

WHITE PAPER



PRESENTED BY:



SOLUTIONS MANAGEMENT:

HOW SOLUTIONS MANAGEMENT AND FORENSICS CONTRIBUTE TO THE SECURITY PLANNING WITHIN THE ENTERPRISE WITH REGARD TO INFORMATION TECHNOLOGY SYSTEMS AND ENTERPRISE BUSINESS FUNCTIONS THROUGHOUT THEIR LIFECYCLE

Nancy Bianco, ISSO
Kevin Kumpf, ISSE

May 9, 2006

INTRODUCTION

Federal Network Services, Inc., Information Security (INFOSEC) Services practice is pleased to present this white paper that describes how establishing a solutions management capability that includes forensics, some design, integration, compatibility testing, and laboratory services acts to increase the viability of the systems throughout the system's lifecycle. Initially, however, there needs to be an understanding of what solutions management includes, how it is defined.

Solutions management is a phrase that describes an overall process or view of processes and their inter-relationship on a local and global scale. The term is used to describe technical as well as nontechnical aspects of the process.

It is a collaborative process, with a goal to mapping or translating specific needs into a plan to meet those needs. In a technical world, the meaning is to map supporting research data into a project, and within that project to translate the data into products and services necessary to support requirements.

Solutions management generally includes several well-defined functions and/or concepts and their terminologies. These include Business Process Commitment Language (BPCL), Customer Relationship Management (CRM), Supply Chain Management (SCM), and Business Process Management (BPM) to name just a few.

Each component of the process is capable of being viewed independent of each other. What is unique about the solutions management process is the ability to take the independent components and view them dependently without losing the relevance of each component. A process, or subprocess, for example, can be viewed end to end; and pertinent data can be gathered without leaning on another component. When that process is viewed in conjunction with different processes and/or components or in conjunction with the exact same process from a different physical location, you have the building blocks for solutions management.

The goal of solutions management is not to provide a magic number or a bottom line result, but to provide better insight as a result of a holistic view into all areas and levels of an organization. This insight can and will mean different things to those involved in the process, but it will open their eyes to other views in the short and long term, and will allow for better solutions to needs and requirements within the enterprise.

This document will focus on the impact of solutions management on Information Technology (IT), and Information Security (IS) systems and solutions.

What solutions management is not is the process of looking at processes solely for the purpose of cost reduction or cost justification, which are pre-conceived reasons for starting the process that describe the intended outcomes.

A pre-conceived agenda and purpose of intent will only cloud "true facts" discovered during the process. What will be discovered, in fact, is not the "true facts", but the desired result. When an IT professional looks at the solutions management process, the professional must look at all areas equally. This means that the weighting will not be influenced (passive result), but that the weighting must influence (active cause) as a result of external, observable factors that cannot be circumvented.

For example, an organization might desire to do what is technologically correct for them and their customers. They have, through due diligence, determined the right solution to meet their needs. Unfortunately, their solution cannot be implemented because it does not meet governmental compliance and regulation requirements that are placed on the enterprise from external controls.

Some may argue that they have failed in the principles and process framework of solutions management. Some may argue that they came to a result that did not take all factors into proper consideration. The sage view is that they came to a pre-destined conclusion based on unequal weighting of the factors and influences. If there is a mitigating process result that cannot be changed or modified, then consider the mitigating process result as a driver of the solutions management process, not a supporting result of the data. If compliance must be met before the beginning of a process, compliance is a driver to achieve. If on the other hand, lack of awareness at the beginning of the process and throughout the process, should result in heightened sensitivity to issues that arise allowing awareness. This process of moving from lack of awareness to becoming aware is considered discovery within the solutions management process and must be weighted differently than they were originally in order to ensure the proper process results.

These are vastly different from going into a process with the core focus requiring cost savings for bottom line organizational enrichment.

SOLUTIONS MANAGEMENT METHODOLOGY

Solutions management is needed in today's secure IT environment. If there is a question, it should not be "Why is solutions management needed in today's secure IT environment?" but "How can your organization function in today's secure IT environment without solutions management?"

In today's environment, IT security needs to be viewed as one of the pillars of IT management and oversight within almost any type of enterprise. Unfortunately, many enterprises view Information Security (INFOSEC) as merely oversight or a "rubber stamp" to seek for completion of a business process or requirement in order to checkmark a compliance box.

This approach is under much scrutiny from internal as well as external sources. The new breed of external forces is not just auditors and governmental regulators as they were in the past, the new external forces are the media and a more keenly aware public.

In the past, it was the norm to have a security breach or incident and not have it leave the enterprise's "inner circle" of knowledge or awareness. In today's society, everything is under the microscope. Employees are aware that they are the true victims of things such as identity theft. It may be the enterprise's name on the front door or public reputation, but it is everyone else's information behind it. Companies don't lose jobs, people do. The advent of tools such as e-mail, Instant Messaging (IM), facsimile (FAX) and even cellular telephones give employees relatively anonymous ways to "get the word out" about what has happened. The Government also is very focused on this current concern and is very eager to introduce new regulations to exert deeper control at a moment's notice; not to mention the fines that will be handed down from multiple agencies.

The driving factors above, as well as the tried-and-true security audits, and common or best practices require a way to correlate the results and to examine the results in order to determine the best approach on all levels. This is a pragmatic view to a theoretical problem. The theoretical problem has always been, "How much money do I need to spend to be secure; and if I spend that money am I truly more secure?"

The answer is that nothing can make an enterprise completely secure (barring burying the IT equipment 15 feet underground, allowing no electrical pulses to get to the equipment, and barring any users from having a relationship with the equipment). No one can provide a dollar amount to attain peace of mind. What solutions management provides is a roadmap, a vision of how to determine the direction to head towards after reviewing all processes and factoring in internal and external drivers.

Steps needed to Begin Implementing Solutions Management

Team Selection

The most critical item to consider in implementing a solutions management approach is trying to ensure an open mind on the part of everyone involved. The process needs to be structured so that all areas of the enterprise and its external partnerships and/or resources are represented equally.

These representations are not just about physical presence, but also about informational, cognitive, and directional presence. Within an enterprise, it is critical to not just have an entity representative "show up", but all individuals must be physically involved in gathering the proper information from all levels within their grouping.

The team members also must be dedicated to this task in a full-time manner when the workload warrants. This cannot be an “after hours” or in their “free spare time” arrangement. As everyone is aware, no one in today’s society has a “free” moment. That time needs to come out of somewhere. Once it comes out of someone else’s “somewhere,” conflicts begin. This also should be viewed by management as something that cannot be reduced to a five-minute effort.

In reality if a person is dedicated to this on a full-time basis, it generally tends to take less time than initially thought. This is because people can complete things more competently and in a more timely fashion when that is their sole focus. The multi-task concept does not work well in certain types of situations, and solutions management is one of the primary ones, due to its need to consume a holistic thought process.

Any team member designated to this task must be given leeway and authority to ask others for help in gathering any required information. This does not mean they require their own staff or should formulate a delegation type role, but should judiciously ask for help in areas that they do not have direct access to information or skills.

The reason this cannot be a delegation-type role is because the person assigned to this function must be active in the meetings and other representations of the team within the group.

If this role is not filled competently and correctly, the results of this process will not be proper and will cause major headaches going forward.

This is particularly true in INFOSEC, where the ability to holistically conceptualize solutions in real time with attacks or at the same level of effort of the attacker(s) is critical to having a successful outcome for the enterprise. In itself, this justifies the need for a solutions management segment in any INFOSEC practice.

Team Manager

Another critical component is the team manager. A solutions management team manager in many cases should be much like the manager of a sports team, rather than like a coach. The team manager needs to be well versed in all areas of business, IT, policy, compliance, and governance. The team manager must be keenly aware of process itself. While a team manager does not need to be as knowledgeable as all the individuals or groups forming and composing the team, the manager needs to rely on and trust the team members. One of the major downfalls of having a coach as opposed to a manager is that a coach is generally involved deeply in all areas of a situation. A perfect example of this is a football coach who calls every play, leads his troop down the field to his marching orders and his decisions. While this is helpful, what truly needs to happen is to have the person be more functional in the manner that a manager of a baseball team is. A sports team manager allows his team to do what they are trained to do, to play the positions in which they are well trained as a result of the coaching staff. The manager watches the play on the field, and generally does not get involved unless situational changes need to be made, such as the acquisition of new players with specialties needed on the field. The manager is a guide and mentor to the coaching staff allowing the coaches to work with the players.

SOLUTIONS MANAGEMENT METHODOLOGY

Data and the Phased Approach

A project needs to have supporting data to understand its requirements as the drivers for the tasks, budget, funding, and timeframe. This accumulates and ensures comprehension of data, processes the data into usable information, formulates solutions (knowledge) that resolve the problems at hand and that conform to policies and compliance requirements of the enterprise, and communicates the solutions and methods to implement solutions to the target audience in acceptable terms. For example, the following phases describe the overall process with Phase 2 having specific applicability to the formulation of any remediation plan. The phased approach can be described as:

- Phase 1 – Accumulate supporting data through:
 - ⇒ Forensics
 - ⇒ Risk Analysis
 - ⇒ Understanding of policies, procedures, and business practices
 - ⇒ Environmental (hardware, software, skill set) analysis
 - ⇒ Understanding of the political environment
- Phase 2 – Translate data to provide a supportable concept through the use of:
 - ⇒ Current plans and architecture
 - ⇒ Current product solutions in place identifying the need to augment or replace
 - ⇒ Technology set to be used with the buy-vs.-build decision criteria defined
 - ⇒ Service skill sets and the decision to perform in house or to outsource
 - ⇒ The understood impact on current business process and practices
 - ⇒ Timeframe allotted
 - ⇒ Budget available
- Phase 3 – Project presentation and acceptance
 - ⇒ Presentation of project concept to management with correlating data
 - ⇒ Proof of concept as needed
 - ⇒ Acceptance procedures
 - ⇒ Plans for purchase, training, implementation, and continued support

As an example:

The CEO of a large e-commerce as well as brick-and-mortar retail corporation sends an edict to all IT and INFOSEC personnel to secure all customer data by November 1. The data includes name, credit card number, Social Security number, and addresses. The driver is Payment Card Industry (PCI) Security Standard from VISA. The credit card houses will be required to perform audits within six months of November 1.

The solution to be developed needs to be considered and incorporated as many of the security policies, standards, and guidelines require the use of that information as furnished from each party to strike a balance between the needs of the business and the security program. Balance in this case becomes a defining factor.

The regulations were written into corporate policy and general business practices. An emergency budget is passed to cover the cost of analysis all the way to problem remediation. Internal and external teams are created to perform both risk and gap analysis. Reports are generated with regard to which business processes will be considered noncompliant.

A solutions management team is created. The Enterprise Security Architect (ESA) is part of the team. The ESA's role as conduit between business, technology, and security is an essential

part of developing a realistic project plan. The ESA must be able to guide the team through the corporate political set up and the process to integrate security control into the organization.

This team should analyze and interpret all the data, specifically answering the following questions

- What are the problems(s)?
- What are the products and services needed in order to put the effort into compliance?
- How should a project plan be created that would not heavily impact the ongoing business processes, stay within policy and practice guidelines, and use in-house products and services as much as possible to keep the cost down.

For this example, risk analysis concludes that the root cause of identified problems was customer data in the clear, unencrypted, from the Point of Sale to the credit card clearing house as well as in processing servers to the backend application servers. Several application and security options were researched. The criteria for choosing a solution were:

- Very little or no application modifications will be required.
- Very little or no modifications to the network infrastructure will be needed.
- Very few changes are required from the standpoint of ease of use and support.
- The solution is scalable as the applications and network grows.
- The selected solution(s) is a common solution for multi-vendor platforms (e.g., Microsoft Windows, UNIX, Linux and Z/os).

Example

For this example, a public key technology solution is determined to be the optimal solution (Solution A), to encrypt the data within the application to the end-point server. However, a whole new infrastructure needs to be developed. Applications will have to be enabled for the public key technology. Directories will need to be heavily used. However, ultimately the solution may be viewed as being overly time and resource intensive, that it will take too long and be way out of budget range.

As a result, another solution is recommended as well. The second solution (Solution B) provides encryption in transit in a manner that allows data integrity protection from end to end. The processing and end-point servers, however, must be hardened.

Solution A is an open source solution with no up front product cost. On the other hand, Solution B is a commercial version that comes with a significant price tag. The ultimate decision may be to run the two solutions side by side; however, the various factors need to be considered. Solution B's processing speed is greater for small transactions, but when larger transactions and amounts of data are used, Solution A is the better performer. The strength of Solution B is that it is feature rich, ported to many platforms and can be centrally controlled.

After testing it is determined that despite the upfront price tag, Solution B product will have a higher Return-on-Investment (ROI) due to ease of use, less network overhead (more processing speed=more transactions=more revenue), standards bases, and auditability. The open source solution had no standard support or development roadmap. Use of a commercial product is favorable to the auditors. The fact that the commercial product can be implemented 10 times faster means the project would meet the November 1 deadline and was a significant consideration.

When the plan is presented, with the ESA's approval, upper management concludes that the Solution B will cost less over a three-year period than supporting Solution A. Since the enterprise was short on resources, the team is asked to recommend a combination of internal staff and outside consultants to train, implement and support the solution.

Data Collection and Sampling

Once the team is established, it is everyone's task to gather the required information from his or her group or department. But data collection is only the first step in this process. Once the data is collected, it needs to be analyzed, compared to time relevance, weighed, formulated, and resultants gathered.

The key to collecting the proper data is to know what you are looking for from the beginning and have the proper person gathering that information. As stated above, if team staffing is not done properly, the solutions management endeavor will be just that, an endeavor that most likely will not be fulfilling for the enterprise or the individuals involved.

Once the data has been collected, it must be converted to information so that it can be understood. Information should not be just a grouping of facts and figures, it must inter-relate to each of the parts and to the environment in which the information will be used.

For example, if asked by management to look over a single firewall log from the past three hours for any anomalies, the task can be completed as long as the person responsible knows what to look for. This all hinges on one key piece of information—"What does management "consider" an anomaly? If management does not know what they are looking for or what will be considered anomalies, how can a solutions manager effectively deliver a proper answer. Variations of this situation must be considered as well in order to further comprehend the time and multiplication factor.

If the situation above is amplified and members of the solutions management team are required to look for anomalies for the past three months and across 10 firewalls at different locations (run by different local staffs), the situation becomes much different.

Fortunately, the practice of solutions management can be applied and the result can be achieved. This occurs by:

- Establishing the goal, determine what is specifically being sought
- Assembling the proper staff
- Dedicating time to the task
- Granting the proper authority to gather information and use resources
- Collecting the required data
- Performing analysis and correlation of the data (on an individual group level)
- Inter-relating the resultant data from each group together to form a team data resultant
- Presenting the unbiased findings to management

Once the data are compiled on a group level, the members of that team must do the formal analysis of the data. Formal analysis is the process of looking at the data and understanding all the factors surrounding it. This includes not only understanding what the data means from a "pure" standpoint, but also anything out of the ordinary that may influence the data initially. A prime example of this might be several business application servers that show nominal Central Processing Unit (CPU) utilization of 35 percent. For this example, assume that during the past week, the CPU utilization on these boxes had been at 65 percent. More information must be gathered to determine the cause of the increase. If this data is just taken at face value, it could potentially skew any results of the process. If an improperly selected person also reviews it, it has the potential to be misunderstood. When the improperly assessed information is added to the information of the other groups it can cause an improper resultant to be achieved just through statistical skewing.

Though many people would not understand how such a simple thing as CPU utilization could cause data to be skewed, to the trained eye this information is critical. This could impact application performance, data transfers, user access, etc. It could also change the results of a

company who was looking at installing a host-based intrusion detection system and that might need to spend financial and staffing resources to do infrastructure upgrades. If determined, for example, that those systems were running at higher rates due to temporary load or stress testing being performed by another department within the enterprise, the data could be discarded as invalid by the individual group and never be injected into the group data.

Team Data Analysis

Once the data has been compiled, it needs to be looked at in a relevant fashion. The weighting of all results must also be equal in all areas. The drivers, which as stated above, are the key overriding factors that must be considered multipliers and that will be used in that capacity. This ensures that the key resultants of the process will rise to the top no matter how many factors are input. The data must never outweigh the drivers; instead, data must amplify drivers, which indicates that there may have been a problem in the data gathering effort. Overriding policies, regulations, and politics must never be viewed as purely input data; they must be considered as drivers to the decision making process.

In the example above, the process was completed successfully, the product was launched successfully in a major part of the world, but yet one key driver was missed and is now considered a global failure or faux paux.

Data Presentation

Once the results have been formulated, debated, reformulated, redebated, and finalized, the results need to be put into proper format from which management can make a decision.

What needs to be clear at this juncture of the process is that the individual team leaders and staff must be released from the process. It is the sole responsibility of the solutions management team manager to pass the information and any resulting recommendations on to enterprise management and to defend and support the recommendations. If the team members are pulled into this part of the process, they are vulnerable to the scrutiny of management. Once this happens, management will start to pick at each team's interpretation of data in a direction that they deem best for their solution. This solution generally does not coincide with the true findings. The solutions management team manager must insulate the staff and also provide the reasoning behind the results.

Many have said to each other on one occasion (or several), "Why should I spend my time and effort presenting the facts, management is going to do what they want anyways!"

If companies are going to go through with a solutions management process they must support the findings and implement them to show all involved that not only their efforts are appreciated, but also their intelligence and decision making. One way to quickly lose employee confidence is to hire people with the acumen and intelligence to perform a given function, and then show a vote of no confidence when they do as asked.

SUMMARY

The goal of solutions management is to develop a practical approach and process to successfully complete a specific project. The aspects of the project will become a working part of the enterprise business process, not just a band-aid for a symptom of a larger problem. A methodology of project management, data collection, and translation of those into a working model to support the requirements for that project will lead to a successful completion as well as act as a model for future projects.

As such, solution management is a key component to ensuring that undo risks are not taken in the process of managing the infrastructure of an enterprise throughout the infrastructure's lifecycle. It allows expertise to be involved in the review and approval of new and upgrade implementations and ensures that the enterprise can always define exactly how the enterprise is pieced together. By using a phased approach with a holistic point of view, solutions management acts as an effective part of INFOSEC, and ensures that the investment in the infrastructure is as efficient as it can be.

The key to a successful IT security program lies in how well systems are documented and evaluated with regard to security issues. Federal Network Systems' INFOSEC Services practice provides a holistic approach to INFOSEC in general and specifically to solutions management efforts for Government and Federally mandated programs for ensure IT systems can be operated safely and securely. In addition, INFOSEC Services provides services that offer Return-On-Investment (ROI) features to increase safe, secure operations of IT systems and to provide for better system protection throughout the life cycle of the system.

For more information, refer to the contact information provided on our Website: www.fnsnet.com and a representative will be happy to provide more information.