Cyber Security Performance Management

Our CyberSecPM™ solution extends best practice Cyber Security Capability Maturity Models into a dynamic performance management framework. CyberSecPM enable you to test and validate or refine your Cyber Security performance improvement strategies across their entire lifecycles. Our dynamic methods and supporting software tools help you reduce risk exposure, increase confidence and consistency in your decisions, and continuously improve your capabilities to manage Cyber Security as a core competency.

The Performance Management Dimension

Cyber Security has two dimensions: technical and management. The technical dimension addresses tools and skills to detect and defend against diverse cyber attacks. The management dimension encompasses governance, processes, and culture to minimize vulnerabilities and maximize preparedness.

Performance Management (PM) refers to how organizations leverage resources to achieve their goals. PM methods work by (1) measuring your organization's performance against relevant metrics; (2) diagnosing shortcomings and setting targets; (3) developing plans to improve performance; and (4) executing those plans.

Our Cyber Security *Performance Management (CyberSecPM)* solution applies PM methods to improve Cyber Security management. CyberSecPM helps you:

- **Measure your Cyber Security performance against industry best practices**
- **Design plans for improving performance**
- **Test and validate or refine your plans using powerful simulation methods**
- **Monitor results during plan execution, so that you can detect emerging problems early and make prompt mid-course corrections to ensure success.**

Measuring Cyber Security Performance is Necessary But NOT Sufficient

The technical side of Cyber Security receives the bulk of attention and funding today, revolving around defensive systems and techniques to detect attacks and either block them or mitigate their harmful consequences. However management is equally critical: most types of cyber attacks can only occur when your organization's "back door is left open," due to poor security practices or lack of compliance.

The first step to improving Cyber Security management is to measure your current performance. CyberSecPM leverages a measurement framework developed by the Software Engineering Institute's CERT organization at Carnegie Mellon University called a Capability Maturity Model (CMM). A CMM is a process improvement methodology. It defines a set of metrics for measuring organizational competency or maturity in terms of a set of recognized best practices and skills. Metrics are, organized into categories and quantified on a performance scale. Rating criteria allow organizations to benchmark their performance against these "maturity" levels.

The core problem with CMMs is that they are inherently static; you apply a CMM to measure performance at discrete instants. Such exercises enable gap analyses against industry best practices, but are not directly actionable: a CMM provides no support for formulating plans to improve your maturity levels, much less for testing them prior to roll-out *or* monitoring their execution and making appropriate mid-course adjustments. In short, a CMM only supports the initial diagnostic phases of PM; you are on your own to address the back-end PM processes that actually drive performance improvement!

Cyber Security Performance Management

CyberSecPM: Improve Your Cyber Security, Don't Just Measure It

In contrast, CyberSecPM "animates" the CMM and extends it into a dynamic maturity process improvement methodology. We collaborate with leading Cyber Security consulting partners to apply our CyberSecPM software to carry out the following five step process:

1. Assess your current Cyber Security maturity levels against CERT's best practices CMM framework
2. Identify performance goals, in terms of a set of target maturity levels for CERT's Cyber Security best practice categories
3. Develop a detailed strategy for improving your processes, governance structures, and culture to achieve your Cyber Security goals. A strategy specifies initiatives to develop Cyber Security practices, with estimated schedules and costs.
4. ***Test*** your improvement strategy, and validate or refine it ***prior*** *to* roll out. This step is critical because CERT's Cyber Security CMM contains dozens of objectives and hundreds of practices. CyberSecPM models your strategies; applies an innovative simulation engine to project their likely outcomes; and analyzes the results. Testing uncovers gaps (CMM practices that you missed) and unintended consequences early, when they can be corrected with minimal effort, cost, and risk.
5. Re-apply CyberSecPM's simulation engine to help you monitor progress while you execute your strategy. Re-testing your strategy is necessary because things don't always go according to plan, and the world keeps changing after you develop your strategy. CyberSecPM provides an Early Warning System that helps you detect emerging problems quickly, diagnose them, and make mid-course corrections to ensure success.

Bottom line

We operate in an increasingly hazardous environment for information and systems security. CyberSecPM transforms Cyber Security CMMs from a static benchmarking exercise into a dynamic performance management process. CyberSecPM drives continuous improvement by enabling you to test and validate or refine your Cyber Security improvement strategies across their full lifecycles. CyberSecPM reduces your exposure to critical risks by helping you adopt and sustain best practices in a timely and cost effective manner.

About Decision Path Since 2003, DecisionPath has been at the leading edge of developing custom decision support solutions. We work with leading consultants and system integrators to help businesses and government agencies "test drive" critical decisions involving risk, transformational change, organizational performance, and competitive strategy. The company's innovative solutions help our clients "practice" and improve critical decisions in a safe virtual environment, where they can compare alternatives, explore results based on different assumptions, and uncover and avoid unintended consequences.

Contact Information:
Dr. Richard M. Adler, President
DecisionPath, Inc. **www.decpath.com**
rich@decpath.com **617.794.9036**