For a SIRP to be effective, there are six stages that need to be addressed. Proper execution of the response plan will require the efforts of various different departments within an organization. Detailing the roles and responsibilities of these individuals as well as creating precise guidelines for analyzing, reacting to, and controlling security violations.

Groundwork

Identify and train the security incident response team (SIRT) on the formal protocal for and tools necessary for detecting and responding to a breach. Compile and record internal and external resources and entities that may need to be contacted.

Identification

Determine if a security breach has occurred and if so the type and extent of the incident. Designate specific members within the SIRT to review, document, and label the impact (low, medium, high). Decide if the SIRP should be initiated and if management should be alerted.

Control

Focus on the necessary requirements for limiting the extent and magnitude of the attack. Identify where your SIRT will assemble, how they will initially respond, what parties need to be contacted regarding the incident, and determine if systems are operable.

Elimination

Remove the cause for the security incident and mitigate any gaps or vulnerabilities that were a result of the attack. Outline the process for discovering how the incident occurred and what needs to be done to prevent another breach.

Recovery

Restore all data and services that were impacted and formalize what actions need to be initiated to validate the affected systems functionality. Notify governing authorities if the incident resulted in unauthorized access to personal information.

Review

Evaluate and learn from the situation. Critique and modify the actions, processes, and procedures contained within the SIRP. Make any necessary changes and refinements that would allow the SIRT to be more effective should another security incident occur.