In the last four columns, I have been pointing out some of the excellent recommendations from the booklet called *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps* by Gene Kim, Paul Love and George Spafford.

Today I’m reviewing their chapter entitled, “Phase 4: Continual Improvement.” But first, a little historical digression.

William Edwards Deming was born in 1900 in Sioux City, Iowa; he graduated from University of Wyoming in 1921 as an engineer. By the 1930s, he had become fascinated by the applications of statistical analysis to practical problems and he increasingly focused on improving production processes by identifying and applying metrics. He was invited to Japan in the early 1950s to help rebuild Japanese industry; his philosophy of management, which became known as Total Quality Management (TQM) and which was enunciated in his text *Out of the Crisis* included the following Fourteen Points:

1. Create constancy of purpose for improvement of product and service (Organizations must allocate resources for long-term planning, research, and education, and for the constant improvement of the design of their products and services)
2. Adopt the new philosophy (government regulations representing obstacles must be removed, transformation of companies is needed)
3. Cease dependence on mass inspections (quality must be designed and built into the processes, preventing defects rather than attempting to detect and fix them after they have occurred)
4. End the practice of awarding business on the basis of price tags alone (organizations should establish long-term relationships with [single] suppliers)
5. Improve constantly and forever the system of production and service (management and employees must search continuously for ways to improve quality and productivity)
6. Institute training (training at all levels is a necessity, not optional)
7. Adopt and institute leadership (managers should lead, not supervise)
8. Drive out fear (make employees feel secure enough to express ideas and ask questions)
9. Break down barriers between staff areas (working in teams will solve many problems and will improve quality and productivity)
10. Eliminate slogans, exhortations, and targets for the work force (problems with quality and productivity are caused by the system, not by individuals. Posters and slogans generate frustration and resentment)
11. Eliminate numerical quotas for the work force and numerical goals for people in management (in order to meet quotas, people will produce defective products and reports)
12. Remove barriers that rob people of pride of workmanship (individual performance
reviews are a great barrier to pride of achievement)
13. Encourage education and self-improvement for everyone (continuous learning for everyone)
14. Take action to accomplish the transformation (commitment on the part of both [top] management and employees is required).

In *Visible Ops Security*, Kim, Love and Spafford exemplify the principles of TQM as applied to integrating security into all business processes. In Phase 4, they start by recommending the formation of an Information Security Oversight Committee (ISOC) which focuses on “whether information security is meeting the needs of the business.” In my own lectures to students at the undergraduate and graduate level, I never fail to emphasize how important it is that security must *serve* the strategic goals of the organization: we don’t run the show!

The chapter has a good discussion of security metrics, which the authors define simply as “measures that indicate the success of our interactions with various groups.” Their examples include the following (parenthetical explanations are my own):

- Customer satisfaction
- Percent of target operational process integration (how many of the identified processes are now including security considerations)
- Number of challenged integrations (how many processes still have conflicts and problems relating to security)
- Percent of codified process integrations (how many of the processes include formal documentation for the security components)

In addition, say the authors, “There are additional indicators of increasing success that are simple but effective measures of progress:

- Invitations to meetings….
- Soliciting of information security input….
- Reduction in frequency of audits, audit preparation effort, and remediation efforts associated with audit findings….”

The authors then systematically present detailed, concrete suggestions for metrics relating to each of the phases enunciated in the *Visible Ops Security* framework. By the end of the chapter, they sketch out what a mature organization should be seeing once the recommendations are implemented and continuous process improvement has become part of the culture: “We are now more integrated with foundational-level activities within the organization, allowing us to target more advanced activities and processes, such as automating some of the processes we have built. For example, through our involvement with SDLC [System Development Life Cycle] we can create automated components (such as MS Project tasks) to give to project managers that are rebuilt on adaptive self assessments.”

Finally, the write, they hope that readers will hear this kind of summary: “Information security is no longer thought of as an outside entity nor does information security have to fight for involvement. We find we are becoming involved in more project and strategic discussions instead of being involved only when problems are discovered. When information security is automatically and without a second thought included in future operations planning, we know we have become part of the team.”

Go forth and read this book. Then start implementing its methodology! And may the Authors be with you.
M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.