Awareness and Ethics in the Operations Environment

Applications within Department of Defense (DoD) Vendors

Andrew Bruce, CISSP, PMP, FITSP-D
CTO, RiVidium Corporation (http://www.rividium.com/)
andy.bruce@rividium.com
29 December 2010

Topic Summary:

- Characterize security awareness (and formal programs) in our industry
- Highlight operational support for security awareness and ethical decision making
- Identify advantages of and recommend improvements for security awareness programs

Table of Contents

About the Author....3
1.0 Introduction....3
2.0 Why the Worry?....3
3.0 The DoD Fights Back....4
4.0 Recommendations....10
5.0 Acronyms....11
Reference List and End-notes....12

Illustration Index

Figure 1: A world of awareness at IASE....5
Figure 2: NIST Security Awareness Training Model....7
Figure 3: SAT Lifecycle....8

About the Author

Andrew Bruce is Chief Technical Officer for RiVidium Incorporated, a Service Disabled Veteran Owned Small Business in the suburban Washington, DC area. RiVidium provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that leverage our proprietary technologies. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing RiVidium's network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers.

1.0 Introduction

Working in the Department of Defense (DoD) demands providing excellent results, utilizing strong security measures, delivered in a cost-effective way. The DoD has high standards for industry and the great majority of industry vendors take pride in exceeding requirements, especially when it comes to security awareness and ethics. As a defense contractor, DoD principles, regulations, and best practices guide our security policy. In this white paper, we analyze how DoD's practice and approach to security awareness training and ethical decision-making helps to make the entire defense community safer.

Such an approach to security awareness and ethics doesn't just assist the DoD in achieving its mission, by any means. By using a high standard of training, the DoD helps to ensure that this level of commitment is reflected throughout the Federal Government. The Executive branch has recognized the need for standardized training programs and standards by empowering the National Institute for Standards and Technology (NIST) to create guiding documents, and these documents both influence and have been influenced by DoD training initiatives. This type of self-improving feedback loop adds to the overall level of ethical decision-making within Government, ultimately leading to a better governing and working environment for all Americans.

2.0 Why the Worry?

"Colleagues, as you may be aware, several news organizations are about to publish stories on hundreds of thousands of stolen classified State Department documents."[*] Bryan Whitman had to announce this on November 28, 2010 as the latest Wikileaks fiasco showed just how big of a problem the Computer Information Technology Insider (CITI) remains and why Dr. Jerrold M. Post considers that insiders represent the greatest threat to systems.[1]

The DoD agrees with Dr. Post; particularly in that the first (and last) line of information defense is a human being. That human being needs to be armed with an effective security awareness program powered by a reliable Operations department.

Security awareness programs address more than just the malicious insider threat; sophisticated modern attacks

[*] Bryan Whitman, *Wikileaks Briefing* (Office of the Assistant Secretary of Defense, Public Affairs: 28 November, 2010). Available at http://tinyurl.com/2bdf52r (accessed: December 9, 2010).

defeat even strong network firewalls simply by targeting users outside the protected corporate enclave. Consider a site like Facebook, filled with prospective DoD targets, all of whom are busy putting as much personal information online as they can. This scenario simply begs for a criminal to socially-engineer access to these pages and to scrape data to his heart's content. Considering the ease with which user IDs can be guessed combined with the fact that most people base passwords on birthdays, children's names, or interests then at least a few logon credentials will emerge.

The need for security awareness expands into every aspect of our interaction with technology. One topical news event concerns the just-recently raised ban on USB sticks within DoD (the origin of which was due to an infected USB containing the SillyFDC worm being plugged into a military network.)[**] That type of failure (inserting infected media directly into a military system) correlates directly back to a failure in the security awareness program.

3.0 The DoD Fights Back

We contend that effective Security Awareness Training (SAT) makes the best defense against information security breaches (as one popular poster proclaims, "There is no secUrity without U"). While an exhaustive review of all of the security programs currently in use within DoD would fill more than a few books, in this section we cover some of the ways that DoD and industry are preparing their workforce to anticipate, recognize, and defuse the threats posed by malicious insiders and online thieves.

3.1 Formal Awareness Programs and IASE

As guardians of the Nation's national security data infrastructure, workers in the DoD community have a special obligation to demonstrate that they understand security awareness and ethical decision-making. Moreover, having excellent awareness and training resources counts for little without having an equally excellent Operations infrastructure in place to deliver, monitor, and record the results.

The Information Assurance Support Environment (IASE, http://iase.disa.mil) provides the starting point – and the general public can access and run many of the links from the **Online IA Training** option without a password.

[**] Kevin McCaney, "DOD lifts ban on USB drives," *Federal Computer Week*, February 22, 2010.

Figure 1: A world of awareness at IASE

Federal Information Systems Security Awareness – This topical and relevant training starts off by clearly stating that "Social Networking is Everywhere" and goes on to explain just why it is such a bad idea to share the most intimate details of one's life on what is essentially an open site. (Conside that attackers can now seek to access desirable targets like defense workers by searching for and "friend"-ing family members.) The training format is user-friendly and aids in the memory process by making the presentation interactive. Test takers must demonstrate that they know and understand the security and ethical consequences of their actions.

Personal Electronic Devices and Removable Storage Media –DoD has taken active steps to ensure that unsanitized removable media do not cause the types of problems seen in 2008. In reality USBs were not the only problem, cellphones, PDAs, even a GPS in a rental car…these can all be attack vectors. Most users are not aware that the same data protection which applies to a Government-issued laptop applies equally to a personal Android phone if that phone contains forwarded mail from the user's ".mil" address.

Many more security awareness and ethical decision-making programs exist on this Web site and readers are encouraged to discover the powerful and effective programs available.

3.1 Operational Support

DoD agencies and contractors must prove that all persons accessing information technology systems have taken at least the minimally required subset of security awareness and ethical decision-making training briefings from the IASE Web site. Moreover, DoD Directive 8570.01 (Information Assurance Workforce Improvement Program) provides additional guidance on requirements for personnel involved in planning, implementing, and supporting information technology programs from a technical or managerial level. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50 (Information Technology Security Awareness, Training, Education and Certification) provides an excellent model on how security awareness should be designed, implemented, and maintained as shown below:

Figure 2: NIST Security Awareness Training Model

The NIST document separates the concepts of *awareness* ("allow individuals to recognize IT security concerns and respond accordingly") from *training* ("seeks to teach skills, which allow a person to perform a specific function").[2] From the DoD's viewpoint, SAT encompasses both aspects and all users must demonstrate they can apply the security principles that are being shown, and all technology support personnel must provide certifiable proof that they understand and can actively apply security principles.

Leaving the semantics aside, Operations remains the key component to a successful security awareness and ethical decision-making training program. Consider the high-level SAT lifecycle below:

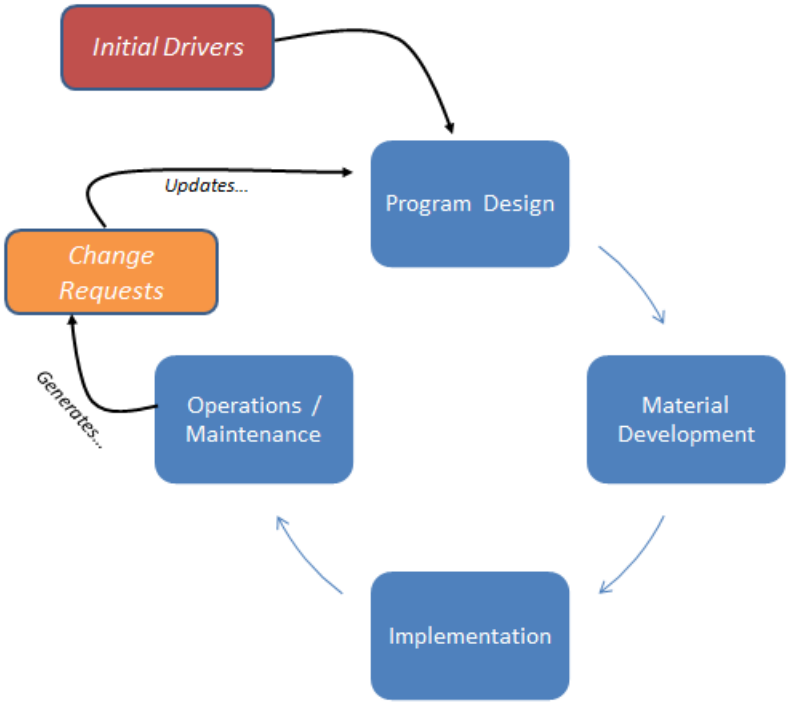

Figure 3: SAT Lifecycle

We generally think of operational support as "running the computers," but for SAT we see that Operation's role entails much more. Ensuring that end-users can take the courses, that line managers can provide reports proving compliance, and that program designers reliably update SAT programs to reflect new regulations and Federal guidance all require significant operational support from the organization.

An example use case might help to clarify the concept:[*] Typically, end-users take required training both at onboarding and then annually. After completing a training course the end-user should receive a completion certificate at a provided email address. The end-user retains the certificate for her records and forwards a copy to her assigned Security Officer (SO). The SO verifies that training is complete based on the end-user's job functions and ensures that all required organizational support databases are updated. Rollup reports get generated showing the overall compliance at each organizational level (division, department, agency, and so on) and these compliance reports get submitted as necessary to Governmental agencies.

Simply put, without a strong Operations department, SAT programs cannot succeed.

[*] Interview with Security Officer at customer site, December 13, 2010.

3.2 Ethical Standards

Ethical decision-making (EDM) lies at the heart of protecting our national security within DoD. Consider the persons who provided classified information to Wikileaks; would they have taken their actions if they believed that they were acting unethically? We posit that this would not have been the case; the people involved truly believed that their decisions, while *illegal*, were not *unethical*. History abounds with examples of this type of decision-making as the Underground Railroad from the 1850s in our own country demonstrates. So the key question becomes: How can DoD (and business in general) ensure that personnel internalize defined ethical standards of conduct? How can we prevent the next Wikileaks scandal before it begins?

One critical component of an individual's EDM involves his view of "the moral content of the organizational culture" as Dr. Linda Trevino wrote back in 1986.[3] The DoD recognizes the value of this approach and has taken definite steps to address this problem. While the Wikileaks data releases have led to a number of technical and administrative mitigation strategies (two-man control, separation of duties, disabling write capabilities to removable media on classified computers), a determined intruder can still bypass these controls. As the old saying goes, "An ounce of prevention…" holds true here: convincing an individual that actions such as sending unauthorized documents to Wikileaks violates his own internal code of conduct is the best way to prevent the action from occurring.

The DoD has no shortage of guidance and directives on EDM. This paper looked at DoD Directive 5500.7r (Joint Ethics Regulation) which serves as the "single source of guidance" for all standards of ethical conduct. This document goes into great detail on the different roles and ethical responsibilities that individuals have within DoD (for example, large prime contractors as opposed to temporary Government interns), and requires that all defense agencies "implement and administer a comprehensive ethics program."

As Dr. Trevino pointed out, an individual bases at least part of his ethical decisions on the organizational culture. From a practical standpoint, that translates to *ethics must be driven from the top*. If the top leadership is seen to be unethical, then the rank and file will feel no special duty to enforce ethical standards. Directive 5500.7r addresses this by requiring that each Agency Head take *personal responsibility* for promulgating and enforcing a verifiable code of ethics throughout her department. This top-down approach ensures that personnel know the core values of the institution itself as well as those of the specific missions and initiatives supported by each department.

From a practical viewpoint, the DoD's IASE security awareness training includes a strong component of ethical decision-making, and individual DoD agencies also provide mandatory live ethics training sessions for all personnel. DoD agencies do not hide this information from the general public either; many of the ethics course materials are provided free-of-charge and online. As just one example, Fort Sam Houston provides a thorough guide to real-world ethical decision making through their ethics Web site at http://www.samhouston.army.mil/sja/ethics.asp.

3.3 Security Awareness as a Competitive Advantage

Throughout this paper, we have concentrated on DoD, and that includes all contractors. In order for a contractor to win even a small award, that contractor must demonstrate:

- Conformance to the highest level of business conduct;
- Existence of a formal SAT and ethical decision making program;
- Commitment to ensuring that all employees meet or exceed security and ethical requirements for their job function; and,
- Willingness to submit to periodic audits that verify its commitment.

Without this fundamental commitment to security awareness and ethical decision-making, the contractor has little chance of being successful in the DoD environment.

4.0 Recommendations

This paper Has examined how security awareness training (SAT) and ethical decision-making (EDM) apply to DoD and the defense community. SAT and EDM have special relevance today with the Wikileaks scandals as individual persons made the conscious decision to disclose information, and the existing security infrastructure did not detect this behavior. That translates to a failure of both EDM *and* SAT.

Specific recommendations include:

Leadership drives SAT and EDM from the top. Employees know whether ethics and security awareness truly matter to the company. Having senior leadership issue memos, speak at training sessions, and provide funding for ethics- and security-related collateral (think posters) sends a clear message that these things matter.

If it isn't auditable, it isn't real. Reliable written records are essential for a successful SAT / EDM program. Not only does this satisfy Governmental regulations, it also shows the company's commitment.

Operations turns SAT and EDM programs into reality. SAT / EDM programs are living processes; they must repeat and they must evolve. To this end, companies must invest in a well-defined change management program in conjunction with the physical and administrative infrastructure to support these programs.

Get the message out. Finally, personnel must take SAT and EDM courses. All too often employees balk at this because "I already know right from wrong" or "I'm too busy for this." The only way to combat this is by having everyone take the tests: from the CEO down to the receptionist.

Our final thought: Security Awareness Training transforms "information security" from a noun into a *verb*!

5.0 Acronyms

CITI	Computer Information Technology Insider
DoD	Department of Defense
IASE	Information Assurance Support Environment
NIST	National Institute of Standard and Technology
SAT	Security Awareness Training
SO	Security Officer
SP	Special Publication

Reference List and End-notes

Bosworth, Seymour, M.E. Kabay, Eric Whyne, eds., *Computer Security Handbook: Volume 1, 4th ed.* Hoboken, NJ: John Wiley & Sons, Inc., 2009.

DoD Directive 5500.7r, "The Joint Ethics Regulation (JER)," July 2, 2010. Available from Standards of Conduct Office: http://www.dod.gov/dodgc/defense_ethics/ (accessed: 9 December, 2010).

DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004.

Trevino, Linda K. "Ethical Decision Making in Organizations: A Person-Situation Interactionist Model." *The Academy of Management Review*, Vol. 11, No. 3. (July, 1986), pp. 601-617.

Wilson, Mark and Joan Hash. "Building an Information Technology Security Awareness and Training Program." *NIST Special Publication 800-50*. Gaithersburg, MD: National Institute of Standards and Technology, October, 2003.

---

[1] Bosworth et. al., CSH, pg. 391.

[2] Wilson and Hash, pg. 20.

[3] Trevino, pg. 602.