

Six Sigma And The Security Plan

Six Sigma

Six Sigma is the constant striving to take what you are doing today and improve it. Can Six Sigma be used for improving security and emergency management? Yes it can. One must start with the DMAIC process taught within Six Sigma as a disciplined approach to project management. DMAIC stands for, Define, Measure, Analyze, Improve, and Control.

Six Sigma combined with a proven Vulnerability Assessment method

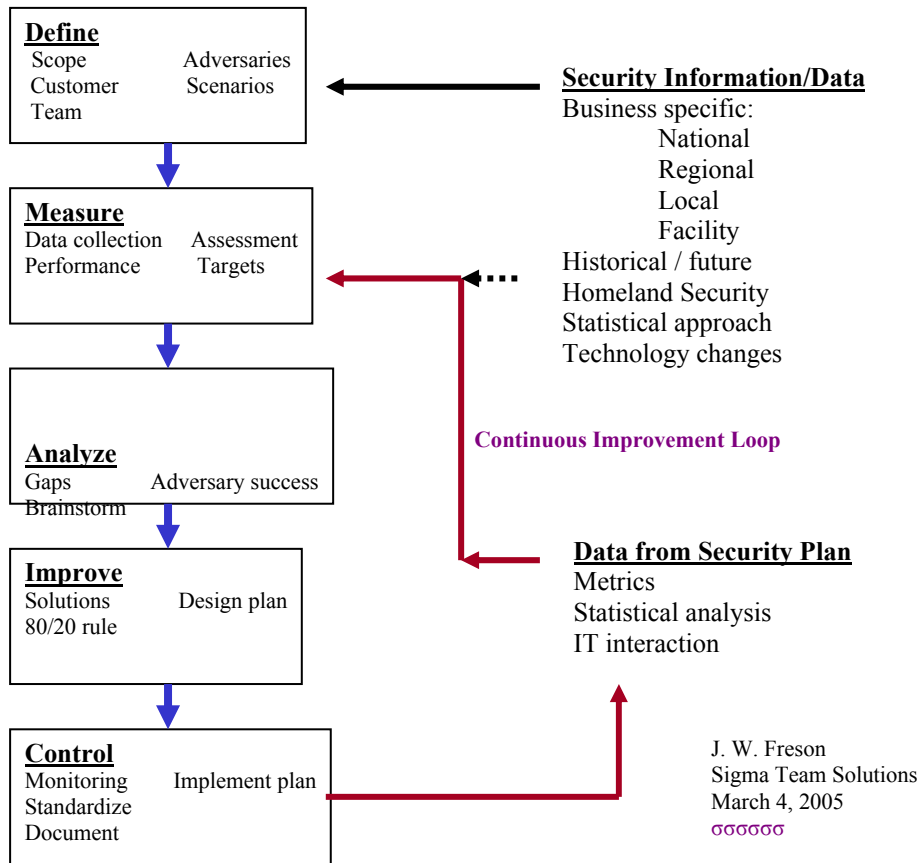
In the area of Security and Emergency Management, we don't just employ the Six Sigma DMAIC process. Since 9/11 there has been several nationally recognized vulnerability assessments developed towards improving IT and physical security. While performing vulnerability assessments, it became apparent that we needed better project management. More importantly we needed to take the assessment all the way to the development of a plan. This was not happening in most cases. The results were some noted need for improvement, but no plan for the future. As Six Sigma looks to include all knowledge, the path forward become one of using the Vulnerability Assessment framework matched to the DMAIC process. The result is a well-disciplined project incorporating the latest knowledge in the security area, which together is designed to give you a Security Plan. The plan will include how to improve security, how to keep the business operating in an emergency, and a method to achieve continuous improvement.

The quest for data

Six Sigma is customer focused and uses the DMAIC project management process. Both of these are an essential part of the Six Sigma methodology. Also important are management commitments to the process, teamwork, and statistical analysis of information. The last will be the most important part of a good Security Plan, a plan that is in constant flux as it pushes towards improvement and the elimination of defects. The use of statistics has one important role and that is to allow us to get more and better information from our data. It will be the driver to guide us towards our improvement goals.

The chart below shows the merging of the DMAIC process with a proven vulnerability assessment format. The assessment format seeks to know who the adversary is and what scenarios may be used to interrupt our business or harm our people. It bases improvement on achieving a balanced and layered security plan. Most importantly, it uses internal and external data. The initial assessment and plan development will use both sources of data. After the initial assessment and development of the Security Plan, the "continuous improvement loop" provides for analysis of how we are doing and gives us the basis for making changes to improve. However, we are only improving based on the external data used in the initial assessment. External factors may, and will change, including new adversaries or information from Homeland Security. Whatever the change, we must bring that information, the data, into our improvement loop. The new information is combined with existing and an assessment is made as to the impact on our plan.

Six Sigma & Security



Conclusion

While Six Sigma will enhance the vulnerability assessment to provide a state of the art Security Plan, one must always realize that the plan cannot be a fixed document. It must not be allowed to become an obsolete plan and any emergency response must be practiced. How often it must change is hard to say, but, if you continuously bring in new information, continuously analyze how your plan is performing, and update it; you will be improving the security of your organization. While most work has been towards physical security, the process is easily applied to the IT world. In fact, a smart company would see the advantages of creating one system, one plan to handle both physical and IT security and contingency planning.

Jack Freson
Certified Black Belt
Sigma Team Solutions, LLC
Associate of: Six Sigma Security, Inc.
www.sixsigmasecurity.us
513-315-4440