Training…Asset or Risk?

As security professionals, we are accustomed to identifying assets and protecting them. We are also familiar with the process by which this is accomplished: identify our assets, identify the threats to those assets, assess our vulnerability to those threats, and – finally – manage the risk by decreasing the threat or vulnerability.

Most of us are also accustomed to assuming that our own professional training, and the training of our team members, is a key tool in the ongoing process of reducing the risks faced by our organization. This is certainly the case, but it is equally important to recognize the ways in which the converse can be true. Inadequate training is, in and of itself, an *additional* risk factor, and – as with more traditional threats – we need reliable means of assessing the risks posed by inadequate training.

This is particularly true considering the significant developments that have taken place over the last few decades in the various areas which comprise security management. In every area, from IT to patrol, the expectations for security professionals have changed dramatically. If your training methods and protocols have not kept pace, and if you have not updated your means of evaluating those procedures, then your training program could prove more of a liability than an asset. All security organizations can benefit from a structured, formal approach to assessing the effectiveness of the level of training within their workforce.

Although the methods and mechanics of that assessment must adapt to changing environments, the basic principles are well established. Thirty years ago, Dr. Norman Bottom published an innovative systems approach to security management, in which he identified "Training" as one of the tripartite fundamentals of loss control, and along with that observation he introduced the acronym WAECUP:

Waste
Accident
Error
Crime
Unethical **P**ractices[1]

The WAECUP model asserts that these variables, and their inter-relationships, are at the heart of what security professionals must protect against. A loss due to any one of the above variables has the potential of escalating into additional losses, not the least of which may be those associated with subsequent civil litigation. One means of assessing the efficacy of a training program, therefore, is identifying whether or not it is sufficiently comprehensive to address potential threats and vulnerabilities associated with *all* of the identified categories.

In addition to this general framework, it is important to assess training in terms of measurable standards. When I conduct an assessment of an organization's training, I

typically ask three initial questions to determine whether or not their personnel are properly trained. I'm sure it is not always the case, but it has been my experience that the organization's approach to training is likely to be risk-laden if the answer to any of the following questions is "no."

1. **Is requisite training based upon currently published guidelines and standards?**
2. **Is there evidence validating that members of the organization possess the knowledge, skills and abilities expected or required of them?**
3. **Are the training programs reviewed and updated by qualified experts?**

Complying with Guidelines and Standards

It is beyond the scope of this article to enumerate the vast number of valid sources for guidelines and standards. They range from state laws to professional accrediting bodies, and they include published research regarding "best practices" and industry norms. It is nevertheless incumbent on every security professional to seek out those sources and translate them into clear, documentable, assessable guidelines for organizational training. Put simply, if a recommended guideline exists and is relevant to our operation, failure to apply that recommendation makes us vulnerable to WAECUP and/or civil litigation.

The first place to start is government guidelines. Many training programs, even in national organizations, are still relying on the conclusions of the earliest studies on security procedures: the Rand Study (1971)[2] and the National Advisory Commission Report (1974)[3]. Although these studies were groundbreaking for their time, over the past forty years many state and federal agencies have moved far beyond the foundation laid by this early research. It is incumbent on all security professionals that they continually research the constantly-evolving federal and state guidelines relevant to their organization, and then assess their training accordingly. At a minimum, this should include familiarity with:

- Occupational Safety & Health Administration (starting with the "General Duty Clause")
- National Institute of Standards and Technology (starting with the "FISMA Implementation Project")
- National Incident Management System; and
- Sarbanes-Oxley Act (especially relevant for IT security requirements)

This is only the beginning. In addition to government guidelines, security professionals also need to regularly evaluate the relevance of recommendations published by other entities. Although these publications cover a wide range of specialties, the ones that are relevant to the assessment standards I recommend must all meet a common criterion. They are all developed through an in-depth process of research, discussion and expert consensus. The flow chart included in this article illustrates one example of that process [*see chart, p9:* http://www.asisonline.org/guidelines/docs/SGquickReferenceGuide.pdf]. As a starting point, all of the following are useful sources:

- The ASIS International *Private Security Officer Selection and Training Guideline* (guidelines for contract and proprietary security personnel)
- The International Organization for Standardization (ISO) 27000 series (guidelines for managing physical and informational security)
- The National Fire Prevention Association (NFPA) 730 (recommendations regarding Premises Security considerations for various venues; includes training recommendations); and
- The National Fire Prevention Association (NFPA) 731 (relates to the installation of electronic premises security systems)

This list is far from exhaustive, but it does provide a starting point for assessing the currency and liability of an organization's training criteria and protocols.

Verifying Training

Once an organization's training criteria have been determined to be consistent with industry and government best practices, the next step is ensuring that the procedures for training the workforce are sufficient to meet those criteria. Traditionally, this means identifying the *knowledge*, *skills*, and *abilities* ("KSA") necessary to reach the established standards, and then establishing reliable means for assessing those KSA.

It is not enough simply to assume that someone possesses requisite KSA just because they have years of experience or have completed certain training modules. How many times have we interviewed someone who had "one year of experience, repeated ten times," as opposed to ten years of experience? Or, have we not each encountered someone who had a stack of certificates reflecting "training sessions attended," but their professional competency did not reflect any of it. The assumption that training has resulted in competency must be tested – literally.

A Criterion Referenced Instruction (CRI) framework provides an excellent option for providing and assessing training within the security field. As developed by Dr. Robert Mager, it begins with an assessment phase (as mentioned above, identifying applicable guidelines and essential KSA). Once the training needs have been identified, a program of instruction is designed to meet those needs, and testing is administered to evaluate whether the trainee has met the objectives.[4]

Though an organization may develop their own CRI-based training agenda, there are plenty of existing CRI-based options, and combining internal training with external resources may prove beneficial to many organizations. External training resources include everything from traditional classroom instruction to online distance learning, and specific courses are available ranging from introductory training through advanced academic degrees. There are advantages to each, but online training has gained much popularity in recent years, due largely to improvements in technology and an increase in content availability. John J. Fay, CPP (former Director of the National Crime Prevention Institute and the founder of an online security training service) notes that, "online learning is a standard instructional method in nearly every teaching institution in the United States, from 6th grade to the PhD level." In addition, he points out that online

training "automatically keeps records of scores, courses completed, and other data that must be available for inspection by a regulatory agency." This greatly eases the burden on organizations for documenting training.

In addition to specific CRI-based tests, there are also well-respected, international exams which offer comprehensive test batteries to assess a security professional's experience and mastery of a broad set of relevant knowledge. These exams offer certifications which can be used as objective assessments of the relevance and effectiveness of a team member's training.

ASIS International offers the following individual certifications:

- **Certified Protection Professional (CPP®)** - demonstrated competency in all areas constituting security management
- **Professional Certified Investigator (PCI®)** - demonstrated education and/or experience in the fields of case management, evidence collection, and case presentation; and
- **Physical Security Professional (PSP®)** - demonstrated competency in conducting threat surveys, designing integrated security systems that include equipment, procedures and people, or installing, operating and maintaining those systems.[5]

In addition, the International Society of Crime Prevention Practitioners offers the **ICPS (International Crime Prevention Specialist)** designation, indicating competency in a published body of knowledge relative to preventing crime.

For those whose responsibilities include information security, The International Information Systems Security Certification Consortium, Inc., (ISC)²®, offers several certifications, including:

- **Certified Information Systems Security Professional (CISSP®)** - mid and senior level managers who develop policies and procedures in information security
- **Systems Security Certified Practitioner (SSCP®)** - Network Security Engineers, Security Systems Analysts, Security Administrators and personnel in other non-security disciplines that require an understanding of security but do not have information security as part of their primary job description; and
- **Certified Authorization Professional (CAP®)** - those responsible for formalizing processes used to assess risk and establish information security requirements.[6]

As with the previous section, the above-referenced resources are not intended to be an exhaustive list, but rather a summary of *some* of the ways we can meet the training verification need.

Reviewing and Updating Training

Once appropriate training has been identified, provided and verified, the final phase is to provide a mechanism by which the process can be evaluated and revised as appropriate. Threats and vulnerabilities change and evolve, and individuals retain or lose information at different rates. Assessment of training, therefore, must be an ongoing process which allows for review of individual levels of competency. This process can include:

- Performance Evaluations (based on criteria established on relevant standards and norms)
- Re-testing
- Practical Exercises (based on relevant threats and vulnerabilities)
- Evaluation of Exercises and/or Objectives by Outside Consultants

Conclusion

Inadequate training presents vulnerability for any organization, and security professionals must treat it as they would any other vulnerability. One familiar problem solving model for assessment is SARA (Scanning, Analysis, Response and Assessment), and this model is easily adaptable to the process I have already described of making sure that adequate training standards are established, implemented, and verified:

- **S**canning **–** determine the various missions of your organization and identify relevant knowledge, skills and abilities
- **A**nalysis **–** identify regulations, standards and guidelines relevant to your training needs
- **R**esponse – develop training objectives; administer and verify training
- **A**ssessment – determine whether objectives are being met and revise as needed

It is to be expected that the "Assessment" phase will often identify new areas of training, or areas where re-training is needed. Whether we employ this model or use some other methodology, this phase is an important part of ensuring that training objectives are current and that our workforce is comprised of appropriately trained personnel. In fact, this final step (Assessment) may be considered the first step in beginning the whole process again. As with many palliative interventions: "repeat as needed."

Endnotes

[1] Bottom, N., & Kostanoski (1981). *WAECUP – An Explanation*. Journal of Security Administration, 4 (2), 5-10.

[2] The Rand Corporation (1971). Private Police in the United States: Findings and Recommendations. Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration.

[3] National Advisory Commission on Criminal Justice Standards and Goals (NAC-CJSG) (1976). *Private Security: Report of the Task Force on Private Security*. Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration

[4] Mager, R. (1975). Preparing Instructional Objectives (2nd Edition). Belmont, CA: Lake Publishing Co.
[5] ASIS International Online. Retrieved from http://www.asisonline.org/certification/index.xml.
[6] The International Information Systems Security Certification Consortium, Inc. Retrieved from https://www.isc2.org/credentials/default.aspx .