

# Rapid System Repair/Recovery Strategies and Concepts

Robert Martin

781-271-3001 • [ramartin@mitre.org](mailto:ramartin@mitre.org)

Exploratory MITRE Sponsored Research



# Problem



- **In the event of a cyber attack, processes and procedures are needed that:**
  - **When executed will return a system to full operational capability in hours rather than days**
  - **When executed will render the system somewhat less vulnerable to similar attacks**
  - **Be repeatable for a wide range of attacks/scenarios.**

# Background



- **There is considerable risk of cyber attack.**
- **Recovery processes are in place to deal with simple software problem reports**
  - **Uncertainty and chaos associated with cyber attack not addressed,**
- **Cyber attack detection and forensic capabilities are limited.**

# Objective



- **Identify and document processes and their significant inputs that, in the event of a cyber attack, can be used to return critical command and control systems to an operational state in minutes to hours**
  - **Significant inputs – those factors that must be understood to make the desired timeline feasible**
  - **Identification of system requirements that support recovery processes.**

# Activities



- **Poll systems of record to determine the “best” current approaches to emergency patching.**
- **Perform a literature search to determine what commercial solutions would be applicable to problem space.**
- **Consult with other industries that have similar concerns to see what processes/tools they have in place that address this problem.**
- **Develop and document rapid recovery processes.**
- **Improve critical cyber-enabled systems in following areas:**
  - **Rapid problem analysis**
  - **System recovery**
  - **Resumption of the mission.**

# Impacts



- **Rapid recovery processes result in more robust command and control systems in the face of cyber attacks.**
- **The ability to rapidly return a system to an operational state can also improve our response to non-cyber related problems.**

# Future Plans



- **Identify new areas of research that focus on cyber attack response versus cyber attack prevention.**