IA Policies: Do we Allow any Wiggle Room?

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?

My friend and colleague Adjunct Professor Richard Steinberger, CISSP, CISM from the MSIA Program<http://infoassurance.norwich.edu/> at Norwich University<http://www.norwich.edu> recently raised the issue of rigidity of security policies and how employees get around those policies. I invited him to expand on his thoughts; everything that follows is entirely Ric’s work with minor edits.

* * *

A recent article<http://lifehacker.com/5302841/use-gmail-drafts-to-mail-yourself-unallowed-files> asked readers the following question: “Got your own file-sending solutions for places where the filters are strong? Tell us all about them in the comments.” The context was a story about an employee who had used Gmail to send himself material that his organization’s deployed IA policy was blocking. Many Lifehacker readers happily contributed their not-especially-sophisticated approaches, such as, “Use https instead of http,” or “Zip the document, and then add a password,” or simply, “Change the file suffix to something that doesn’t get filtered.”

The Lifehacker article helps remind us of a few important points, including:

1) No matter what an organization’s IA policies are, some staff members convince themselves that they have a legitimate need, even a right, to bypass them;
2) Unless an organization’s IA policies reflect the existing business culture, then at least some staff members will feel they have a right or even a need to ignore some of these policies; and
3) Employees, i.e., insiders, can be quite skilled and persistent at discovering new approaches towards subverting, ignoring or going around inconvenient policies.

Consider an analogy with traffic laws (i.e., policies). Does this sound like someone you know? Joe (or Joan) always comes to a complete stop at red lights. At stop signs, Joe reduces his speed to about five MPH, and if it’s clear to cross the intersection, he speeds up and drives through. On the highway, where the speed limit is posted as 65 MPH, Joe usually drives about 70 - 75, especially if other drivers do the same. Joe recently purchased a radar detector to notify him of local policy enforcement zones. Joe’s been driving for many years and receives an insurance discount that reflects his safety record.
Almost all of us have employees like Joe where we work (and indeed, we may even be a Joe or Joan). We do our best to create and deploy IA policies that:

1) Keep the organization in compliance with statutes and regulations,
2) Make sure that our organizations follow our own rules (e.g., we will strictly limit access to customer data),
3) Follow best practices for our industries, and
4) Implement any special requirements we may have (e.g., protect our intellectual property, require strong passwords).

As IA professionals, we would be naïve to imagine that Joe doesn’t work as he drives: Joe understands the traffic laws, and bends them when he judges it’s in his best interests to do so. If he is a good employee, he may bend our security policies when he judges it’s in the organization’s best interests. The question we should be asking ourselves is not, “How do we find and discipline (or fire) Joe?” Instead, we should think about these issues:

- To what extent do our IA policies reflect our business values and culture? Have we done our best to make sure that staff understand specifically those polices which will frequently seem to be especially inconvenient?
- How tolerant/flexible are we prepared to be with policy infractions and how much effort are we willing or able to spend on detecting them?

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 adds: 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. In the next article in this two-part series, Ric Steinberger and I propose examples of how to adapt policies in the face of changing business needs or of new understanding of employee functional requirements.]

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.