Policies, Practices, Standards and Procedures (P^2SP)

Applied for DoD Contractors

Andrew Bruce, CISSP, FITSP, PMP
CTO, RiVidium Corporation (http://www.rividium.com/)
andy.bruce@rividium.com
23 January 2011

Topic Summary:

- Policies and Procedures supporting the Information Security Policy
- Acceptable Use policies and ethical behavior
- Using social psychology to support organizational needs

Table of Contents

Illustration Index

1.0 Introduction

Effective and relevant organizational policies, practices, standards and procedures (P^2SP) provide the direction and guidance necessary for vendors to work successfully with the Department of Defense (DoD). Successful implementation of P^2SP creates a productive work environment in which stakeholders understand their roles and responsibilities, as well as how their individual efforts help to support larger goals and objectives. By using a standards-based set of responses to the common pressures and situations these stakeholders face, P^2SP translates into overall organizational savings: improved productivity, measurable performance benchmarks, and effective overall information security.

Three key elements make an organization's P^2SP successful:

- *Existence* as *formal documents*;
- *Communication* to all stakeholders; and,
- *Internalization* by recipients.

This white paper uses real-world situations to analyze how P^2SP helps to support the organization's Information Security Program (ISP), and how social psychology can be used to help team members internalize their training.

2.0 Background: P^2SP and the Information Security Program

For vendors working with the DoD, security and Information Assurance (IA) concerns must always be paramount. Individual proposals to Government, delivered work products, and employment guidelines must all be governed and judged by DoD security standards. This is true not only in DoD, but in the wider Federal arena; as demonstrated by the Federal Information System Management Act (FISMA, 2002). This Act recognizes the importance of information security to the economic and security interests of the nation and requires agencies and vendors alike to have a verifiable ISP in place. Organizations use P^2SP to demonstrate their due diligence in identifying and planning for risks to information assets in support of the ISP. Additionally, an organization must show that due care has been taken to implement P^2SP: periodic testing of the established information security controls; demonstrable evaluation of the test results; and, that a reliable incident response policy exists to handle the inevitable breaches. Truly, without well-considered P^2SP in place, an organization cannot be said to have an effective IA posture. This translates to a direct effect on the organization's bottom-line by preventing it from effectively competing within the DoD marketplace.

DoD requirements do not exist in a vacuum. A quick examination of some recent headlines shows that McDonald's Corporation suffered an email attack via a third party, as well as warnings that purported computer disk defragmentation utilities downloaded from the Internet can actually be malware. It is only by defining and implementing an effective information security policy that an organization can mitigate the risk from such threats.[*]

[*] Visit *cnet News Security* at http://news.cnet.com/security/ for up-to-the-minute mainstream security breach headlines.

3.0 Applying P²SP within an Organization

How can P²SP be implemented within a DoD-centric environment? To answer, consider the high-level employee lifecycle from "Welcome Aboard!" to termination.

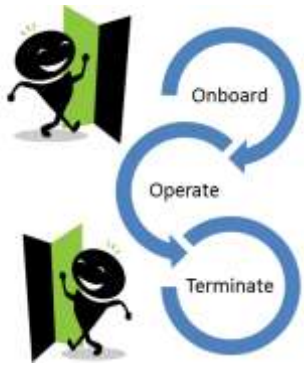

Figure 1: Employment Lifecycle[**]

Specifically, this section explores how organizations should combine formal requirements with best practices throughout the entire employee lifecycle.

3.1 Formality: The New Business Casual

Despite the influence of modern pop culture (for example, piercings and t-shirts as acceptable "hip" business attire), one area remains a strictly white-tie affair[***]: how an organization creates and manages its policies, practices, standards and procedures. As a starting point, consider some paraphrased definitions from the draft version of the *Comprehensive Information Assurance Dictionary*:

Policy – Administrative decisions determining which security-related decisions become formally-implemented requirements.

Practice – Methods and procedures actually *used* within an organization. [****]

Standard – Best-practices from officially-recognized industrial, trade association, or Government bodies. Can also be an established baseline by which procedures and practices can be evaluated.

Procedure – A set of instructions for performing a particular function (such as a data backup) in support of a policy.

Information security policies define an organization's official response to security needs. To be enforceable, they must be both formal (*written*) and demonstrably delivered to all affected information stakeholders (anyone who has access to protected information). If the policies are not formal, not delivered, or simply not easy to acquire, they can become worthless. Additionally, Sorcha Diver pointed out in 2006 that they must be living documents *[26]*. That is, as the organization's business needs and landscape change, the policy documents must change

[**] Drawing by the author.

[***] White tie events are the most formal (*Martha Stewart Weddings*, http://tinyurl.com/white-tie).

[****] Source: BusinessDictionary.com (http://www.businessdictionary.com/definition/practice.html).

accordingly. Finally, policies must be mapped not only to business needs but to an appropriate set of supporting recognized standards. For example, if DoD vendors create and implement arbitrary policies that do not map to a relevant DoD regulation, then these policies become more of a hindrance than a help.

3.2 Onboarding: Employment Policies

Bringing new employees into an organization is an inherently risky process that, as Edward Freeman put it, highlights "the unquestioned need for absolute confidentiality, security, and personal ethics" from these new employees *[Tipton and Krause, 584]*. When a position must be filled, it is imperative to discover if candidates are either untrustworthy or come with "baggage" from a previous job (like binding trade secret or non-compete agreements). Employment policies provide the key to help an organization mitigate such risks, as illustrated here by four practices:

Reference Authorization: Allows an organization to contact previous employers for reference information, including any binding prior employment agreements (such as trade secret restrictions). Of course, that begs the question of *liability* for the previous employer; for that reason, most companies provide nothing more than bare verification of employment. This leads to the second tool…

Hold-Harmless Agreement: Signed by the candidate, this document explicitly releases both the previous employer and the new employer from legal liability. Even with this guarantee, most companies will still not release potentially negative information about an ex-employee, so an effective approach should include...

Multiple Interviews: For sensitive positions, at least one interview should be conducted by a certified, organization-provided security expert. This interview seeks to evaluate the candidate by asking IA-related questions such as the candidate's thoughts on the latest file-sharing software or semi-legal topics like suspect search-engine optimization techniques. By interspersing these questions with innocuous queries and casual conversation, it may be possible to get a candidate's unguarded views. Of course, no interview cycle would be complete without…

Full Reference Checks: By far the most important policy is simply to investigate all references. And for DoD work, vendors must perform this investigation if they wish to get a security clearance for the candidate in question.

Finally, new employees should sign an Acceptable Use policy and other documents related to protecting the organization's trade secrets and patents as their job functions may require (for example: Non-Disclosure Agreements (NDAs)).

3.3 Operations: Implementing Acceptable Use

Once a new employee is onboard, he must follow corporate standards and use information technology resources correctly. This requires that the employee receives information management and general security awareness training, and also to follow the set of pertinent Acceptable Usage Policies (AUPs). AUPs cover all manner of activities: from acceptable ways to surf the Internet (no WikiLeaks or FaceBook); to how internal computer systems can be accessed; and, to proper use of corporate travel resources. DoD vendors are subject to numerous DoD regulations in this area, and one finds DoD Directive 8570 (*Information Assurance Workforce Improvement*) to be highly relevant due to its classifications of and requirements for information technology end-users, technicians, administrators, and managers. Organizational AUPs must abide within these requirements.

The Operations department plays a vital role in supporting AUPs and other elements of the organizational

security policy. As an example, the author's own organization uses DoD standard 5200.1-R (*Information Security Program*) to drive corporate policy and practices. This standard is somewhat older (1997, with minor wording updates) but contains a wealth of good techniques that DoD vendors must apply. These operational elements include:

- Ensure that information is properly classified by system owners.
- Apply proper access controls to information and system access.
- Inform end-users of their rights and responsibilities on secure systems.
- Provide demonstrable awareness and training programs to end-users.

Social psychology tools also help organizations to communicate policies and standards to end-users. For example, employees are supposed to challenge anyone they do not know within their department's designated work areas. However, some employees may feel awkward about challenging someone directly (especially if that person has a badge). Effective policies can address this problem, as the following real-world example shows: "If you feel uncomfortable about a coworker's presence within your area and do not want to challenge them personally, proceed to one of the marked red hallways telephones and contact Security immediately."[*] This allows a shy person to respond to a possible violation without forcing him to act against his *schema*, which is "the complex picture of reality upon which we base our judgments" *[Bosworth et. al., 50-3 (1305)]*.

Finally, information security controls exist to enable business productivity. To use the author's own organization as a specific example, an open-door policy regarding security policy has been found to be quite effective, as is welcoming (and rewarding) comments and suggestions from the workforce in identifying areas of improvement. This policy led directly to a recent change in the corporate security policy: in response to employee request, mobile devices are now allowed to connect to the corporate email. Technical employees were involved in the policy development such that end-users must demonstrate that appropriate password, lockout, and auto-erase controls have been applied to the mobile device in question.[*] When an organization demonstrates that it values its people's needs, and that good and ethical practices on the employee's side can be rewarded, it reinforces the positive aspects of working within the policy boundaries.

3.4 Termination: Making a Clean Break

Termination provides an excellent opportunity to ensure that workers recognize their ex-employment responsibilities. Consider the following practices:

1. **Lessons Learned.** From an IA view, it is imperative to observe how a person left. Was that person bitter or full of anger at perceived mistreatment? As malicious insiders constitute the greatest threat to any organization, organizations are wise to listen carefully during exit interviews in order to understand the work environment that remaining employees face.
2. **Exit Procedures** – An organization should use an integrated management system where terminated employees are entered into an automated "exit workflow" ahead of time. This allows emails to be sent to all responsible IT administrators, and for access accounts to be centrally disabled as of an effective

[*] Interview with project manager at customer site, January 7, 2011.

[*] "Run iPhone in James Bond mode," *osXDaily.com*, August 12, 2010 (accessed: January 15, 2010).

date (*not* deleted, as it is possible that the account may need to be reactivated in the future). During the exit interview, all company property should be collected (such as access cards or equipment).

3. **Looking to the future** – Ex-employees should clearly understand their need to protect the organization's trade secrets as they pursue their future endeavors. Also, the organization should clearly define its post-employment recommendation policies. Finally, employees must realize that any NDAs signed as part of the hiring process remain in effect after termination. This helps to prevent any possible gray areas from putting a cloud over the ex-employee's relationship with the organization.

7.0 Summary and Recommendations

This paper examined ways that security policies, practices, standards and procedures help to support an organization's overall security posture. Specific recommendations for the reader to ponder include:

Enable an automated policy impact analysis. Finalized formal project documents always include references to authoritative DoD and Government policies, and it can be extremely difficult to determine the effect of a change in one of these authoritative policies to executing projects. By first creating a centralized policy database containing all of the authoritative policies and standards, one can use "bookmarks" within project documents to indicate these relationships. When a specific policy changes, the organization can then run an automated job to search for project dependencies so that policy analysts get a better feel for the overall impact of a policy change and the set of affected stakeholders.

Improve policy change communication. Employees can easily view a policy change as yet-another-burden imposed from above with no practical value. To mitigate this, policy analysts and security administrators need to take a lesson from Professor Mich Kabay and do "more listening and […] less commanding" *[Bosworth et. al., 50-6 (1328)]*. Rather than sending out generic email notifications about policy changes, send out a Request for Comment (RFC) to the company to try and discover how a proposed policy change may affect day-to-day operations and to ask for user input on how best to implement the change.

Make following policy…fun! Human beings love the element of play, and any effective security policy practice needs to recognize and leverage that fact. Sponsoring "security days" where employees can compete to answer questions drawn from the security policy or company procedures for small prizes (think: keychains, fuzzy dice, baseball caps, or anything that can be emblazoned with a security message). This not only helps to socialize the security policies and procedures, it gives the employees bragging rights on their security prowess.

In the end, organizations must recognize that their *people* make the organization successful; policies and procedures provide the guidance as well as the specific tools and techniques that allow these people to work safely and effectively to accomplish the organizational mission.

8.0 Acronyms

AUP	Acceptable Use Policy
DoD	Department of Defense
FISMA	Federal Information Systems Management Act of 2002
IA	Information Assurance
ISP	Information Security Program
NDA	Non-Disclosure Agreement
P^2SP	Policies, Practices, Standards and Procedures
RFC	Request for Comment

Reference List

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

Diver, Sorcha. "Information Security Policy - A Development Guide for Large and Small Companies." *SANS Institute InfoSec Reading Room*, 2007.

DoD 5200.1-R. *Information Security Program*. January, 1997.

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

Tipton, Harold F. and Micki Krause, eds. *Information Security Management Handbook on CD-ROM, 2006 Edition*. CRC Press LLC, 2006.