Project Remedies Inc.

Rapid Cyber Remediation Response Management

Using the Game-Changing Capabilities from Project Remedies Inc.

A White Paper from Project Remedies Inc.
January 2014

Abstract

Rapid Cyber Remediation Response optimizes the time and people resources needed to manage and remediate the cyber attacks, vulnerabilities, and failures in an Information System. The inability to manage complex and multiple remediation efforts simultaneously creates its own set of system risks. Project Remedies brings mature capabilities to solve this constant and evolving problem of complex and rapid remediation response with limited resources, and affords a degree of situational awareness previously unavailable.

The Need for Rapid Cyber Remediation Response Management

"The Network" enables Military Operational speed, precision and lethality around the globe and is increasingly the backbone of commerce and technology development. Cyber attacks 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 vulnerability is discovered in a node or system, or the system goes down -- a response has to happen. Either: 1) Some responses can be handled by some available technical solutions, or 2) Many responses must be handled by a sophisticated Incident Response Team (or others) using high tech and in some cases low tech solutions to remedy the problem, which may include both "fixes" and preventive measures.

For incidents that are complex, contain unpredictable elements, and are security-urgent, organizations must be equipped to move rapidly into coordinated, multiple smart remediation responses. Several 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).

Because the Cyber Security operational tempo is so intense -- and because many organizations have become over-reliant on passive technology solutions -- the ability to maximize the human resources needed to remediate cyber events has tended to lag behind the cyber security 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,* ***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 events, often becoming more reactive and losing the ability to be proactive and preventive.

> "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.**

With cyber remediation in mind, 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. A key to successful Cyber Remediation Solution is to maximize and coordinate the various high-value components of each Incident Response Team's cyber remediation response.

Developing A Rapid Cyber Remediation Response Solution

Event detection sets in motion a number of critical steps. Managing these steps effectively over the long term requires developing a cyber remediation response concept that is rapid, structured, and agile enough to manage today's cyber security operational tempo and changing threat matrix.

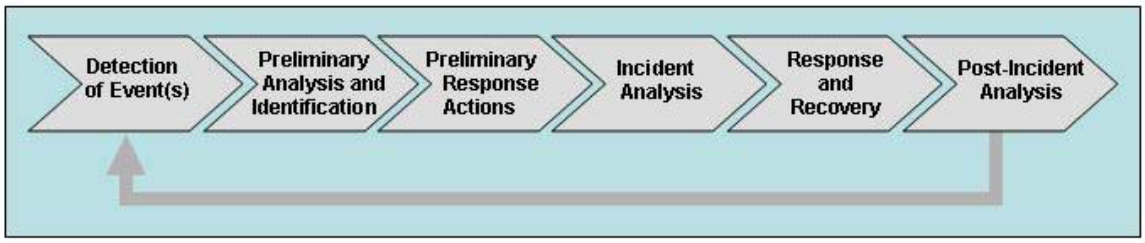


Diagram 1. Overview of the Generic Cyber Remediation Response

Each organization will have its own processes and protocols that snap into place when called to accomplish these tasks in order to launch an effective remediation of the cyber event or vulnerability.

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

1. **Event Entry into a "Common Operational Picture" (COP)**
2. **Remediation Prioritization**
3. **Launch 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 20-year old technology and services company that has created many BMC Remedy-based solutions, which can leverage legacy BMC Remedy systems. Several of these are "game changing" tools and processes for Cyber Remediation because they fill in the often-overlooked critical component of Cyber Remediation –"You have to have the right people with the right tools doing the right things at the right time."

Project Remedies Inc.'s **Cyber Action Manager™** 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.

Cyber Remediation Management is about having the right people with the right tools doing the right things at the right time.

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, costing and project status of the remediation throughout the event response life cycle.

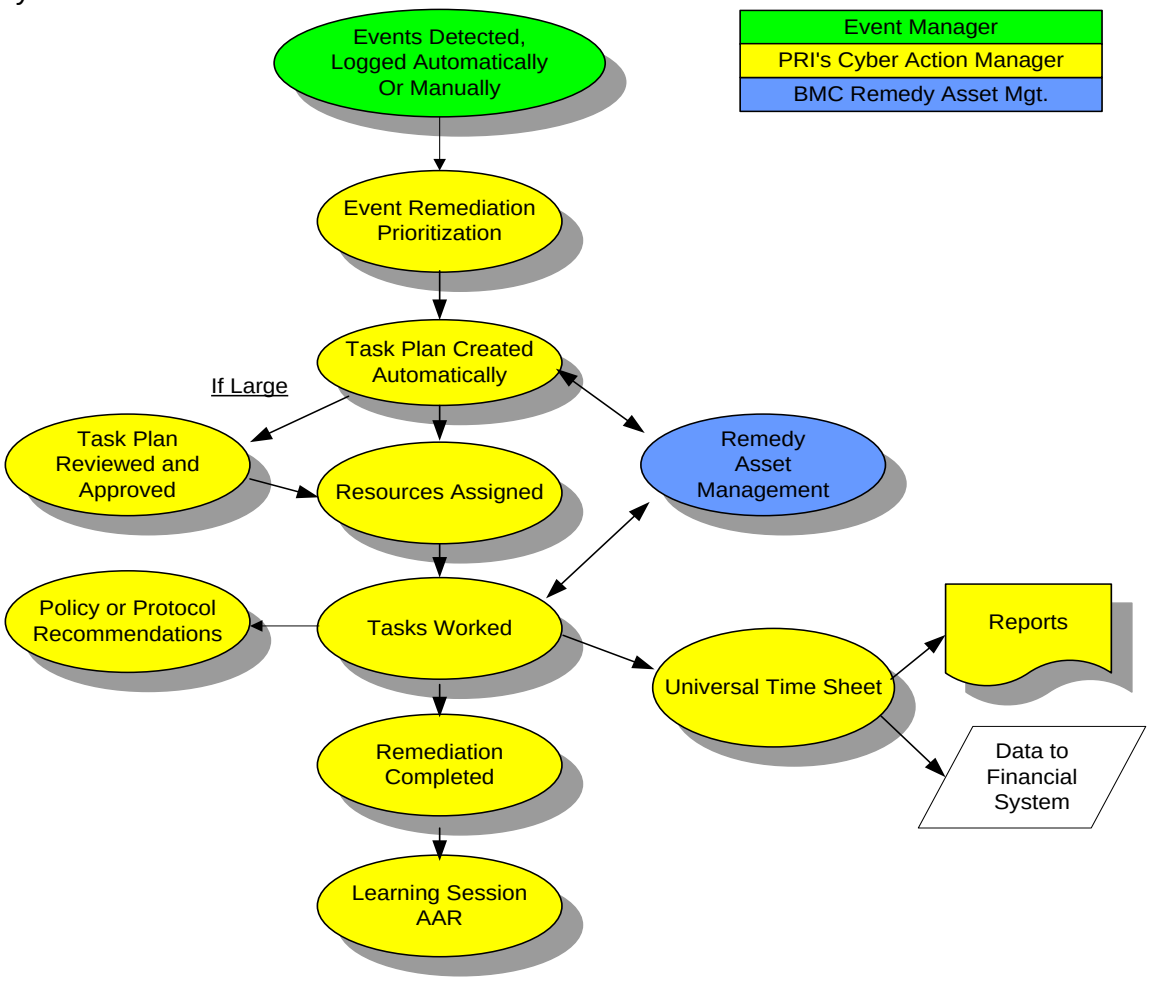


Diagram 2. The Project Remedies Cyber Remediation Life Cycle

1. Event Entry into a "Common Operational Picture" (COP)
Incidents or vulnerabilities are automatically created in **Cyber Action Manager™** in real-time as HBSS, ArcSight, Cauldron or some other event manager or monitoring system captures them. Other events or vulnerabilities can be entered manually into BMC Remedy Action Request System (AR System). The aggregation of remediation issues into the **Action Manager™** creates a "Common Operational Picture" (COP) for Cyber Remediation Response**.** One of the advantages of importing the event log to **Cyber Action Manager™** is the reduction of "white noise" or false and redundant events.

The resulting Cyber Remediation COP can then manage the whole range of cyber remediation issues and coordinate the Incident Response Team, showing the current status of all tasks performed, by all of the individuals or organizations involved, and who is available for further tasking. The entire cyber remediation life cycle can be managed across multiple organizations.

2. Remediation Prioritization
Once the Cyber Remediation COP has the current cohort of issues, it is important to apply the organization's Remediation Prioritization Protocols, creating a unique spectrum of criticality for the proposed Remediation activities. 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 in the **Cyber Action Manager™.** Developing the core of these decision criteria should be part of any Cyber Security Strategy.

The Cyber Remediation COP can be used across multiple inter-connected organizations. Designated commanders and managers can see the status of each incident and task at any time. Because all of the data (incidents, resources, tasks and costs) are in the Remedy database tables, they can integrate and share multiple data inputs in an integrated workflow.

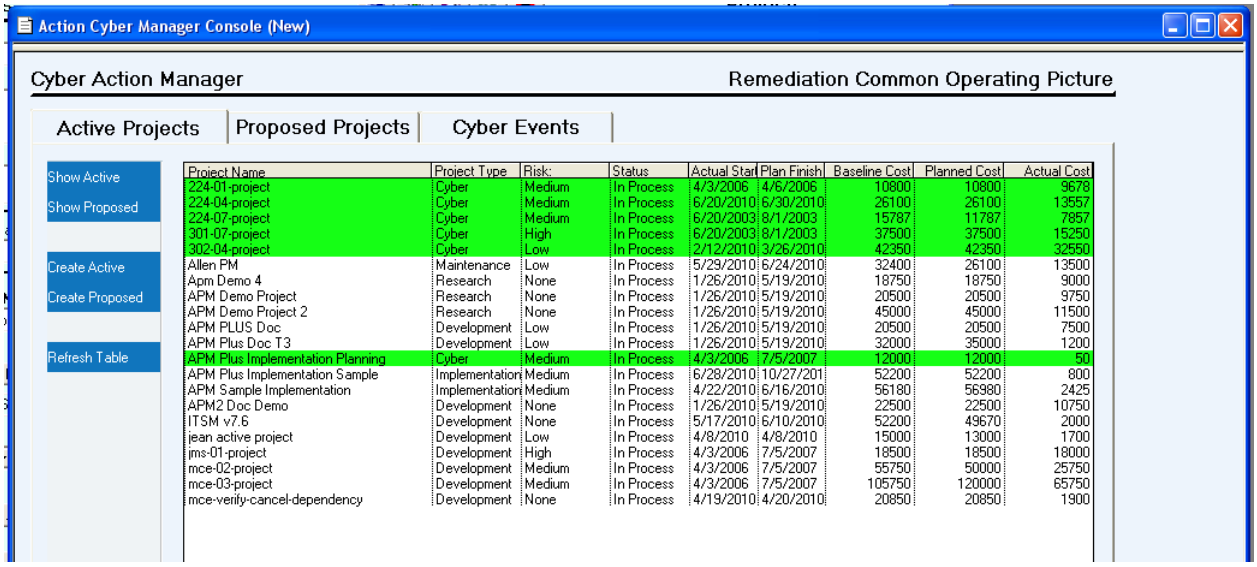


Diagram 3. Cyber Remediation "Common Operating Picture"

Diagram 3 shows all Active Projects (those "In Process"), Proposed Projects (those not "In Process"), and individual incidents. With one click, the project record opens and

offers more details to the analyst or manager. Shared access to events and event details shared across teams affords a degree of situational awareness previously unavailable.

3. Launch Task Plan for Each Remediation Event

Once the event is in **Cyber Action Manager™** and has been prioritized, a Task Plan is created automatically using standardized "Work Templates" that are embedded in **Cyber Action Manager™.** Each required Remediation activity is spelled out in the "Task Plan," which acts as an "Express Project Plan." Task Plans using the filled-in Work Templates, act as both the tasking instruction and the ongoing project plan for the remediation activity. Task Plans can be 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

Cyber Action Manager™ 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.

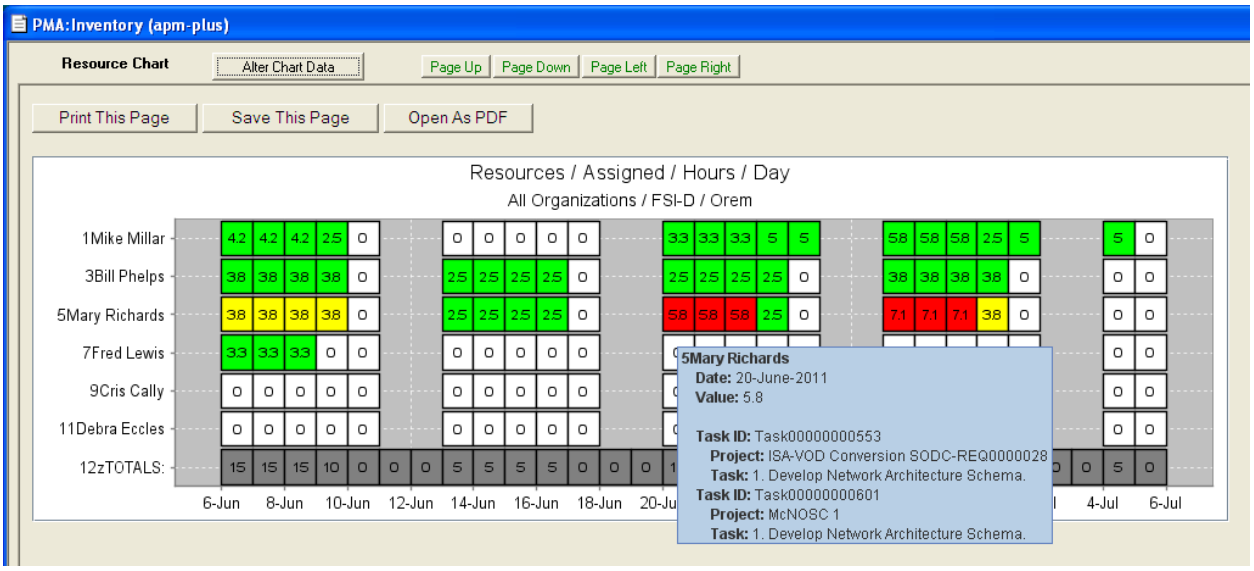
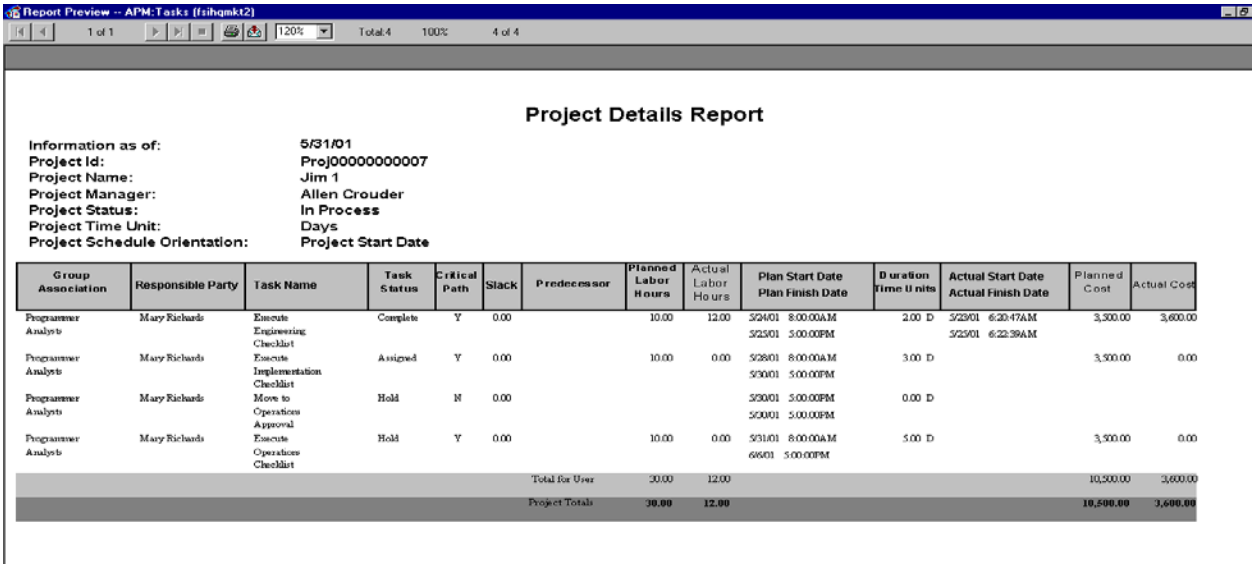


Diagram 4. Resource Management Chart Daily

Each tasking can break down the number of hours being given to an individual or work group for the project timeline. This is critical to maximizing your staff resources and measuring performance and costs. This staffing process can also be sorted by skills, location, and organizations. **Cyber Action Manager™** can automate notification, tasking and acceptance of the people and organizations involved.

5. Real-time Remediation Status, Performance and Cost Monitoring
Once the people and organizations accept the task plan, their performance in the remediation can be tracked against timelines and time expenditure. This tracking provides important insight how long tasks take and who is available for the next task.

One of the critical advantages of **Cyber Action Manager's™** time tracking against incidents, changes and project tasks, is that it can be integrated with an Asset Management System. Integrating **Cyber Action Manager™** with Remedy's Asset Management System, or another Asset Management system allows detailed asset costing to be brought into each task or project. All costs, time, expense and asset cost can also 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 such as electronic time cards, so a more robust costing picture can emerge.


Report Preview -- APM:Tasks (fsihqmkt2)

1 of 1 | 120% | Total:4 | 100% | 4 of 4

Project Details Report

Information as of: 5/31/01
Project Id: Proj00000000007
Project Name: Jim 1
Project Manager: Allen Crouder
Project Status: In Process
Project Time Unit: Days
Project Schedule Orientation: Project Start Date

Group Association	Responsible Party	Task Name	Task Status	Critical Path	Slack	Predecessor	Planned Labor Hours	Actual Labor Hours	Plan Start Date / Plan Finish Date	Duration Time Units	Actual Start Date / Actual Finish Date	Planned Cost	Actual Cost
Programmer Analysts	Mary Richards	Execute Engineering Checklist	Complete	Y	0.00		10.00	12.00	5/24/01 8:00:00AM 5/25/01 5:00:00PM	2.00 D	5/23/01 6:20:47AM 5/25/01 6:22:39AM	3,300.00	3,600.00
Programmer Analysts	Mary Richards	Execute Implementation Checklist	Assigned	Y	0.00		10.00	0.00	5/28/01 8:00:00AM 5/30/01 5:00:00PM	3.00 D		3,300.00	0.00
Programmer Analysts	Mary Richards	Move to Operations Approval	Hold	N	0.00				5/30/01 5:00:00PM 5/30/01 5:00:00PM	0.00 D			
Programmer Analysts	Mary Richards	Execute Operations Checklist	Hold	Y	0.00		10.00	0.00	5/31/01 8:00:00AM 6/6/01 5:00:00PM	5.00 D		3,300.00	0.00
						Total for User	30.00	12.00				10,500.00	3,600.00
						Project Totals	**30.00**	**12.00**				**10,500.00**	**3,600.00**

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

6. Near Real-time Policy Updates
Cyber Action Manager™ has the capacity for all the Incident Response Team to share and document insights in real time. As the remediation is undertaken and the problem is understood, insights develop as to how to prevent the problem using policy or protocol changes. These policy insights can be shared with the leadership who may want temporarily or permanently change policies or protocols in near real-time. Because Cyber Action Manager™ runs on a legacy BMC Remedy environment, informing the help desk and critical staff of proposed and in force policy changes is easy

7. Real-time and Post Incident Learning (After Action Review)
One of the critical components of effective Cyber Remediation is learning as an organization. Cyber Action Manager™ 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, so the Incident Response Team and the IT Team as a whole can get smarter, faster. With this knowledge, Work Templates can be easily modified in minutes.

Summary

Gen. Alexander has said that the speed with which we respond to events 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 remediation projects, insuring the right people resources as well as the right technologies are focused on the right problems.

Project Remedies' **Cyber Action Manager™** creates a Common Operational Picture (COP) for the remediation effort that provides real-time full-picture "Situational Awareness" of issues, staffing, costing and project status of the remediation process throughout the incident handling lifecycle. It creates real-time shared information, system policy insights and learning as the remediation is ongoing, which is critical to successfully managing the current and emerging challenges to cyber security.

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: http://www.projectremedies.com

stanf@projectremedies.com

310-230-1722