTP implementation.

Mitigation Discussion

Making sure that management remains aware of the importance of the InTP suggests tracking data to justify its continued operation:

> **Trends in incidents of concern:** Did the InTP identify this as a previously undetected concern? Did incident rates decrease after the InTP?
>
> **Cost avoidance:** Calculate the costs the organization avoided by using the average cost of damage by insider threat type (IT Sabotage, Fraud, IP Theft, Espionage, and Unintentional) multiplied by the number of incidents that were detected early or avoided.
>
> **Cost savings:** Compare the time, manpower, and costs of resolving incidents of employee misconduct prior to the InTP to those same costs after full deployment of the InTP.

Improving InTP performance requires fine-tuning alerts. While such fine-tuning is as much of an art as it is a science, there are approaches to ensure alerts are as accurate as possible, such as defining clear thresholds for alerting and reporting, clear requirements for incident identification (when an anomaly is officially declared), and clear procedures for incident response that include procedures that vet alerts against other data sources to establish reasonable suspicion that warrants further inquiry.

Although minimum standards for due care and due diligence are continually evolving in both the legal sense and the public opinion realm, insider threat programs can produce scenarios for leadership to consider, wherein the ignorance of insider threat scenarios would demonstrate an ineffective shield against lawsuits or negative public opinion. Remind leadership (perhaps as part of regular insider threat awareness training) of the cyclical nature of threats based on new hires, mergers/acquisitions, policy changes, etc. InTPs should remind leadership that the purpose of the insider threat program is not to “catch bad guys,” but to manage the risk to critical assets. Data that shows critical assets are proactively monitored and have been adequately protected can be a significant demonstration of both due care and due diligence.

Purposeful Misuse of InTPs by Its Staff or Others

Table 4: Unintended Consequences that Involve Purposeful Misuse of InTPs

4a. False Accusations Undermine the InTP.		
	Behavior	Employees use InTP reporting mechanisms to falsely report on other employees or force them out of the organization.
	Consequence	InTP staff time is wasted, confidence in the overall system is eroded, and lawsuits ensue.
	Mitigation Strategies	To the extent possible, establish the veracity of allegations before escalating and protect the identity of accused during the investigation.
4b. Abusive Staff Corrupt the InTP Function.		
	Behavior	InTP staff members use their power in the InTP to corrupt the InTP function for their own benefit (to hide bad activities or to punish others).
	Consequence	InTP staff time is wasted, confidence in the overall system is eroded, and lawsuits ensue.
	Mitigation Strategies	Enforce separation of duty and least privilege principles in InTP job functions. Hold InTP staff members accountable for their actions with investigation and adjudication by an entity independent of the InTP when needed.
4c. Anxious Employees Put up a Smokescreen.		
	Behavior	The InTP does not adequately inform or convince employees that its functions are not used for performance monitoring.
	Consequence	Employees falsely manipulate online profiles of activities to improve appearances.
	Mitigation Strategies	Regularly remind employees (possibly as part of insider threat training) of the responsibilities and limitations of the InTP with regard to monitoring and the use of the information collected.
4d. Opportunistic Managers Monitor Productivity.		
	Behavior	The InTP does not adequately separate its function from other performance monitoring activities.
	Consequence	Management uses the InTP as an unintended means of monitoring employee productivity.

	Mitigation Strategies	Formally restrict the scope of InTP operations to prevention, detection, and response to insider threat, and regularly remind employees (possibly as part of insider threat training) of the responsibilities and limitations of the InTP with regard to monitoring and use of the information collected.
4e. Overblown Threats Mis-prioritize Resources		
	Behavior	InTP staff exaggerate the scope of the insider threat to gain support.
	Consequence	Scarce resources could be better spent from the organizational perspective.
	Mitigation Strategies	Base the characterization and analysis of the organization's insider threat on reputable insider threat research, best practices, and industry-specific statistics.

The intended function of legitimate and necessary activities can be subverted by individuals who have other goals in mind. Table 4 describes ways that the InTP mission or the well-being of the organization and its employees can be purposely subverted by InTP staff or others. The InTP could be used by unscrupulous individuals to falsely accuse or hide the malicious activities of InTP staff members or fellow employees.

Targeting certain employees over others or using InTP functions for purposes other than those intended, such as monitoring employee productivity as general performance evaluation, is counter to effective InTP functioning. Employees who are suspicious of the InTP or the InTP staff may waste time manipulating their online profile to look good to InTP monitoring. This inappropriate monitoring could be particularly problematic if InTP investigations (appear to) negatively affect the future careers of employees, even when the investigations ultimately clear suspected individuals.

InTPs themselves may cause problems by exaggerating the insider threat faced by the organization to garner greater support, taking resources away from possibly more critical functions within the organization. We classify this last unintended consequence as purposeful if it involves outright misrepresentation or fraud. However, it is human nature to expound the benefits of one's work to others and the need for that work to justify the group's continued existence, so this unintended consequence could just as easily be accidental.

The unintended consequences in the InTP can trigger other consequences described previously that relate to worsening relationships among the InTP staff, management, and other employees.

Mitigation Discussion

The InTP may be purposely misused by employees, managers, or the InTP staff themselves.

Employees who misuse the InTP function to harm others are particularly disruptive. Each allegation should undergo an initial rigorous determination about the veracity of the claim. Only after veracity is established should supporting user activity data be reviewed to either support or refute the claim. In cases where veracity cannot be established, such as when reporting is made through totally anonymous means, the identity of the accused should be known only to the insider threat team that is reviewing data sources to support or refute the claim. In this way, knowledge of the allegation and the identity of the accused are not known outside of the insider threat program unless the allegation is supported by validated insider threat data.

InTP staff who purposely misuse the InTP function for their own benefit undermine the very foundations of the program. All allegations or suspicions of abuse of power by staff should be immediately referred to an independent organizational entity (one not part of the insider threat program) for investigation and adjudication. Separation of critical tasks and duties in the InTP, along with rigorous auditing of all insider threat program functions, will help mitigate misuse by InTP staff. For example, staff who deploy monitoring policies should not be the ones that review the data collected by those policies and vice-versa. In addition, auditors should not have the authority to employ policies or review data collections. Only auditors should be able to configure and review auditing policies and data.

Finally, clear and detailed mission, charter, and operating procedures for the insider threat program can help avoid inappropriate requests by managers. For example, requests by managers for badge access reports to establish time and attendance of their employees could be redirected to Human Resources/Human Capital for appropriate action since that request would not be a mission (or in the charter) of the Insider Threat Program.

Accidental Misuse of InTPs by Its Staff or Others

Table 5: Unintended Consequences that Involve the Accidental Misuse of InTPs

5a. Inconsistent Execution Breeds Unfairness.		
	Behavior	The InTP inconsistently enforces insider threat related policies.
	Consequence	The organization violates HR employment laws or employee privacy rights; lawsuits ensue.
	Mitigation Strategies	Clearly define and document insider threat related policies, and have an independent entity regularly audit and evaluate InTP processes for adherence.
5b. Investigations Unfairly Affect Employees' Careers.		
	Behavior	The InTP investigates unfounded suspicions of employees.
	Consequence	Stigma/records associated with InTP investigations negatively affect an employee's future career.
	Mitigation Strategies	To the extent possible, establish the veracity of allegations before escalating, and protect the identity of accused during the investigation.
5c. InTP Detection Allows Accidental Disclosure.		
	Behavior	InTP staff accidentally review protected artifacts while trying to detect or respond to insider threats.
	Consequence	Unauthorized disclosure of sensitive information occurs.
	Mitigation Strategies	Educate the InTP staff about which artifacts to ignore during investigations, and establish procedures for notifying data owners and for using non-disclosure agreements in cases of the accidental disclosure of sensitive information.

Some misuse of the InTP function can be accidental in nature as illustrated by the unintended consequences listed in Table 5. These accidents may lead to violations of HR employment laws or accidental disclosure of confidential information as part of the InTP detection function. A side effect of InTP investigations might include harm to the reputation or career of someone who was under suspicion, but later cleared, of an illicit act.

Mitigation Discussion

While the consistency of policy enforcement can be mitigated through well-documented policies and independent auditing, a more thorough examination can employ a type of separation of critical tasks. For example, after one team member or members investigate the anomaly or allegation, a completely separate member researches how the organization has addressed similar incidents in the past. The findings from both teams can be presented to a third member (not involved in either evidence gathering or researching prior incidents) for development of mitigation recommendations. The mitigation recommendations can then be provided to an adjudication council that weighs the facts, how the organization has previously handled similar incidents, and the mitigation recommendations from the uninvested third party to make an official disposition.

To mitigate the potential for investigations to unfairly affect careers, all allegations should undergo an initial rigorous determination about the veracity of the claim. Only after veracity is established, should supporting user activity data be reviewed to either support or refute the claim. In cases where veracity cannot be established, such as when reporting is made through totally anonymous means, the identity of the accused should be known only to the insider threat team that is reviewing data sources to support or refute the claim. In this way, knowledge of the allegation and the identity of the accused are not known outside of the insider threat program unless the allegation is supported by validated insider threat data.

Insider threat programs should also consider establishing formal “taint” procedures to mitigate inadvertent exposure to sensitive information. Some examples of these procedures might include the following:

- A formal recusal process, whereby the individual exposed is identified as recused from future proceedings associated with the sensitive data or individual in possession of the data.
- A signed, specific non-disclosure acknowledgement by the team member exposed to the sensitive data.
- Notification of one or more of the parties that own the sensitive data. For example, upon accidental disclosure, the InTP staff could notify legal counsel that a legal work product was inadvertently exposed to a member or members of the insider threat team and then implement agreed upon mitigation procedures.

FEEDBACK AND EXTENSION OF NEGATIVE UNINTENDED CONSEQUENCES

We conducted two sessions to get feedback on our initial set of negative unintended consequences: one internal and one external to the Software Engineering Institute (SEI). In this section, we describe the conduct of and conclusions from these sessions.

Internal Feedback from the Insider Threat Team

The internal SEI session was conducted with eight members of the SEI staff. We described the initial set of potential negative unintended consequences and solicited ideas for others that participants thought were important for organizations to consider. Seven additional potential consequences were identified in these discussions:

- 2e. The InTP Inhibits Employee Reporting.
- 2f. Early Suspicions Bias Investigations.
- 3e. Apparent Success Diminishes the Perceived Need.
- 4e. Overblown Threats Mis-prioritize Resources.
- 5b. Investigations Unfairly Affect Employees' Careers.
- 5c. InTP Detection Allows Accidental Disclosure.

These additions were included in the tables outlining the consequences in the previous section, but due to time limits, we did not include them in participant voting that occurred at the end of the meeting.

Participants voted for the consequences that they thought presented the biggest risk to organizations in terms of both the likelihood of occurring and the severity if they did occur. A multi-voting (or N/3 voting) scheme was used in which each participant had a number of votes to place on any number of the consequences. They could place all of their votes on one consequence or distribute them more evenly. Since there were 15 items in the initial voting pool, each participant got 15/3 or 5 votes, as is commonly accepted practice for multi-voting.

The results of the voting are shown in Figure 1. While this vote was just an informal exercise, it is instructive to look at this initial response. The participants definitely favored certain consequences over others. Over a quarter of the consequences (4/15) received no votes. Over half of the consequences (8/16) received one vote. There was one consequence that received two votes and one that received three. A quarter of the consequences received four votes and one received five votes.

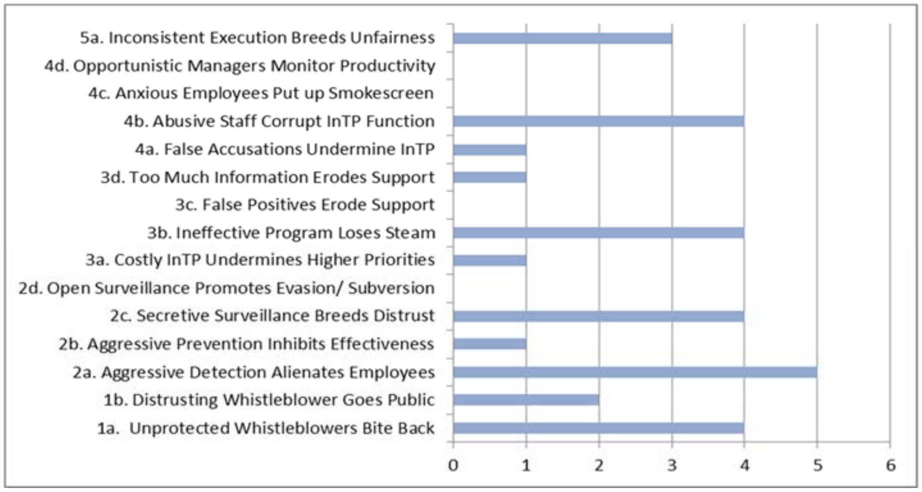


Figure 1: Voting Results on the Initial Set of Unintended Consequences

The consequences that received four or five votes were

- 1a. Unprotected Whistleblowers Bite Back.
- 2a Aggressive Detection Alienates Employees.
- 2c. Secretive Surveillance Breeds Distrust.
- 3b. An Ineffective Program Loses Steam.
- 4b. Abusive Staff Corrupt the InTP Function.

These voting results do not suggest that the other consequences should not be considered, but rather that the consequences with highest votes should be considered first. Interestingly, each of the four consequence groupings has one consequence with four votes, with group 2 also having a consequence with five votes. We believe these voting results provide prima facie evidence that the initial grouping was a reasonable breakdown. Of course, future work will continue to elaborate these potential negative consequences and assess both their likelihood and severity. Discussions with larger audiences of InTP operational staff will also help establish more evidence for prioritization of the consequences along with stories told by organizations in which the consequences have arisen.

External Feedback from InTP Manager Training

In the first week of September 2014, the CERT Division of the SEI provided the *Insider Threat Program Manager Certificate: Implementations and Operations Course*. Module 17 of that course, “Considerations When Standing up an InTP,” presents each of the four consequence groupings as a student discussion topic to raise understanding of the potential for an InTP to go wrong, to talk about programs’ experiences with the potential consequences, and to assess organizational concern over the possibility. (The slides for Module 17 are provided in Appendix B.)

The discussion in the course was more free form than our internal discussion, with less definite conclusions or additions to the set of negative unintended consequences. There were clear differences between the view of an InTP in the U.S. Government and U.S. Government contractors, on one hand, and non-government industry on the other.

U.S. Government organizations (and possibly U.S. Government contractors in the future[1]) that handle classified information have a mandate, per Executive Order 13587, to have an InTP in place. These organizations must call it an InTP to satisfy the mandate and get any funding that comes with implementing that mandate. Employees with clearances are used to monitoring their actions and have agreed to that monitoring as a condition of their access. Participants in or associated with the U.S. Government did not express much concern about disrupting relationships between personnel or the morale of personnel due to the existence or function of the InTP.

Non-government industry, on the other hand, was much more concerned about the effects of the InTP on employee morale. They had serious reservations about the very name “Insider Threat Program” because of its potential to alienate the workforce. Other names—such as “asset protection program”—were viewed much more favorably. While organizations associated with the U.S. Government are concerned about classified information, non-government industry was concerned about the organizations intellectual property, the loss of which could severely reduce its competitive advantage. If the InTP in non-government industry are not shown to be effective against the theft of IP and/or strained the working relationships among its employees, management may lose much of their incentive to support the InTP.

All of the participants seemed to recognize the value of an official whistleblower process within organizations separate from the InTP. The discussion seemed to create greater awareness for understanding that these two programs are separate and distinct. Participants also recognized the need to be careful about when employee behaviors are associated with an official whistleblower process versus potentially malicious behavior that needs to be reported as part of an InTP function.

[1] U.S. Government contractors will be required to follow EO 13587 if Confirming Change 2 to the National Industrial Security Program Operating Manual (NISPOM) is accepted, which is anticipated in 2015.

Many participants agreed that it is a good idea to publish InTP successes so that employees understand the value of having an effective InTP that employees and managers support.

AN EXAMPLE ARCHETYPE SPECIFICATION

Similar to the way Peter Senge, in his book *The Fifth Discipline*, applies system thinking to elaborate recurring problems of organization management, we can elaborate an InTP archetype using *causal loop diagrams* to describe potential unintended consequences [Senge 1990]. This approach has been applied before at the SEI in the development of a comprehensive set of software acquisition archetypes that characterize recurring problems in DoD software-intensive system acquisition identified through years of study and analysis in independent technical assessments (ITAs) of troubled acquisition programs [Novak & Levine 2010]. Insider threat program archetypes can help establish a set of principles by which organizations can develop InTPs that balance the organization's need to achieve its mission with its need to be vigilant to insider threats. This section elaborates an InTP archetype associated with the negative unintended consequence (4f.) of InTPs: *Investigations Unfairly Affect Employees' Careers*.

Archetype: Investigations Unfairly Affect Careers

This archetype involves the situation in which an investigation of unfounded suspicions of an employee negatively affects that employee's future career. The archetype elaborates a fictional but representative story in which the problematic consequence occurred, and includes a discussion of the big-picture dynamic involved, a causal loop representation of that dynamics, and a description of some general techniques for breaking the pattern.

The Archetypal Story

Cloud of Suspicion

The Counter-Intelligence (CI) team at a classified government agency site received a strong warning from the FBI that they had credible source information that one of the employees at the site was a spy who had been operating for a foreign intelligence service for many years. The CI team took the warning very seriously and, as part of the investigation, needed to ensure they could collect information to support or refute the allegation in a way that protected national security information as well as the privacy and civil liberties of the subject and the other employees in the facilities. To do that, the CI team explained to the site manager, a senior executive in the organization, the allegation and the special investigative techniques that would be employed in accordance with a federal court order. It just so happened that the individual they were investigating was one of the site manager's deputies.

Star Performer

The CI team began by meeting with the site manager, a brusque and straight-shooting military officer, to ask about the performance and character of the subject. The site manager reported that the deputy in question was his best guy, someone who had always been very sharp, had great attention to detail, and who was used for the hardest projects—a model employee who received consistently high performance appraisals and merit bonuses during his three years on assignment working for the site manager. The CI team explained the allegation made against the deputy and that they would need to operate covertly within the facility during the period of the investigation. The CI team needed the site manager to provide confirmation for a cover story about who the CI team was and what kind of work they were doing at the site. The team also needed a way to enter and exit the facility without being observed. The site manager agreed reluctantly, incredulous that his star performer was under suspicion.

Change of Heart

The investigation was thorough, lasting more than eight months. Despite the "close in" nature of the investigation, the employee never became aware that he had been under suspicion. At the end of it, even though the allegation had come from what was believed to be a very credible source, the FBI and the CI team determined that the original allegation had been false. Such an outcome is not uncommon for such investigations since even a good source can provide large amounts of good data that may be sprinkled with false information.

They reported their negative finding back to the site manager, glad to be delivering good news about his star deputy, and told him that everything could return to normal. To their surprise, however, the site manager wasn't that pleased by the news and said he was hoping that this deputy would choose to leave the organization soon as he no longer felt that the deputy was reliable. The CI team didn't understand the site manager's apparent change of heart toward his deputy in light of the original allegation being proved untrue. As far as they'd been able to determine, there was no adverse change in the individual's behavior or performance during the period of the investigation.

The only thing that changed was the site manager's perception of the individual's worth to him and the organization. The manager apparently believed that for the allegation to have been made, there must be something there, despite the investigation's results. The manager didn't seem to realize that he was being unfair to the employee and, when asked about it, only said that he might have been "too nice" in his first description of the employee's qualities. Despite his reputation for forthrightness, the site manager tried to "walk back" many of his original comments to minimize the disparity between them and his current view of the individual.

The Bigger Picture

We know intuitively that once someone is thought to have violated a trust, it's difficult to trust them again. Ideally, we shouldn't care if someone is suspected, but later acquitted. However, it's still difficult for a politician to be elected once they've been indicted in a corruption investigation. The trust relationship in a work environment—especially one involving high levels of trust due to critical security concerns—develops slowly over time, but is still fragile and can be damaged or destroyed if the people involved are presented with even an unproven suspicion that one of their colleagues may be engaging in espionage.

In addition, when a person feels betrayed by another, they feel not only anger, but also embarrassment at having been duped. These feelings therefore become an important issue for the manager to resolve in his or her mind. It is, of course, human nature to give too much credence to negative information like suspicions, even when they're unsupported. This new negative information from the investigators becomes unconsciously fixed (as an anchor) in the manager's mind, and difficult to change.[2]

As people develop a theory of how events could have unfolded—such as a colleague or employee acting as a spy—the anchor remains fixed in their mind, having changed their previous perspective, and now limits their ability to change or adjust this anchored impression. As they look for additional data relating to their

[2] This is an example of a concept called *anchoring* [Tversky 1974]. In anchoring, people make incremental adjustments to the initial impression (the anchor) based on additional information, which is usually insufficient to change it significantly. These adjustments give the anchor inordinate weight. In addition, research has shown that it is quite common for people to assign more weight to negative information than to positive information about others (the *negativity effect*) [Vonk 1993].

theory, they have a strong tendency to focus on data that confirms their theory, to the exclusion of other (especially exculpatory) information.[3]

The manager's negative focus is worsened because he or she is obligated to keep suspicions to themselves, with no one available to balance or refute them. Furthermore, distrust increases with the magnitude of the violation and the perception that the offender intended to commit the violation. Given time, this "echo chamber" effect can grow even small suspicions into deep distrust. Already hurt by the initial perceived betrayal, the manager may now take steps to reduce his or her vulnerability to a possible bad outcome of the investigation, which can manifest as distancing themselves from the employee.

Model of Dynamic

The causal loop diagram, in Figure 2, provides one explanation of the dynamic that played out in this narrative.[4] Figure 2 presents three loops of the narrative, described in the following:

- **Manager-Employee Relationship:** Before the incident that triggered the investigation occurred, there was an ongoing positive reinforcing loop in the relationship between the manager and the employee. The manager trusts the employee, and so rewards the employee for his or her efforts. In return, the employee trusts the manager for being treated fairly, and therefore continues to perform well, showing his or her capability back to the manager. This relationship persists in an ongoing cycle as trust in one another continues to build—potentially over a period of years.

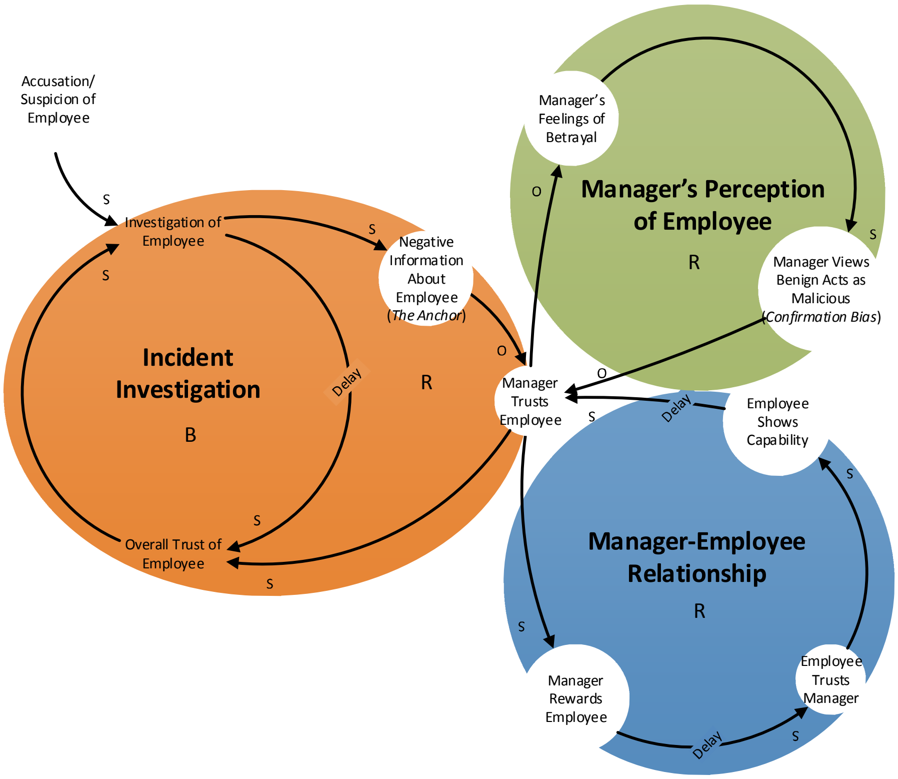
- **Incident Investigation:** When an accusation is made against the employee, or the employee comes under suspicion for some reason, an investigation of the employee is initiated. This investigation takes some time to conduct. In this case, as in many such investigations, the outcome is that the employee is found to be innocent of the suspicion. However,

[3] This is an example of *confirmation bias*, which is another cognitive bias that inappropriately influences decisions [Nickerson 1998]. In trying to make sense of the employee's likely benign actions (e.g., working late or on weekends), they may find a way to interpret those actions negatively, and thus see the suspicious activities that they believed to be there. As an example, think of a person who has been told their spouse may be unfaithful. The spouse's seemingly benign behavior of "working late" that previously drew little attention may now become a key cause for concern.

[4] Additional research is needed to confirm the accuracy of this explanation. See the scientific study proposed in the Summary and Future Directions section of this paper.

before the investigation can conclude and clear the employee, another dynamic begins. If the manager becomes aware of the allegations that have been made against the employee, this negative information—albeit unconfirmed—forms a (negative) anchor in the manager's mind, harming his or her level of trust in the employee.

- **Manager's Perception of Employee:** The manager's natural reaction to this information is to feel betrayed by the employee's alleged behavior—especially in light of the trust that has been placed in him or her, which has grown over time. These feelings of injury, in turn, cause the manager to very carefully observe the employee's actions and to mentally review past actions, interpreting them now through a suspicious lens. This is confirmation bias in action. The result is that even benign behaviors now fall "under a cloud" of suspicion, and the result is a decrease in the manager's trust of the employee.



Accusation/ Suspicion of Employee
S
Investigation of Employee
S
Negative Information About Employee (*The Anchor*)
S
Incident Investigation
B
Delay
R
O
S
Overall Trust of Employee
S
Manager's Feelings of Betrayal
O
Manager's Perception of Employee
R
S
Manager Views Benign Acts as Malicious (*Confirmation Bias*)
O
Manager Trusts Employee
S
Delay
Employee Shows Capability
S
Manager-Employee Relationship
R
S
Manager Rewards Employee
Delay
S
Employee Trusts Manager

Figure 2: The Dynamic that Played out During the Archetypal Story[5]

The manager’s biased perception of the employee’s behavior reverses the positive reinforcing loop of the manager-employee relationship, setting it on a cycle of declining trust. The initially positive effect of the Manager-Employee Relationship loop is overwhelmed, or dominated, by the negative effects of the Manager's Perception of Employee loop that has been set in motion by the investigation. This is known as “shifting loop dominance,” where the dominant behavior shifts from one loop to another, tipping the balance of the dynamic. By the time the investigation concludes and the employee is cleared of suspicion, the manager has already stopped trusting the employee who was formerly viewed in a positive light. The fact that the investigation has cleared the employee’s name is no longer relevant given the changed relationship between the employee and the manager.

Breaking the Pattern

Unfortunately, in the instance of a trusted insider employee who comes under suspicion, the employee can do little if anything to regain trust because they are likely to be unaware that trust has been lost. They may see the outward manifestations of this loss of trust in others who are secretly aware of the suspicion, but they will not know its source.

The standard advice about rebuilding trust—that the person in whom trust has been lost must gradually and incrementally prove that they can be trusted again—does not apply here. Regaining lost trust is difficult at best, but becomes almost impossible when the loss of trust is undeserved and unjustified. The manager feels betrayed by the employee and, when that sense of betrayal starts to become apparent to the employee, the employee will then feel betrayed by this seemingly inexplicable change. Neither individual caused the loss of trust so neither one feels responsible for trying to restore it.

Furthermore, even if the employee wanted to, he or she can’t demonstrate trustworthiness to rebuild trust—all he or she can prove is that others are no longer able to detect any espionage. Once a manager has suspected an employee of a violation, the manager will be reluctant to ever give the employee a good review

[5] In causal loop diagrams, variables affect each other in the following manner: S indicates that variable values move in the same direction; O indicates that variable values move in opposite directions. Feedback loops labeled with “R” (for reinforcing) describe aspects that tend to drive variable values consistently upward or downward. Feedback loops labeled with “B” (for balancing) describe aspects that tend to drive variables to some goal value [Meadows 2008].

or promotion, worrying that he or she may be giving a potential criminal a top rating.

Since it is so difficult to re-establish trust that has been lost in a colleague, it is critical to avoid damaging that trust in the first place. Some key preventive steps that could be taken are

- Very few in the workplace other than the investigators themselves should be aware of the investigation—and especially not the target's colleagues or management chain. This best practice exists in many organizations that regularly conduct internal investigations and there are many methods used to disguise the fact that an individual is being investigated, such as
    - including the names of multiple randomly selected individuals (referred to as "padding") when requesting data to disguise the name of the individual under scrutiny
    - routinely requesting a number of personnel files each week to establish a pattern of a normal business process that avoids alerting people when there is an actual investigation in progress
    - having direct access to any records that may be required so that others in an administrative capacity do not become aware of the target of the investigation through record requests
- It's essential to thoroughly vet an accusation being brought against an employee before triggering an investigation. Given the damage that can be done to the employee's reputation, and consequently to the organization's morale and productivity, every effort should be made to determine the veracity of the accusation prior to beginning an investigation.
- There are also some methods suggested in the literature to combat the anchoring and confirmation bias that underlies the dynamic in play in this archetype [Kahneman 2011], for example, having managers explicitly consider both positive and negative reasons for employee behaviors. Perhaps most importantly, if managers must be informed about an investigation, for whatever reason, they should be warned in advance about the dangers of misinterpretation of events due to the potential for anchoring and confirmation bias.

SUMMARY AND FUTURE DIRECTIONS

This paper describes the results of a short-term (two-month) effort to elaborate potential negative unintended consequences of organizations' efforts to establish and execute an insider threat program. Widespread effort to establish such programs is a recent phenomenon and, as such, there is not yet a lot of data on how the programs can go wrong. The purpose is to get ahead of the game—to make sure that we've at least thought about problems that could occur and to use this information to create balanced strategies for designing and implementing programs that have a greater chance of success.

The progress so far is just a first step. As organizations continue designing, implementing, and executing InTPs, more data will become available about the concerns of organizations and actual problems that occur during execution. This data can be fed back into the enumeration and refinement of the consequences, including more stories validating their likelihood and severity. Some consequences will likely be "weeded out" and others added that we have not thought of yet. Validation of consequences justifies more effort in their elaboration, including structured analysis of the circumstances surrounding the problem and the range of mitigations (e.g., as a full-fledged archetype with causal loop diagram as shown in Section 4). The range of InTP courses and instructional materials offered by the CERT Division can then be updated in light of this information. The taxonomy that we started in Appendix A can also be refined.

We propose both opportunistic data collection as well as a more formal, scientific study:

Opportunistic Data Collection: We propose continuing to use CERT insider threat training as a vehicle to engage with the community about their concerns and experiences with establishing InTPs. Clearly, the U.S. Government and its contractors have different perspectives that will need to be considered. Presenting at the RSA Conference also could be used to collect data from the broader community.

Scientific Study: While the U.S. Government mandate for organizations handling classified information to establish InTPs is fairly recent, a small cadre of organizations have relatively mature programs that have been operating for years. A carefully crafted survey or face-to-face interview of these organizations could help provide scientific evidence for the likelihood and severity of the consequences as well as elaborating measures that have proven effective at mitigating them. Precedent for a scientific analysis of problematic organizational behavior can be found in the MIT study of software acquisition archetypes, *An Examination of the Patterns of Failure in Defense Acquisition Programs* [McNew 2011]. Extension of the goals of such a study could and probably should include analysis of the aspects of InTPs that work well—resulting in a kind of best-of-class analysis of InTPs. Possible funding sources for such a project include the Intelligence and National Security Alliance, The National Counter Intelligence Executive, and SEI internal research funding.

We would also like to continue developing the archetype descriptions as shown in Section 4. These descriptions can be very valuable to help organizations understand

- what can go wrong
- how it goes wrong
- what to watch for to determine whether it is going wrong
- what to do about it

The last of these—mitigations to the problematic behavior—can be difficult to determine, but may arise as a result of the discussions and studies proposed above. Of course, these kinds of problematic organizational behaviors are not unique to InTPs. For example, the internal audit function within organizations can create tensions between the internal audit team and the rest of the organization similar to the tensions possible for the InTP function. Mitigations that are now being tried as part of internal audits—such as having audit team members be part of the IT operations staff, having IT staff members rotate through the internal audit function, and having IT staff members self-assess their IT operations—may be useful in reducing the negative unintended consequences of the InTP [Anderson 2009]. Additional study is needed to determine the effectiveness and applicability of these mitigations.

ACKNOWLEDGEMENTS

We would like to thank Rich Caralli and Summer Fowler for their help in the original motivation, structuring, and design of the work performed here. We also thank participants in the brainstorming and review session—Sam Perl, Dan Costa, Robin Ruefle, Mark Zajicek, and Bill Claycomb (all from the CERT Division of the SEI)—for their insights and additions to the growing list of potential unintended consequences. Finally, we thank Sandy Shrum for her excellent technical editing of this paper.

REFERENCES

Kahneman, D. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Meadows, D. (2008). Thinking in Systems: A Primer. White River Junction, VT: Chelsea Green Publishing.

McNew, G. J. *An Examination of the Patterns of Failure in Defense Acquisition Programs*. Massachusetts Institute of Technology, 2011. (http://hdl.handle.net/1721.1/67565)

Nickerson, R. S. Confirmation bias: A ubiquitous phenomenon in many guises. Review of general psychology, 2(2), 175, 1998.

Novak, W. E., & Levine, L. *Success in Acquisition: Using Archetypes to Beat the Odds*. Software Engineering Institute, Carnegie Mellon University, 2010. (http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9519)

Senge, P. *The Fifth Discipline: The Art and Practice of the Learning Organization*. Doubleday/Currency, 1990. (http://infed.org/mobi/peter-senge-and-the-learning-organization/)

Tversky, A.; Kahneman, D. "Judgment under Uncertainty: Heuristics and Biases". *Science* 185 (4157): 1124–1131, 1974.

Vonk, R. “The Negativity Effect in Trait Ratings and in Open-Ended Descriptions of Persons". *Personality and Social Psychology Bulletin* 19: 269-278, 1993.

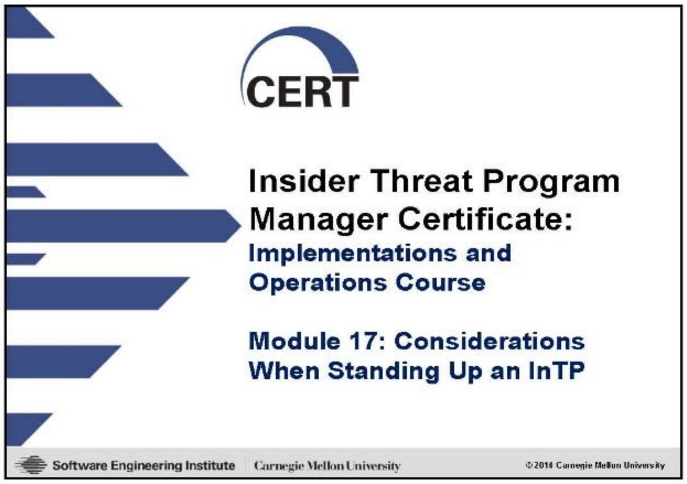
Anderson, U. *Assurance and Consulting Services*. “Chapter 4 Assurance and Consulting Services,” Institute of Internal Auditors Research Foundation, 2003. (https://na.theiia.org/iiarf/Public%20Documents/Chapter%204%20Assurance%20and%20Consulting

APPENDIX A: INITIAL TAXONOMY OF INTP POTENTIAL UNINTENDED CONSEQUENCES

- Behaviors
  - Purposeful/Deliberate/Intentional (Malicious?)
    - Misuse/Abuse of InTP by InTP Staff
      - Abusive Staff Corrupt InTP Function
    - Misuse/Abuse of InTP by non-InTP Managers/Employees
      - False Accusations Undermine InTP
      - Opportunistic Managers Monitor Productivity
  - Unintentional/Innocent
    - Business Management
      - Costly InTP Undermines Perceived Higher Priorities
      - Ineffective InTP Program Loses Steam
      - False Positives Erode Support
      - Too Much Information Erodes Support
      - Apparent Success Diminishes Perceived Need
    - Employees/Managers
      - Fear/Distrust of InTP (This is a consequence of some other cause)
        - InTP Inhibits Employee Reporting (*Passive*)
        - Anxious Employees Put Up Smokescreen (*Active*)
        - InTP Inhibits Whistleblowing
        - Distrusting Whistleblower Goes Public
    - InTP Staff
      - Overly aggressive
        - Aggressive Detection Alienates Employees
        - Aggressive Prevention Inhibits Performance
        - InTP Detection Allows Accidental Disclosure
        - Investigations Unfairly Affect Careers
        - Unprotected Whistleblowers Bite Back
      - Secretive or Deceptive (i.e., use of a “honeypot”)
        - Secretive Surveillance Breeds Distrust
      - Overly transparent (InTP actions are obvious)
        - Open Surveillance Promotes Evasion/Subversion
        - InTP Response Reveals Strategy
      - Inconsistent InTP Execution
        - Inconsistent Execution Breeds Unfairness
- Consequence
  - Program Deemed Successful
    - Needs to continue
    - Should be terminated
  - Program Deemed Unsuccessful
    - Should be terminated

APPENDIX B: COURSE SLIDES

These slides were presented as part of the *InTP Managers Training Course* regarding InTP potential unintended consequences.



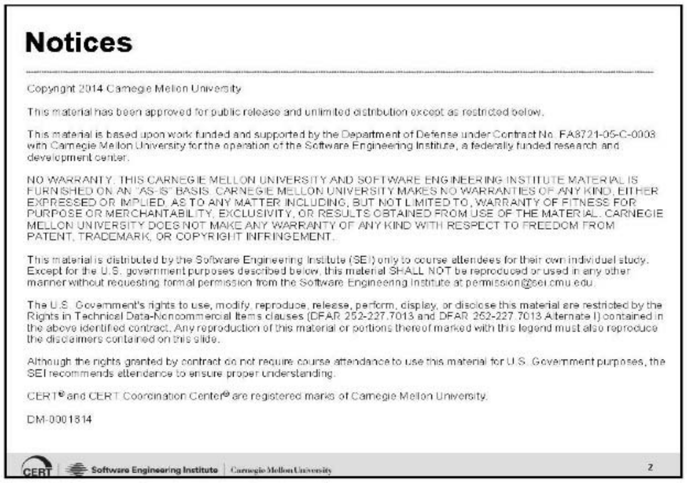
CERT

Insider Threat Program Manager Certificate:

Implementations and Operations Course

Module 17: Considerations When Standing Up an InTP

Software Engineering Institute | Carnegie Mellon University ©2014 Carnegie Mellon University



Notices

Copyright 2014 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

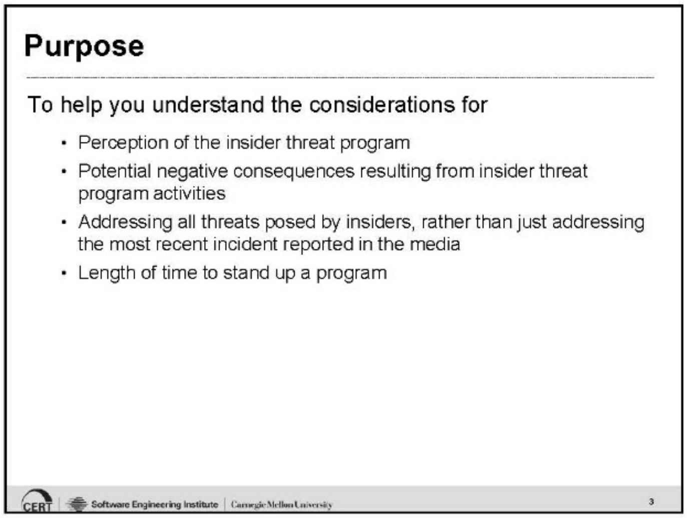
The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0001814

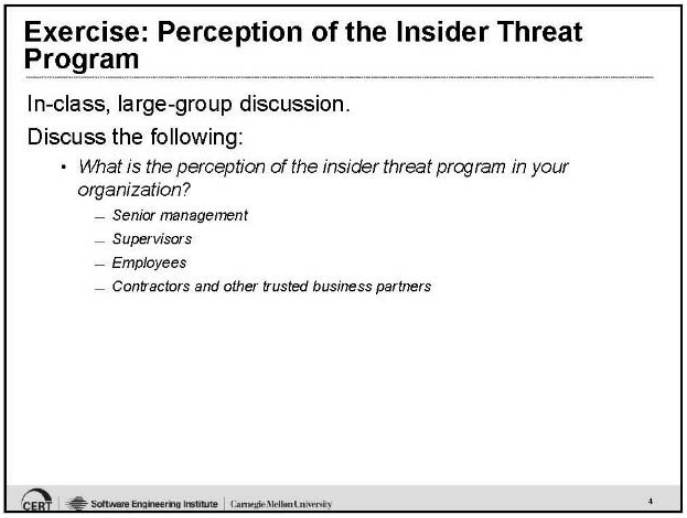
CERT | Software Engineering Institute | Carnegie Mellon University 2



Purpose

To help you understand the considerations for

- Perception of the insider threat program
- Potential negative consequences resulting from insider threat program activities
- Addressing all threats posed by insiders, rather than just addressing the most recent incident reported in the media
- Length of time to stand up a program

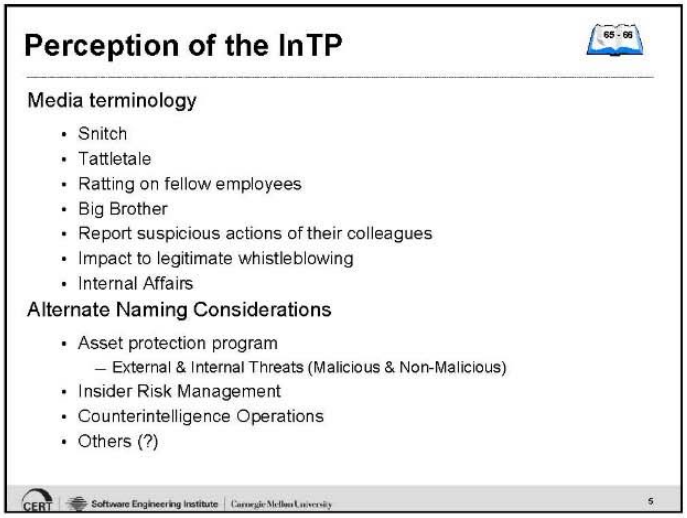


Exercise: Perception of the Insider Threat Program

In-class, large-group discussion.

Discuss the following:

- *What is the perception of the insider threat program in your organization?*
  - *Senior management*
  - *Supervisors*
  - *Employees*
  - *Contractors and other trusted business partners*



Perception of the InTP

65 - 66

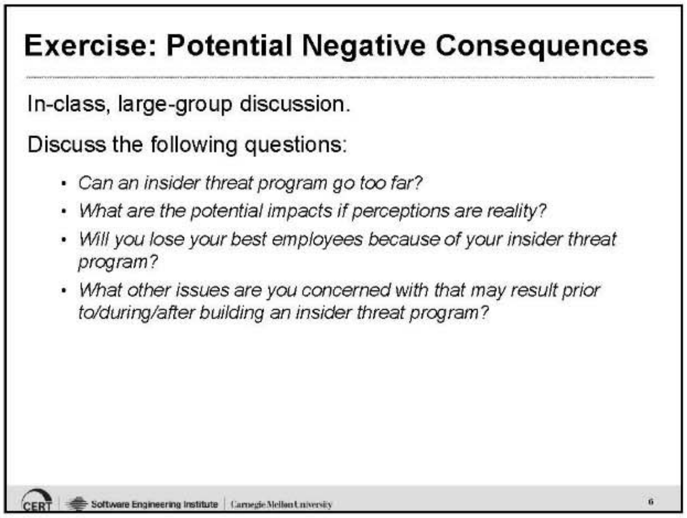
Media terminology

- Snitch
- Tattletale
- Ratting on fellow employees
- Big Brother
- Report suspicious actions of their colleagues
- Impact to legitimate whistleblowing
- Internal Affairs

Alternate Naming Considerations

- Asset protection program
  - External & Internal Threats (Malicious & Non-Malicious)
- Insider Risk Management
- Counterintelligence Operations
- Others (?)

CERT | Software Engineering Institute | Carnegie Mellon University 5



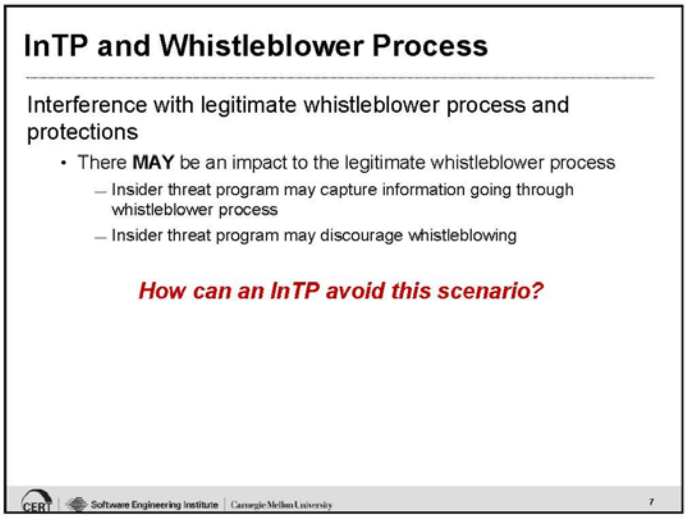
Exercise: Potential Negative Consequences

In-class, large-group discussion.

Discuss the following questions:

- *Can an insider threat program go too far?*
- *What are the potential impacts if perceptions are reality?*
- *Will you lose your best employees because of your insider threat program?*
- *What other issues are you concerned with that may result prior to/during/after building an insider threat program?*

CERT | Software Engineering Institute | Carnegie Mellon University 6

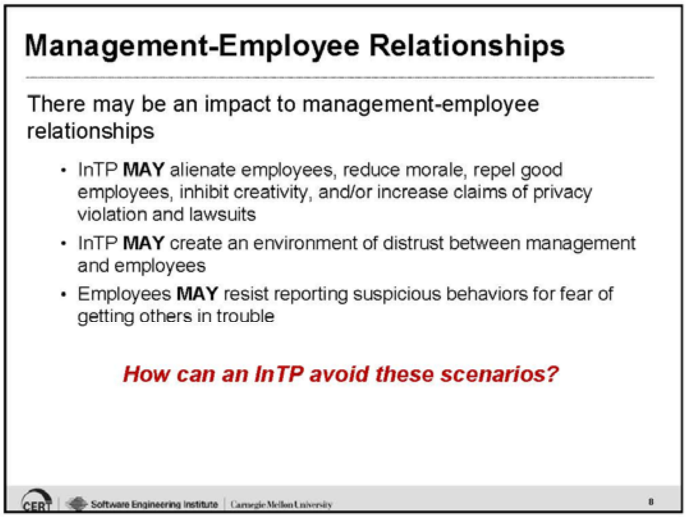


InTP and Whistleblower Process

Interference with legitimate whistleblower process and protections

- There **MAY** be an impact to the legitimate whistleblower process
  - Insider threat program may capture information going through whistleblower process
  - Insider threat program may discourage whistleblowing

How can an InTP avoid this scenario?

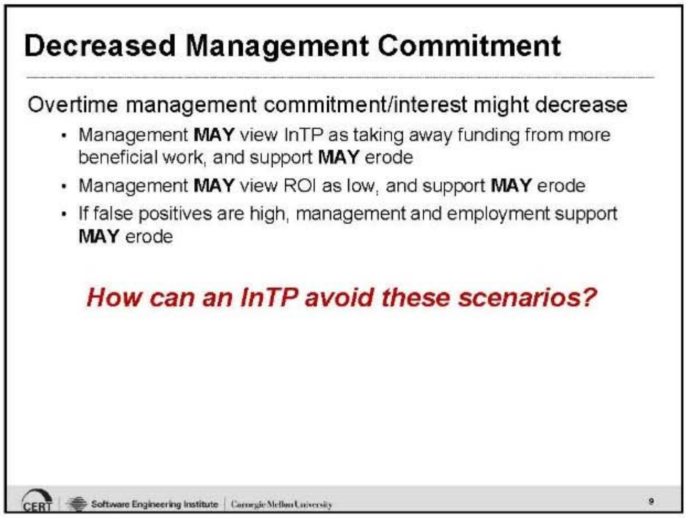


Management-Employee Relationships

There may be an impact to management-employee relationships

- InTP **MAY** alienate employees, reduce morale, repel good employees, inhibit creativity, and/or increase claims of privacy violation and lawsuits
- InTP **MAY** create an environment of distrust between management and employees
- Employees **MAY** resist reporting suspicious behaviors for fear of getting others in trouble

How can an InTP avoid these scenarios?

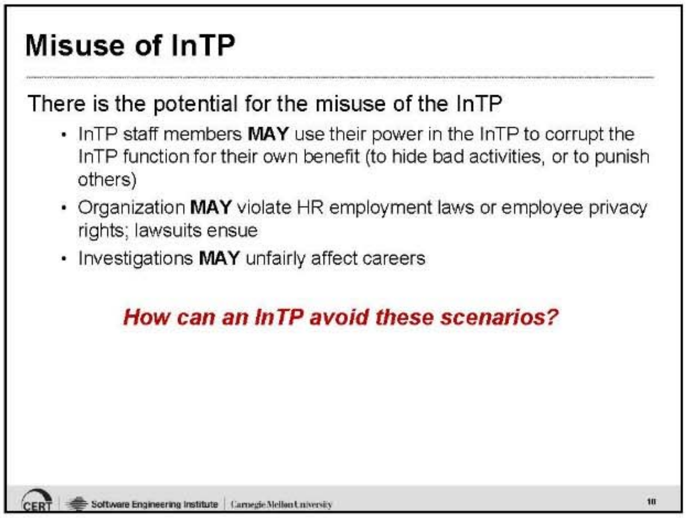


Decreased Management Commitment

Overtime management commitment/interest might decrease

- Management **MAY** view InTP as taking away funding from more beneficial work, and support **MAY** erode
- Management **MAY** view ROI as low, and support **MAY** erode
- If false positives are high, management and employment support **MAY** erode

How can an InTP avoid these scenarios?

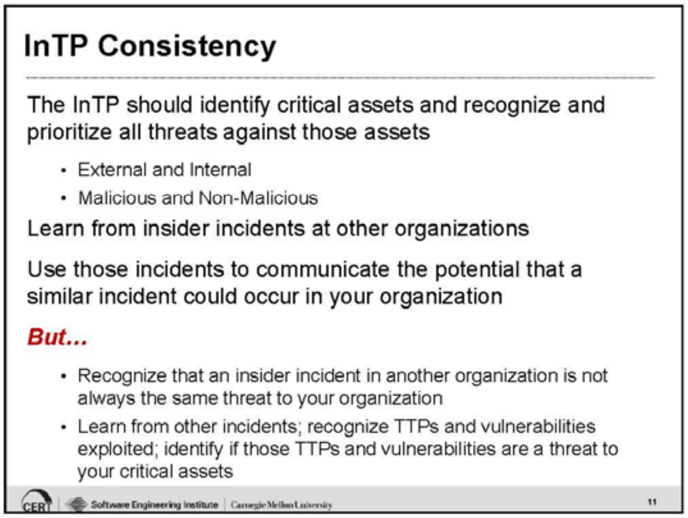


Misuse of InTP

There is the potential for the misuse of the InTP

- InTP staff members **MAY** use their power in the InTP to corrupt the InTP function for their own benefit (to hide bad activities, or to punish others)
- Organization **MAY** violate HR employment laws or employee privacy rights; lawsuits ensue
- Investigations **MAY** unfairly affect careers

How can an InTP avoid these scenarios?



InTP Consistency

The InTP should identify critical assets and recognize and prioritize all threats against those assets

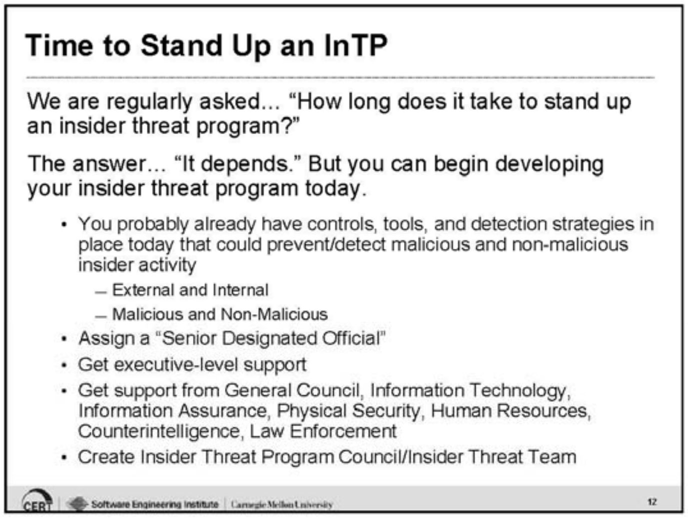
- External and Internal
- Malicious and Non-Malicious

Learn from insider incidents at other organizations

Use those incidents to communicate the potential that a similar incident could occur in your organization

But…

- Recognize that an insider incident in another organization is not always the same threat to your organization
- Learn from other incidents; recognize TTPs and vulnerabilities exploited; identify if those TTPs and vulnerabilities are a threat to your critical assets

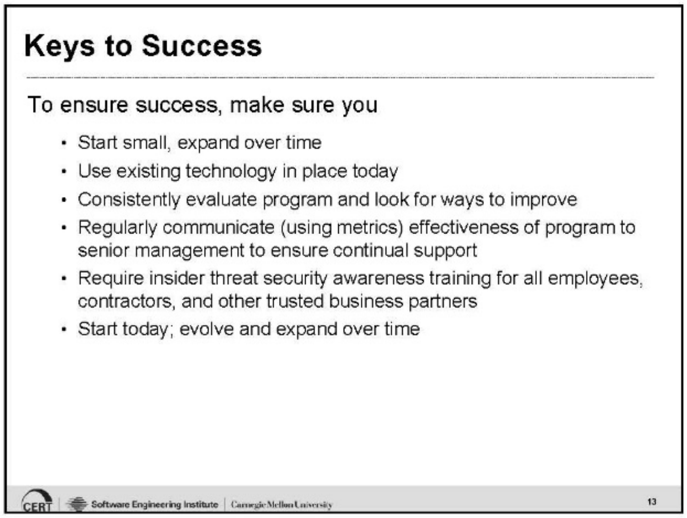


Time to Stand Up an InTP

We are regularly asked… "How long does it take to stand up an insider threat program?"

The answer… "It depends." But you can begin developing your insider threat program today.

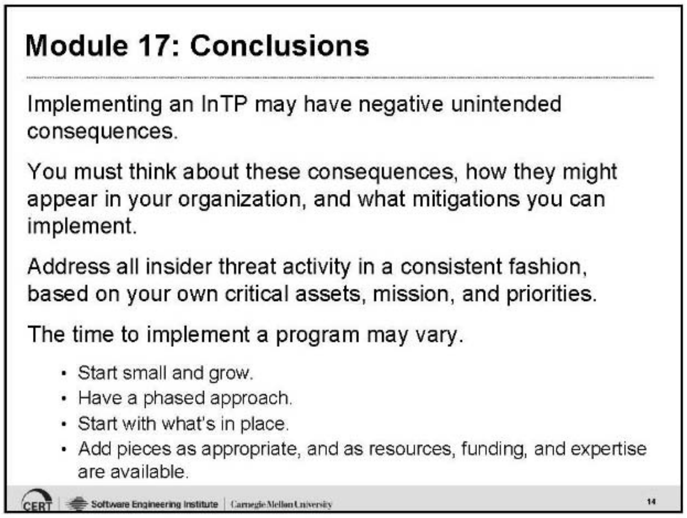
- You probably already have controls, tools, and detection strategies in place today that could prevent/detect malicious and non-malicious insider activity
  - External and Internal
  - Malicious and Non-Malicious
- Assign a "Senior Designated Official"
- Get executive-level support
- Get support from General Council, Information Technology, Information Assurance, Physical Security, Human Resources, Counterintelligence, Law Enforcement
- Create Insider Threat Program Council/Insider Threat Team



Keys to Success

To ensure success, make sure you

- Start small, expand over time
- Use existing technology in place today
- Consistently evaluate program and look for ways to improve
- Regularly communicate (using metrics) effectiveness of program to senior management to ensure continual support
- Require insider threat security awareness training for all employees, contractors, and other trusted business partners
- Start today; evolve and expand over time



Module 17: Conclusions

Implementing an InTP may have negative unintended consequences.

You must think about these consequences, how they might appear in your organization, and what mitigations you can implement.

Address all insider threat activity in a consistent fashion, based on your own critical assets, mission, and priorities.

The time to implement a program may vary.

- Start small and grow.
- Have a phased approach.
- Start with what's in place.
- Add pieces as appropriate, and as resources, funding, and expertise are available.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0001900