Project Remedies Inc.

# Rapid Cyber Remediation Response Management

Using the Game-Changing Capabilities from Project Remedies Inc.

A White Paper from Project Remedies Inc.
August 2016


Project Remedies Inc.

***Abstract***

*Rapid Cyber Remediation Response requires planning. If there is an attack, how will your team respond? This means implementing enterprise-wide processes quickly and easily, being able to see the current status of the remediation effort at any time, and measuring performance. To do this requires:*

- *Defining and having a repository of processes used for different types of remediation efforts. These are called "'work templates."*
- *Eliminating the need for training the people involved on the processes. They are too spread out and this takes too long. They just need to be trained on working the tasks assigned to them. The process is in the template.*
- *Eliminating silos within and between organizations because processes cross organizational boundaries.*
- *Capturing performance, which means time spent and task duration. These are the key performance metrics needed. These are the metrics needed to determine if and how a process can be done faster, improving tempo.*
- *Defining and tweaking processes needs to be fast and easy, so you can be responsive as you get more information about performance.*
- *Measuring cost. "Time spent" times an average rate for each labor category gives you a labor cost for each remediation effort. At a briefing, one manager said that if they knew how much it cost for each remediation effort, they might not want to do all of them.*
- *Understanding resource availability and how they are performing. Having automatic notifications is important if someone is not responding quickly enough.*

*All of this is needed to manage and improve the remediation of cyberattacks, vulnerabilities, and failures in the IT infrastructure. The new Federal Cyber Security Framework requires a structured incident response capability, which is what Project Remedies' ActionProgram Manager Plus offers.*

*ActionProgram Manager Plus brings mature capabilities to solve this constant and evolving problem of complex and rapid incident remediation response. It gives you a degree of situational awareness previously unavailable and is a major part of your overall situational awareness goals. ActionProgram Manager Plus organizes and tracks tasks, manages staffing, captures cost and monitors each Remediation Response task/project status in near real-time.*

---

## The Need for Rapid Cyber Remediation Response Management

Cyberattacks are escalating on an increasingly more valuable set of targets. For example, Next Gov 2013 reports:

- British energy company BP says it suffers 50,000 cyber intrusion attempts per day.
- The Pentagon reports getting 10 million attempts per day.
- The National Nuclear Security Administration, an arm of the Energy Department, also records 10 million hacks per day.

A huge rush of technologies is moving forward to monitor and analyze the networks looking for bad actors and other risks. Much of this technology is quite good and effective. But -- once an attack penetrates the firewalls, or a staff member unwittingly downloads malicious code, or a vulnerability is discovered in a node or system, or the

system goes down -- a response has to happen and as quickly as possible. Responding quickly is a key to winning, General Alexander said.

When incidents occur, organizations must be equipped to move rapidly with coordinated, multiple smart remediation responses. Skilled and knowledgeable specialists from independent organizations in multiple locations become an Incident Response Team. This "smart team" is required to execute a precisely orchestrated series of co-dependent tasks on a strict schedule. Some of these tasks can be performed in parallel, and some have sequential dependencies and take the form of a rapid-momentum Plan of Action & Milestones (POA&M). People from multiple internal organizations are involved and people in external organizations may get involved as well. The faster they do this, the better.

Because the Cybersecurity operational tempo is so intense, the ability to maximize the human resources needed to remediate cyber incidents has tended to lag behind the Cybersecurity technology curve.

> "The speed with which a response to a "cyber incident" is initiated is critical to the successful remediation of the incident," Gen. Keith Alexander, Commander **USCYBERCOM.**

The critical elements needed in managing cyber remediation are:

- **Speed of the cyber mediation response.**
- **The right cyber remediation approach and plan.**
- **The right people to execute the remediation.**
- **Multiple measures of remediation status and performance.**

Cascading problems emerge when the Incident Response Team is overwhelmed by unplanned and uncoordinated activity as they are trying to respond to multiple incidents. They often become more reactive, losing the ability to be proactive and preventive.

The Federal Government has initiated the new Federal Cybersecurity Framework, which intended to create Cybersecurity standards and protocols across the government, public and private sector. The Department of Homeland Security has created a cross-agency "Continuous Diagnostics and Mitigation (CDM) Program." NIST SP 800-61 defines Incident Handling standards and specifically calls for this kind of approach. Project Remedies Inc.'s **ActionProgram Manager Plus™** supports the controls specified in this document.

On the Department of Defense side, the Chairman of the Joint Chiefs of Staff published Instruction 6510.01F which covers "Information Assurance (IA) and Support to Computer Network Defense (CND)." This guidance details the responsibilities of each of the organizations involved with each incident within the DOD context.

The key to successful Cyber Remediation Strategy is to manage together the unanticipated incidents that result from system intrusions and intrusion agents, with the planned events such scheduled asset outages or updates to software, or the ongoing identification of system or network vulnerabilities. Managing and coordinating holistically these planned maintenance and remediation events with the high-value response to intrusion and vulnerabilities of the Incident Response Team (IRT), maximizes the organization's total Cyber Security remediation efforts and optimizes the staffing

resources. Tracking and costing these efforts is critical to overall Cybersecurity program success.

## Developing a Rapid Cyber Remediation Response Solution

Event detection sets in motion a number of critical steps. Managing these steps effectively requires implementing a cyber remediation response capability that is rapid, structured, and agile enough to manage today's Cybersecurity operational tempo and changing threat matrix. Senior Management needs the ability access to this information, which is current up to the last entry, at any time.

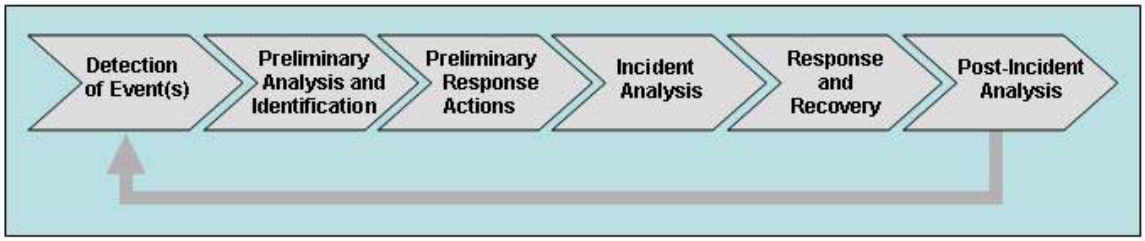


**Diagram 1. Overview of the Generic Cyber Remediation Response**

Each organization has their own processes and protocols that must snap into place as quickly as possible when called to accomplish these tasks.

The Core Elements for optimized Rapid Cyber Remediation Response Management are:
:

1. **Incident or Event Entry into an "Event Log"**
2. **Remediation Categorization and Prioritization**
3. **Launching a Task Plan for Each Remediation Event**
4. **Remediation Staff Resource Management**
5. **Real-time Remediation, Status, Performance and Cost Monitoring**
6. **Near-Real-time Policy Updates**
7. **Real-time and Post Incident Learning (After Action Review)**

## The Project Remedies' Approach

Project Remedies Inc. is a 24-year old services and technology company that has developed Remedy-based solutions, which run on your existing Remedy environment and leverage your Remedy investment. Our services support your effort to define your remediation processes and our technology enables the rapid implementation and operationalizing of the processes. You have to have the right people with the right tools doing the right things at the right time.

**ActionProgram Manager Plus** brings together the pool of incidents and vulnerabilities; defines and plans all of the tasks involved into the remediation effort for each; matches them with a pool of staff resources; and then monitors performance and cost for each task.

### The Steps of Rapid Cyber Remediation Using the Project Remedies Approach

Project Remedies' **Cyber Action Manager™** creates a Common Operational Picture (COP) for remediation effort that provides full-picture "Situational Awareness" of issues, staff, cost and project status of the remediation throughout the event response life-cycle.

**1. Incident or Event Entry into a "Common Operational Picture" (COP)**
Incidents or vulnerabilities are automatically created in **Remedy Incident Management** in real-time as HBSS, ArcSight or some other event manager or monitoring system captures them. Other events or vulnerabilities can be entered manually. One of the advantages of using the Remedy system is, when a user realizes that something is happening, they will contact the Service Desk. The person on the Service Desk can look at their existing Incident or Problem Management application and see what is happening and inform the caller.

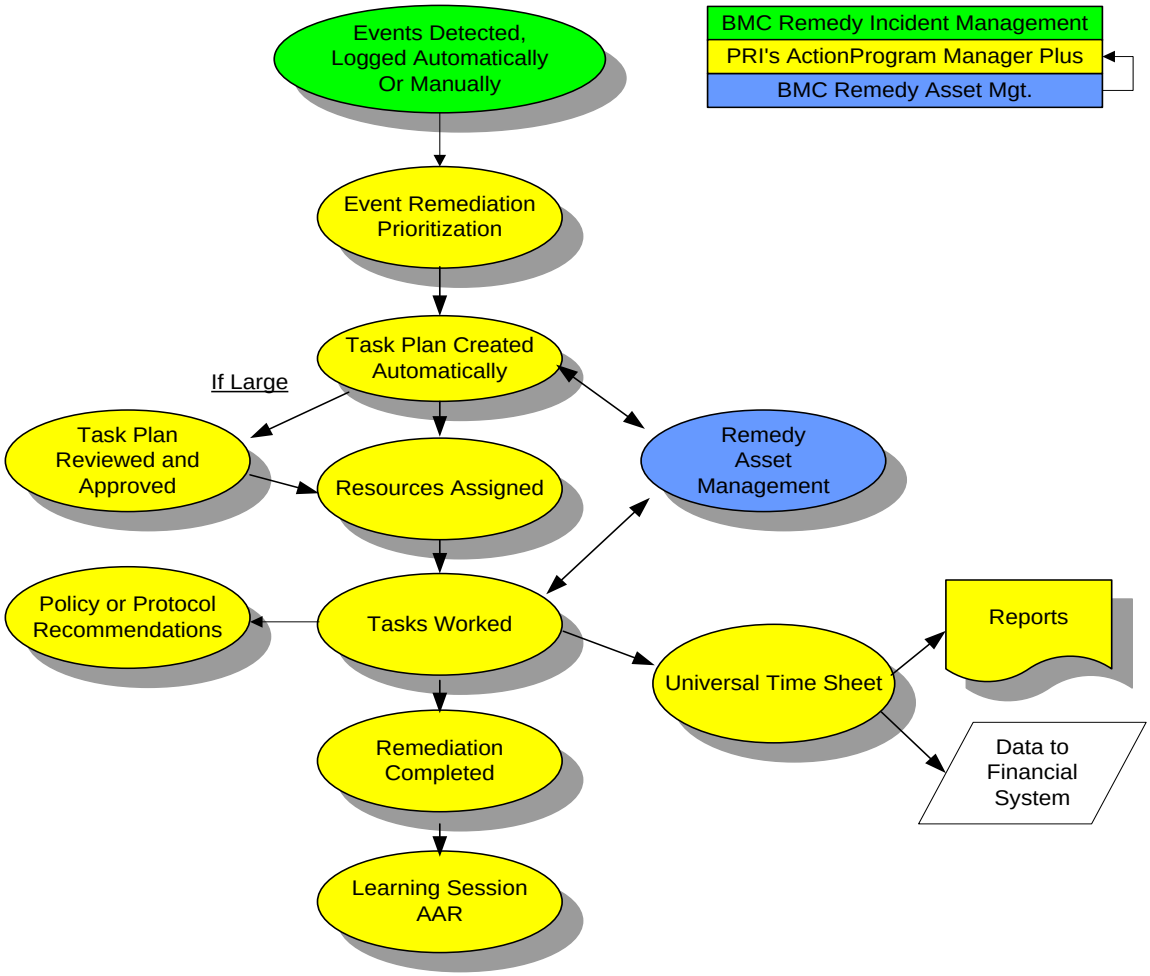


**Diagram 2. The Project Remedies Cyber Remediation Life Cycle**

**2. Remediation Categorization and Prioritization**
Once captured, the organization's Remediation Categorization and Prioritization Protocols is used to determine which pre-defined process should be used for this remediation effort. By applying these decision and prioritization rules to the event list, the response to these cyber events can be structured, prioritized and planned using a number of imbedded or added decision criteria. Developing the core of these decision criteria is part of any Cybersecurity Strategy.

The aggregation of remediation issues into one place, your Remedy system, allows management to look for trends and answer various questions: What types of incidents

are occurring? From where do the threats come? How frequently? What have we done? How long did each remediation effort take? How much did each one cost?

The Cyber Remediation COP can be used across multiple inter-connected organizations. Designated commanders and managers can see the status of each response, particularly the tasks that they are responsible for, at any time. Because all of the data (incidents, resources, tasks and costs) are in one place, the Remedy database tables, they can integrate and share multiple data inputs in an integrated workflow. Access to all fields and forms is permission-based so only the people who are supposed to see the data will see the data.

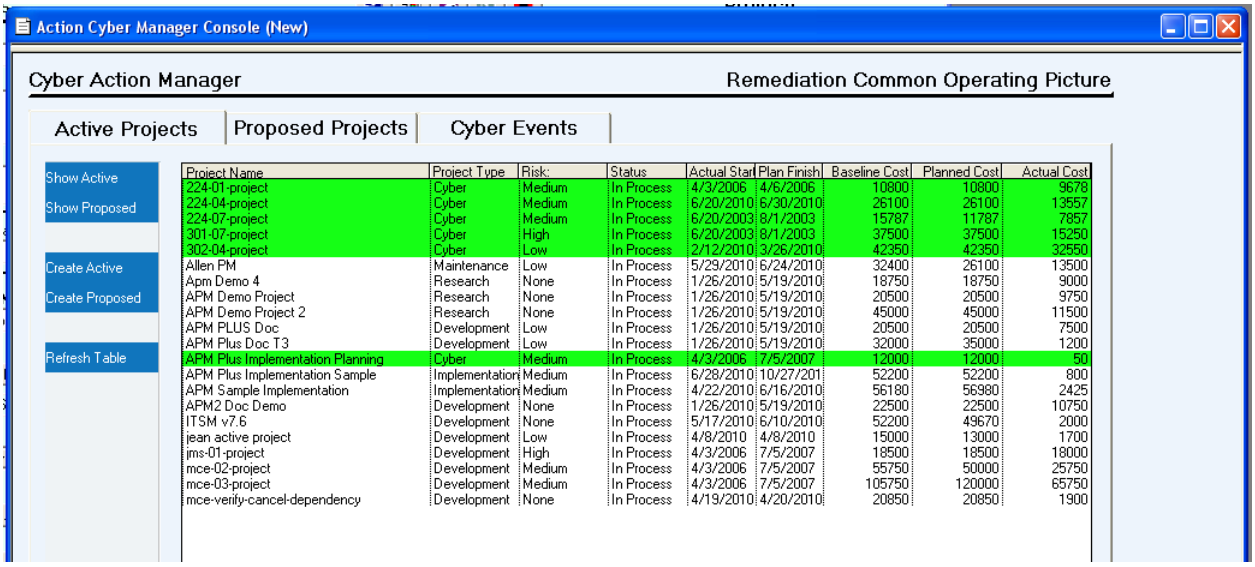


**Diagram 3. Cyber Remediation "Common Operating Picture"**

Diagram 3 shows all Active Projects (those "In Process"), Proposed Projects (those not "In Process"), and individual incidents. With one click, the manager can see the detail he or she wants to see. Shared access to incidents and response details across teams affords a degree of situational awareness previously unavailable.

### 3. Launch Task Plan for Each Remediation Event

Once the incident is in **the system** and has been categorized and prioritized, the analyst selects a pre-defined "Work Template" from a repository of Work Templates stored in ActionProgram Manager Plus. The work template is used to automatically generate a Task Plan**.** Work Templates are tested, consistent, repeatable processes which typically cross organizational boundaries. They conform to Cybersecurity "best practices" and can easily be updated based on experience and the performance metrics captured.

Task Plans using the Work Templates, act as both the tasking instruction and the ongoing project plan for the remediation activity. Task Plans are used to rapidly coordinate multiple complex remediation responses, while reducing duplicative tasking activity. If approval is needed for additional levels of staffing or fiscal resources for the remediation, the Task Plan can act as an internal proposal and workflow for getting and tracking that approval.

## 4. Remediation Staff Resource Management

ActionProgram Manager Plus gives leadership the ability to match individuals or team resources to each incident and task in the remediation effort. These tasks can be standalone or grouped as larger efforts, so commanders and managers can see time-lines and how busy people are over time.

Each tasking breaks down the number of hours given to an individual or work group for the project timeline. This is critical to optimizing staff resources and measuring performance and costs. This staffing process can also be sorted by skills, location, and organizations. ActionProgram Manager Plus automates notification, tasking and acceptance of the people and organizations involved. When one task is completed, ActionProgram Manager Plus automatically notifies the person or people responsible for working the successor task(s) at network speed.

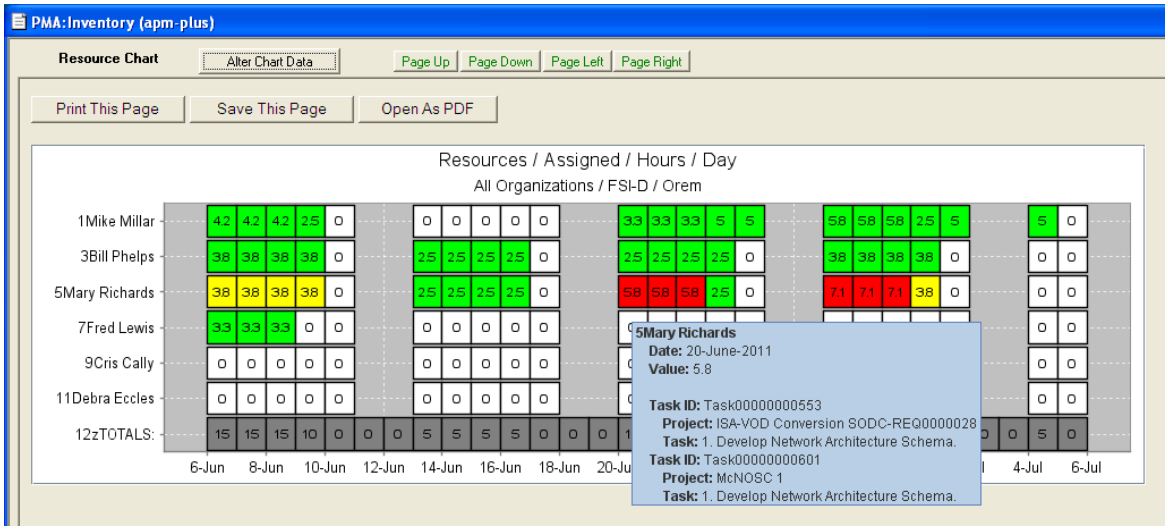


**Diagram 4. Resource Management Chart Daily**

## 5. Real-time Remediation Status, Performance and Cost Monitoring

Once the people and organizations start working the task plan, their performance is tracked against timelines and time expenditure. This tracking provides important insight into how long tasks actually take and how much time was spent.

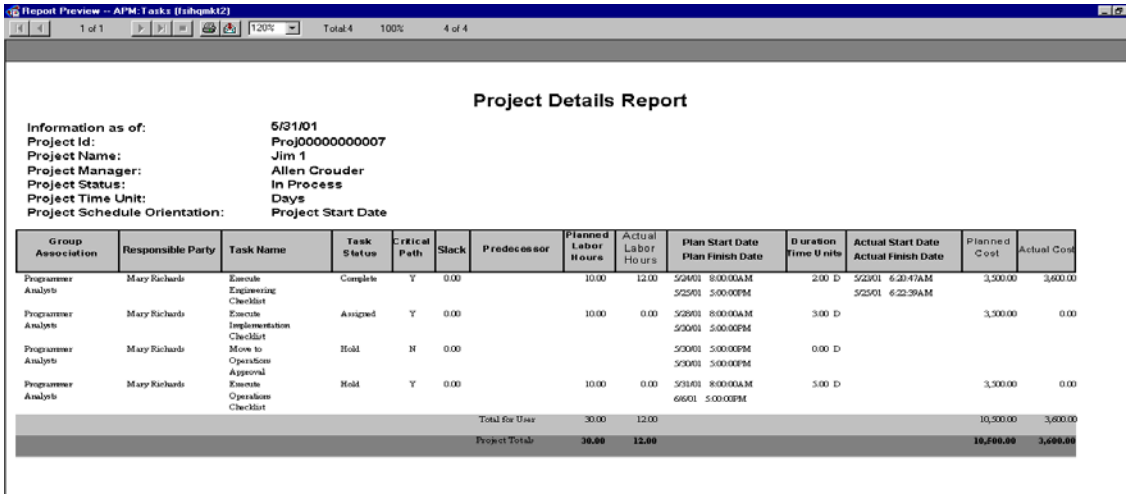


**Diagram 5. Cyber Action Manager Task Plan: Project and Performance Management**

If you have both metrics, senior leadership from the organizations involved can have meaningful conversations about if and how the process can be improved. And without these metrics, they can't.

One of the critical advantages of ActionProgram Manager Plus's time tracking functionality is that it can be integrated with an Asset Management System. Integrating ActionProgram Manager Plus with Remedy's Asset Management System, or another Asset Management system allows detailed asset costing. All costs (time, expense and asset cost) can be seen in aggregate, so the organization's budget burn rate can be monitored. These can in turn be integrated into the organization financial control system allowing a more robust costing picture can emerge.

**6. Near Real-time Policy Updates**

ActionProgram Manager Plus gives the Incident Response Team the ability to share and document insights in real time. As the remediation is undertaken and the problem is better understood, insights develop as to how to prevent the problem. These policy insights can be shared with leadership who may want to temporarily or permanently change policies or protocols in near real-time, and change the work templates. Changing work templates can be done easily and quickly.

**7. Real-time and Post Incident Learning (After Action Review)**

One of the critical components of effective Cyber Remediation is learning as an organization. ActionProgram Manager Plus provides the capacity for all members of the Incident Response Team to share and document insights in real time. This can be critical to managing multi-vector attacks, where insight in one area is immediately useful in others. Knowledge gained from each incident can be aggregated together with other similar incidents into a knowledge base, which can support a Post Incident Learning or After Action Review (AAR) process, enabling the Incident Response Team and the IT Team as a whole can get smarter, faster. With this knowledge, work templates can be modified and immediately operationalized because training the team is not necessary. The process is in the template. Comparing the performance metrics on the new template vs. the original template tells you whether the new one is faster or not.

## Summary

Gen. Alexander has said that the speed with which we respond to incidents is critical in winning the multiple wars in our cyberspace. When technology fails, somebody has to fix it. Rapid Remediation Response is managing the complexities of many small and medium-sized remediation and maintenance projects, insuring the right people resources as well as the right technologies are focused on the right problems at the right times.

Combining your existing Remedy Incident Management and Problem Management applications with Project Remedies' ActionProgram Manager Plus creates a Common Operational Picture (COP) for all the incidents and remediation efforts. It provides a real-time full-picture "Situational Awareness" of issues, staffing, cost and project status of the remediation efforts throughout the incident response life cycle. It creates real-time shared information, system policy insights and organizational learning as the remediation is ongoing, which is critical to successfully managing the current and emerging challenges to the IT infrastructure.

Project Remedies and our partners have the people, tools and experience to facilitate the implementation of Rapid Cyber Remediation Response.

Project Remedies Inc.

For more information: please contact:
Stan Feinstein
310-230-1722
stanf@projectremedies.com

or visit our home page at www.projectremedies.com