Reality Trumps Theory

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

A local reporter spent eight hours interviewing students and faculty in the computer science< http://programs.norwich.edu/business/computerscience/ > and information assurance (IA)< http://programs.norwich.edu/business/csia/ > programs at Norwich University< http://www.norwich.edu > a couple of days before I began writing this article. At one point, he asked half a dozen of our students what they felt was special about their education in the School of Business and Management< http://programs.norwich.edu/business/fac-bus/ >. One young man responded immediately that the focus in our programs is service to organizations in furtherance of their mission-critical objectives; in contrast, he said, he had the impression that some of the students he had met from well-established programs at other institutions participating in various computing and security competitions were focused primarily on details of technology. "People use technology to achieve business goals," he said, "not just because technology is interesting and fun." Another student laughed and pointed at me: "Prof Kabay has drilled us in every course with his motto, 'Reality trumps theory.'" Students nodded and explained that they had learned never to solve problems by applying rote learning as if recipes and checklists could be applied without careful consideration of the specific requirements of any situation.

I was delighted to see that my brainwashing, er, education in principles was having such an effect on our students. The phrase "Reality trumps theory" became the motto for the master's program in IA< http://infoassurance.norwich.edu/ > that I designed and helped to establish in 2002. As the students correctly explained, I have a deep suspicion about absolute rules divorced from the particular details of the problem confronting us. For example, one can easily find a perfectly good principle being turned into rigid dogma; consider "Change your password frequently." I have encountered organizations where the IA or IT staff have dictated monthly changes in logon passwords despite the consequences: employees either chose a ridiculously simple, easy-to-guess passwords or they wrote down complex passwords on papers and stuck them in obvious places such as underneath their keyboard or inside a desk drawer. Bruce Schneier, in contrast (and as usual) takes a far more intelligent attitude to changing passwords.< http://www.schneier.com/blog/archives/2010/11/changing_passwo.html > For example, he concludes his thoughtful review of the question with the following well-reasoned advice:

> "So in general: you don't need to regularly change the password to your computer or online financial accounts (including the accounts at retail sites); definitely not for low-security accounts. You should change your corporate login password occasionally, and you need to take a good hard look at your friends, relatives, and paparazzi before deciding how often to change your Facebook password. But if you break up with someone you've shared a computer with, change them all."

What a contrast with "You must change your password every 30 days and that's all there is to it." The discussion at the end of the article includes many thoughtful postings from readers, most of whom seem to me would agree with the principle that "reality trumps theory."

IA is a balancing act: we must constantly weigh benefits against costs – and I'm not just talking about direct financial costs. Despite our heartfelt yearning for quantitative risk management, we are stymied by the lack of an adequate statistical base for annualized loss expectancies (ALE< http://www.riskythinking.com/glossary/annualized_loss_expectancy.php >). We have neither accurate frequency data for specific problems nor accurate data about monetary losses. As I Have explained for decades< http://www.mekabay.com/methodology/crime_stats_methods.pdf >, information security breaches suffer from the problem of ascertainment (we may not notice a breach at all or not for long time) and the problem of reporting (we have no centralized data collection facility and victims may choose not to report breaches and costs to anyone). Using best practices and formal standards make sense, but no set of prescriptions can be applied as if we were following a recipe.

One of the resources in security-policy development I have used since the 1980s is the evolving series, "Information Security Policies Made Easy" by Charles Cresson Wood (ISPME< http://www.informationshield.com/ispmemain.htm >). Now in its 12th edition, ISPME consistently emphasizes importance of adapting the recommended policies to the specific needs of the customer. I opened my copy of the 10th edition at random and immediately found the following example of Wood's emphasis on thoughtful application of policy rather than dogmatic rigidity:

> 2. Performance Evaluations
>
> Policy: Compliance with information security policies and procedures must be considered in all employee performance evaluations.
>
> Commentary: This policy requires management, at the time they write performance evaluations, to decide whether the involved employee has been be concerned about information security, and if the answer is yes, then to determine whether the employee has acted in compliance with policies and procedures. The policy provided here makes direct reference to the management activity of evaluating employees, and only indirectly to a rank-and-file employee activity of complying with policies and procedures. Nonetheless, it implies that both are expected by management. The words "information security policies and procedures" could be changed to "information security requirements" or other generic terms used at the organization.
>
> Related Policies: "Information Security Responsibility" and "Information Security Liaisons."
>
> Audience: Management
>
> Security Environments: All

In my career, I have been saddened to see IA being damaged by authoritarians who refuse to discuss policies with concerned users. These people act as if their primary goal is enforcement of their initial conception of appropriate security, impervious to warnings that their initial conception is wrong and uninterested in changing circumstances that render their absolute rulings ineffective by any standard. These autocrats enrage their customers – and yes, I always use the concept that information technology and information assurance should consider the user community their customers – and result in widespread contravention of their inappropriate policies.

In closing, I want to remind readers that one of the most effective tools for establishing well-received security policies is to explain the reasons behind every policy. Charles Cresson Wood has used this technique throughout his work, as exemplified in the commentaries for every suggestive policy in his magisterial text. When I ran my own consulting firm, the company's motto was "Progress Toward Autonomy" and I required every contract to include a specific person with whom I could discuss every step of the performance optimization, operations management restructuring, or security assessment for which I was being paid. In my teaching, every recommendation, every principle is explained, not dictated; I constantly urge my students not to memorize, but to integrate knowledge.

Life is not a computer game with rigid and predictable rules; life is a multidimensional manifold that changes all the time.

Reality trumps theory.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *