Appendix B: Insider Threat Mitigation Pattern Thumbnail Sketches

1. Agree On Acceptable Use Policies

Context: An employee is using devices on his employer's network to perform his job.

Problem: Employees may exploit a real or false lack of knowledge about the acceptable use of devices on a network and engage in conduct that is counter to his employer's interests.

Solution: HR representatives of organizations should require employees to sign an acceptable use policy agreement before using devices connected to a network.

Related Patterns: Periodically Raise Security Awareness

2. Agree on Intellectual Property Ownership

Context: An employee is accessing information on his employer's network to perform his job.

Problem: Employees may be unaware of, or chose to ignore, the organization's ownership rights to information produced by employees of the organization, and, as a result, mishandle that information.

Solution: As a condition of employment, HR representatives of organizations should require employees to sign an intellectual property ownership policy agreement that specifies the rights that the organization has to any intellectual property to which the employee has access or develops.

Related Patterns: Periodically Raise Security Awareness

3. Assist Troubled Employees

Context: An employee is involved in a negative workplace event.

Problem: Troubled employees may have a higher likelihood of committing an insider incident.

Solution: Organizations can assist troubled employees in a way that provides them remediation and reduces their ill will toward the organization, thus avoiding an insider incident.

Related Patterns: Increase Monitoring for Indications of Disgruntlement

4. Constrain Remote Work

Context: An employee uses remote access to access the organizations information or systems purportedly to perform authorized functions.

Problem: Employees may exploit remote access to sabotage the organization's operations or to remove intellectual property in an unauthorized manner. [Flynn 2013]

Solution: Organizations should restrict remote access to an organization's network, either by restrictions to access timeframe (e.g., outside normal work hours) or restrictions to access relative to local network use, in a manner that enhances the organization's ability to protect itself and its assets.

Related Patterns: Log Employee Actions

5. Disable Known Access Points

Context: An employee is departing an organization for employment elsewhere and the organization has a comprehensive record of access paths the employee has for accessing the organization's systems.

Problem: Employees who depart an organization under problematic circumstances may become angry to the point of wanting to steal information from the organization or compromise the integrity of the organization's information or information systems. Active access paths into the organization's systems after departure provide the opportunity to do those things. [Flynn 2013]

Solution: Organizations should disable employee accounts that it knows about upon employee departure, and prepare to monitor suspicious remote access after departure for signs of unauthorized access attempts.

Related Patterns: Reconfirm Employee Agreements on Departure, Escort Out on Notice of Departure

6. Escort Out at Notice of Departure

Context: An employee resigns from his or her position within an organization.

Problem: Employees may attempt to exploit a flaw in organization security during the period between their notification of departure (or dismissal) and their exit from the premises.

Solution: The organization escorts the employee from the premises at the point of the employee's notification of departure or of the employee's dismissal.

Related Patterns: Monitor After Departure

7. Handle Employee Departure

Context: An employee has left or is preparing to leave an organization

Problem: Departing employees may be more willing to commit an insider incident due to the removal of dismissal or other disciplinary actions as a potential punishment.

Solution: The organization maintains usable, up-to-date policies on employee departure and trains managers in maintaining sympathetic but unyielding focus on the policies during the exit process.

Related Patterns: Increase Monitoring Due to Upcoming Departure

8. Handle Suspicious Actions

Context: An organization detects suspicious activity attributed to an employee

Problem: It is often difficult to distinguish employee actions that are a part of their normal job function and those that are counter to the organization's interest.

Solution: The organization investigates employee activity to decide whether suspicious activity warrants employee assistance, organizational sanctions, or - in the extreme of criminal conduct - employee termination and legal action.

Related Patterns: Assist Troubled Employees

9. Increase Monitoring Due to Upcoming Departure

Context: An employee is departing an organization voluntarily or not.

Problem: Employees preparing to depart an organization may be more likely to perpetrate an insider incident.

Solution: The organization should increase the monitoring of employees preparing to depart the organization. Previous analysis shows that organizations should consider analyzing employee transactions 60 days prior to the departure date, though smaller or larger monitoring windows may be desirable depending on the risk tolerance of the organization. [Moore 2012]

Related Patterns: Disable Known Access Points

10. Increase Monitoring for Indications of Disgruntlement

Context: An employee has displayed some indication that they are having troubles either personally or professionally.

Problem: Troubled employees may have a higher likelihood of committing an insider incident, even if the organization has tried to deal with the issue previously. [Flynn 2013]

Solution: Organizations should increase monitoring of disgruntled employees to determine whether an employee displays continued or increasing signs of disgruntlement.

Related Patterns: Handle Suspicious Actions

11. Log Employee Actions

Context: An employee is using devices on his employer's network to perform his job.

Problem: Organizations may not be able to attribute suspicious or malicious actions to the employee engaged in those actions.

Solution: Organizations should log routine employee actions that could be a component of a malicious act.

Related Patterns: Monitor Negative Workplace Events, Monitor Remote Access Outside Normal Hours, Handle Employee Departure

12. Monitor After Departure

Context: An employee is involved in a negative workplace event prior to or during their departure.

Problem: Employees may still wish to harm their employing organization even after their departure, possibly by using intellectual property gathered during employment or by using old access paths to harm the organization.

Solution: Organizations should monitor former employees and their potential online actions for signs that they may be trying to harm the organization.

Related Patterns: Handle Suspicious Actions

13. Monitor Negative Workplace Events

Context: An employee has agreed to and is trained on organization policies.

Problem: Negative workplace events may spur disgruntlement and be the motivation for an insider incident. [Flynn 2013]

Solution: Organizations should monitor negative workplace events that could be a precursor to or a component of an insider incident.

Related Patterns: Assist Troubled Employees

14. Monitor Remote Access Outside Working Hours

Context: An employee has authorized remote access to the organization's information and systems.

Problem: To evade detection, employees may exploit remote access outside of working hours to conduct activities that harm the organization.

Solution: Organizations should monitor remote access connections after working hours for suspicious activity. [Flynn 2013]

Related Patterns: Handle Suspicious Actions

15. Periodically Raise Security Awareness

Context: An employee using devices on a network is subject to constraints on their behavior to ensure security.

Problem: Employees may not recall or may feign not recalling a particular policy governing their behavior or controls for the protection of assets.

Solution: Organizations should train employees regarding their security responsibilities and compel them to periodically reaffirm their commitment to policies they have previously agreed to as part of that training.

Related Patterns: Constrain Remote Access, Log Employee Actions

16. Reconfirm Employee Agreements on Departure

Context: A departing employee has agreed to and is trained on organization policies.

Problem: Employees may either forget about previous policy agreements or feign ignorance of employment agreements making violations of those agreements more likely.

Solution: Organizations should discuss with departing employees their previous employee agreements and require them to recommit to those agreements before departure.

Related Patterns: Monitor After Departure

17. Screen Employees

Context: An individual (candidate) is attempting to gain employment at the organization.

Problem: Candidates may have participated in detectable prior incidents that make their employment inherently risky, or otherwise be unsuitable for the position at hand.

Solution: Organizations should perform background checks on candidates and hire only individuals who meet some minimum criteria for employment.

Related Patterns: Agree on IP Ownership, Agree on Acceptable Use Policies