IA Policies (2):
Fair vs Arbitrary Flexibility

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

How do we resolve the issue of acknowledging (to ourselves) that some of our information assurance (IA) policies cannot, or should not, be strictly enforced, while at the same time conveying to staff the importance of always following IA policies?

This is the second of two articles by friend and colleague Adjunct Professor Richard Steinberger, CISSP, CISM from the MSIA Program<http://infoassurance.norwich.edu/> at Norwich University<http://www.norwich.edu> looking at rigidity or flexibility of security policies. What follows is Ric’s work with minor edits plus a question I posed to him in our discussions of his original text.

* * *

Every IA policy developer, implementer and enforcer needs to maintain perspective as to which are the most serious policies – ones that it is vital be followed at all times by all staff – and which policies may be allowed to have some modest amount of flexibility (wiggle room) in how they are deployed and enforced.

Here’s the trouble: We can’t explicitly tell staff members that these are the policies you need to strictly obey all the time, while those are policies that we don’t enforce as much, so they should use their own judgment.

Where certain activities are prohibited by IA policy, but it’s simply not viable, desirable or cost effective to track down every violation, the optimal enforcement language may be something like, “Activity X is not allowed. The organization reserves the right to monitor staff for compliance and to implement appropriate disciplinary action when violations are detected.” Such an approach provides clear notification to staff as to their responsibilities, and leaves the door open for whatever flexible policy enforcement IA staff may chose to deploy. This way, we can ignore Joe, or give him a warning, or revoke his license (terminate him).

[MK asks:] It’s an interesting idea, but inconsistent enforcement of policy is a dangerous trap. <http://www.mekabay.com/infosecmgmt/personnel.pdf> Employees who are punished for the same violations for which other employees are not punished may decide to hire an attorney and initiate legal proceedings such as wrongful dismissal (aka wrongful termination) and discrimination lawsuits. For a list of the bases on which employees can file such suits, see Ellen Simon’s Employee Rights Post. <http://www.employeerightspost.com/> I’d much rather see clear, unambiguous and
uniformly enforced policies that reflect a realistic and flexible appraisal of the strategic objectives of the organization and a sound risk management philosophy.

[RS replies:] There are at least two ways to interpret this:
1) Some policies are "always" enforced, while other policies have more wiggle room, and
2) Some staff members are allowed to bend policy while others are selected for enforcement actions.

Case 2 is highly undesirable, and as you point out, may lead to legal issues. Case 1 is simply policy enforcement in the real world, where economics, staffing issues, technical limits and practicality place constraints on IA staff's ability to enforce all policies all the time.

To use the traffic analogy: It's considered acceptable if the highway patrol allows some degree of speeding, under certain conditions, allowing for traffic density, weather, road conditions, etc. It's considered far less acceptable, and generally illegal, if law enforcement selectively identifies expensive sports cars, or cars driven by people of specific ethnicity or gender, for enforcement actions.<http://www.counterpunch.org/drivingblack.html> We don't seem to mind if the patroller stops the fastest car, while allowing slower, but still speeding vehicles, to drive on. But we do – or should – get upset when cars are selected for ticketing because of the make or model of the car, or the complexion of the driver.

Similarly, flexible enforcement of IA policies must never become an exercise in arbitrary application of power.

What do you think? This is a particularly vexing problem and we welcome your comments in the public discussion area.

* * *

Richard H. Steinberger, CISSP, CISM has over 20 years of hands-on and supervisory experience with computers and networks with special expertise in Internet and network security; security principles and products including firewalls, routers, VPNs, vulnerability assessment tools, intrusion detection systems, and hacking tools; advanced UNIX software development; and system administration. He has taught network security at University California Berkeley Engineering Extension and for several years as Adjunct Professor of Information Assurance in the MSIA Program at Norwich University. You may reach Ric by e-mail.<mailto:ricsteinberger@gmail.com>

* * *

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 © 2009 Richard Steinberger & 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.