Best Practice Adoption: 
Fact or Fiction?

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Regular readers of my column will know that a leitmotif of my professional life, which includes applied statistics, is that we simply don’t have enough solid information about the facts surrounding information assurance events. My colleague Prof Sharon W. Tabor, PhD, Chair of the Networking, Operations & IS Department at the College of Business & Economics of Boise State University is trying to change that. Here’s an interesting project through which readers can significantly contribute to progress in our field. Here’s Dr Tabor’s introduction.

* * *

With all the talk in the press about information assurance, IT governance, and compliance, one might assume that everyone has adopted one or another of the major governance methodologies such as ITIL, CMM, or COBIT. The tactical implementation of those policies takes the form of best practices, a familiar term in the IT world. Security is certainly a major driver toward best practice adoption, along with compliance with legislative action or the threat of zealous auditors. Best practices supposedly offer many benefits. For example, a survey of IT executives in 2004 found that organizations who implemented best practices rated themselves as having higher status within the overall business. Additionally, they were successful at justifying higher budgets to address security issues, and were looking at security in terms of a long-term, risk-based strategy, with fewer security incidences overall.

On the other hand, it appears that not everyone agrees with the need for best practices. In addition to success stories about large company experiences with best practices there is also preliminary evidence that suggests many small and medium-sized organizations continue along their daily activities, putting out fires and remaining predominantly reactive. Whether due to the complexities of the methodologies, or overall lack of time and resources, many organizations don't seem interested in adopting new processes. Others aren't convinced there is a reason for best practices. David Lawson, for example, (Network World, 5/30/05) argues that security best practices don't exist, and if they did the cost would be way too high for most organizations. He discusses the use of good practices, minimal acceptable standards, and appropriate and reasonable controls.

I am conducting research into this controversial topic. I was a middle manager for many years, and my research goal is to separate reality from the trend-setting buzz words that are attached to our field. The survey at the link below queries who has adopted which methods and what the drivers and benefits have been. Survey responders will receive a white paper with an examination of each of the major methodologies, and more important, the perspective from which they have been developed. Finding a perspective that addresses organizational needs more than any other single factor, can help narrow down the choices and yield the desired benefits. Organizations of all sizes can benefit from IT governance and best practice development, but the key is in finding the right fit.
I (Mich) spoke with Dr Tabor and asked her how the research is going. “The response has not been what I had hoped. People are tremendously tired of doing surveys, but this is a really important area. The whole IT governance problem really needs some solid facts and this survey could really be important in identifying key issues that organizations are dealing with.” I asked how this survey would avoid the classic pitfalls of voluntary participation in online surveys – misleading results and biased sampling. Dr Tabor confidently answered that the questions focus on the basics of what organizations have done, which methodologies they have used, and what’s worked for them, thus avoiding the problems of typical opinion-oriented research. She said, “We also included some internal validation measures typical of good surveys.”

Click on <http://telecomm.boisestate.edu/research/BPsurvey.asp> to begin the survey and sign up for a copy of the results. In addition to the white paper, respondents will be entered into a drawing for electronic gift certificates. Please spend a few minutes to do some good for the field and then see what others are doing to get IT security and services under control.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 S. W. Tabor & 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.