Reality Trumps Theory:
GAO Strikes Again, Demonstrates Weakness of FPS

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

One of the mottos of the Master of Science in Information Assurance (MSIA) Program<http://infoassurance@norwich.edu> at Norwich University<http://www.norwich.edu> is “Reality Trumps Theory.” This mantra means that book-learning is great, but actually looking at how the world works is better.

One application of the mantra in the MSIA is the case study<http://infoassurance.norwich.edu/case_study.php> which every student must complete; our expectation is that students will confront contradictions between what experts are writing in their study materials and how their case-study organizations are actually performing information assurance (IA) tasks. These insights provide depth and perspective to our students.


Report GAO-09-959T was released on July 8, 2009. It is of “Testimony Before the Senate Committee on Homeland Security and Governmental Affairs” by Mark L. Goldstein, Director of Physical Infrastructure Issues and is entitled “HOMELAND SECURITY: Preliminary Results Show Federal Protective Service’s Ability to Protect Federal Facilities Is Hampered By Weaknesses in Its Contract Security Guard Program.”<http://www.gao.gov/new.items/d09859t.pdf>

GAO investigators carried out a vulnerability analysis of the physical security measures being enforced largely by security guards working for companies on contract to the Federal Protective Service (FPS)<http://www.ice.gov/pi/fps/org_hfs.htm>, whose “mission is to render federal properties safe and secure for federal employees, officials and visitors in a professional and cost effective manner by deploying a highly trained and multi-disciplined police force.”

Although one can hardly refer to the main points as highlights, here are some of the salient findings of the penetration study:

- Despite written standards for training and certifications required to operate x-ray and magnetometer (metal-detector) equipment, many guards have not received adequate or indeed any such training.
- Out of 663 randomly selected guards, 62% “had at least one expired certification including a declaration that guards have not been convicted of domestic violence, which make them ineligible to carry firearms.”
- The FPS has no systematic program of inspection.
In 10 tests at secure federal government facilities (including “offices of a U.S. Senator and U.S. Representative, as well as agencies such as the Departments of Homeland Security, State, and Justice”), GAO inspectors were able to pass materials for making bombs which they then assembled and carried around in a briefcase without being challenged.

Reaction to the report was vitriolic, but I want to focus readers’ attention on the lesson for security officers and network administrators.

First, security must be more than what Bruce Schneier has called “security theater” in his 2003 book, Beyond Fear: Thinking Sensibly about Security in an Uncertain World. For an analysis of security theater in airport security, see my 2005 paper. Going through the motions of securing our organizations is equivalent to building a Potemkin village: a sham that presents the illusion of security without effectively improving it.

Second, outsourcing security functions raises issues of commitment and supervision. A firm under contract may have even more pressure to reduce costs (e.g., by reducing training and certification) given the fundamental difficulty of knowing whether the lack of security incidents is due to good security, luck, or inadequate recognition of security incidents.

Third, there is no substitute for penetration testing. When was the last time you performed a vulnerability analysis of any type on your systems, including technical penetration analysis and social engineering tests? The latter should ideally be performed on a prepared workforce, as Dr John Orlando explained in a series of articles in this column in 2007:

Social engineering in penetration testing:
- Cases
- Analysis
- Planning

However, the principle is that no matter how confident we are of the wisdom and suitability of our security measures, we need to see how (or if) they are working.

Reality trumps theory.

***

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are “Introduction to IA for Non-Technical Managers,” (July 18-23) and “Cyberlaw for IA Professionals.”(Aug 8-13) Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you
online!

* * *

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 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.