The Security Plan:
Effectively Teaching How To Write One

Paul C. Clark

Naval Postgraduate School
833 Dyer Rd., Code CS/Cp
Monterey, CA 93943-5118
E-mail: pcclark@nps.edu

Abstract

The United States government requires all federal systems to have a customized security plan. In addition, the National Training Standard for Information Systems Security (INFOSEC) Professionals *requires programs that meet this standard to produce students capable of developing a security plan. The Naval Postgraduate School (NPS) teaches courses that comply with several CNSS standards, and therefore requires students to develop a security plan for a hypothetical scenario. Experience in these courses has shown that the same strategies for teaching high school students how to write a research report can successfully be used to teach university students how to write a security plan that is compliant with NIST guidelines.*

KEYWORDS: Education, Information assurance, Computer security, Security Plan

Introduction

> "The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements." [1]

In order to "ensure security in Information Systems", the Office of Management and Budget (OMB) has declared that all United States (U.S.) federal agencies must "incorporate a security plan…that is consistent with NIST guidance on security planning". [2] To further emphasize its importance, the Computer Security Act of 1987 makes it a legal requirement for federal systems to have a security plan. [3] It would therefore be desirable for all college graduates with a desire to work in Information Assurance (IA) careers in the U.S. Government to be able to read, understand, and execute the policies and standards of a security plan. In addition, at some point, IA professionals may need to write or modify a security plan, so there is a benefit to teaching students how to formulate a security plan. Of course, this education would also benefit those who intend to work in the private sector, where security plans may not be required, but are considered a good foundation to an effective computer security program.

In addition to the hard requirement to maintain a security plan, the Committee for National Security Systems (CNSS), formerly known as the National Security Telecommunications and Information Security Committee (NSTISSC), has issued educational standards for Information-Assurance-related positions, many of which require some level of ability

with respect to security plans. For example, Issuance No. 4011, *National Training Standard for Information Systems Security (INFOSEC) Professionals*, expects graduates of compliant courses to be able to "build" a security plan. [4]

The Naval Postgraduate School (NPS) Center for Information Systems Security Studies and Research (CISR) supports the teaching of many courses in the Computer Science department that are dedicated to Information Assurance education. [5] One of these courses, *Secure Management of Systems*, is the capstone of a series of courses that meet the educational requirements of three CNSS training standards, including No. 4011. Therefore, one of the projects in this course is the development of a security plan.

This paper describes our experience and lessons learned from requiring students to write a security plan as part of *Secure Management of Systems*.

Educational Expectations and Roadmap

A project as big as a security plan should be started early in the term, which at NPS is a 12-week quarter. Starting such a project in the first or second week of class would not be possible if the students did not already have some IA education or background. For *Secure Management of Systems*, the following courses are prerequisites:

- Computer Architecture
- Computer Communications and Networks
- Introduction to Information Assurance

The purpose, scope, and content of a security plan are covered in the first week of lecture. Several outlines for a security plan are shown from the following sources:

- OMB Circular A-130 [2]
- NIST Special Publication 800-18 [1]
- Director of Central Intelligence Directive (DCID) 6/3 [6]

This provides a framework for the remainder of the course. Lectures cover material not addressed in prerequisite courses, filling in the gaps not covered, such as contingency planning and physical security.

The Scenario

Secure Management of Systems has been taught for many years, but the security plan assignment has been in place since the Spring quarter of 2003. Over 200 students have completed the course since then, providing a wealth of experience, for both the students and their instructor.

In order to write a security plan, one needs a site to study. This can be done at an operational facility close to the school, but this is difficult to manage when many students are enrolled in the course, and can be time-intensive for the employees of the site. There is also the site's concern about the compromise of real data, and the impact on its reputation if the site does not have very good security to begin with. Therefore, it is often easier to develop a hypothetical written scenario, or an anonymized written description of a real site. The current method of choice for the instructors at NPS is to use a hypothetical scenario. The students prefer the live site.

Developing a hypothetical scenario is no small feat. It requires a written description that has sufficient detail to allow the students to analyze the security of the site without constantly sending the instructor questions via email, or taking up too much time in class. The scenario minimally requires the following details:

- Agency name.

- Agency mission.
- High-level network diagram.
- A description of hardware and software assets.
- A description of the physical and logical security currently in place.
- Floor diagram(s).
- Organization chart(s).
- Some recent bad experiences.

The description that was used most recently at NPS was nearly 1,400 words long. It produced a manageable number of student questions during the quarter. It was written from the point of view that the student has been hired as a contractor to write the required security plan. For "debugging" purposes, it was helpful for the instructor to actually sketch out a security plan for the draft scenario to see where the holes were in the description that might prevent the student from completing each part of the plan.

An unintended benefit of the scenario is the ability to reference the hypothetical site while discussing security topics throughout the quarter.

Template

The first time the security plan was assigned, no particular outline for the completed project was made mandatory. That was a mistake. First, some students could not handle that much leeway and required more guidance to get started. Second, it made grading much more difficult and time consuming because each plan was unique. For example, it was much harder to determine if all aspects of the security plan were covered adequately.

The second time the security plan was assigned, a template was provided to the students. It contained a mandatory outline, constructed by the instructor, to be followed by all students. This resulted in a big improvement, but there were still too many questions from the students about details of the security plan's structure.

For the fourth iteration of the assignment, the outline from the NIST Guide [1] was used as the mandatory format. This not only provided the students with a standard format that they may encounter in their careers, but it came with a "textbook" on what needed to go in each section. It still required some interpretation from time to time, but it allowed the students to work independently from the instructor, which reduced stress for both sides. However, to make sure that there was a consistent look and feel across all submissions, a template of the NIST outline was still provided by the instructor.

Assignments

Another lesson learned through the first two installments of the security plan assignment was that, left on their own, most students waited until the end of the quarter to do any significant work on the quarter-long project, despite constant urgings and warnings. This resulted in lower quality work from the students, and therefore lower grades than they were otherwise capable of earning. In addition, it lessened the learning experience.

Therefore, in the fourth iteration, the project was divided into seven smaller units, with established due dates. This forced the procrastinators to work on the project throughout the quarter, and it gave them feedback as they were going. The drawback to the instructor was an increase in work that had to be graded, recorded and returned. However, this is an approach that is used to teach high school students how to write a research paper: it breaks down the problem until it is manageable, and requires intermediate work along the way.

With respect to grading, the intermediate assignments were not assigned large point values, nor were they heavily scrutinized. They were treated as low value homework assignments because, otherwise, the security plans would have been graded twice: once for each intermediate deliverable, and once for the final complete version. With a smaller number of students it might have been possible to assign grades to the intermediate work that were more indicative of the quality of work.

With respect to the NIST Guide and the standard security plan outline, the following is a short description of the seven intermediate assignments:

1. Read the scenario description, look over the template, and read the Executive summary and Section 1 of the NIST Guide.

   The students were then required to turn in answers to several questions relative to the above reading.

2. Read Section 2 of the NIST Guide. Determine whether the system described in the scenario is a Major Application or a General Support System.

   How this question is answered determines which NIST outline is used.

3. Read Section 3 of the NIST Guide. Complete section 1 (System Identification) of the security plan.

4. Read Section 4 of the NIST Guide. While referring to appendix C of the Guide, complete the following sections of the security plan: 2.2, Review of Security Controls; 2.3, Rules of Behavior; and 2.5, Authorize Processing.

5. Read Sections 5 and 6 of the NIST Guide. For only those controls currently in place, complete the following sections of the security plan: Section 3, Operational Controls; 4.1, Identification and Authentication; and 4.2, Logical Access Controls.

6. Complete the following sections of the security plan: Section 2.1, Risk Assessment and Management; and 2.4, Planning for Security in the Life Cycle.

7. Complete any subsections that were not already assigned, and add in all other controls necessary for secure operation of the site.

The 7th assignment produces a completed security plan. For the students to be able to identify the controls that need to be added to the system in assignment 7, they need to be taught some kind of risk management methodology. The methodology used by the student to decide what controls to add, and what to leave out, is described in section 2.1 (assignment 6) of the security plan. One approach to use is a checklist-based method, such as that provided by the combination of Department of Defense Directive 8500.1 [7] and Department of Defense Instruction 8500.2 [8]. This is an easy approach for the students, but it does not require any real analysis or critical thinking on their part. The security plan may end up with all the controls the site might need, but it may not address current bad practices that need to be eliminated.

The descriptions of the seven student assignments required some occasional interpretation of the NIST Guide, and other hints or requirements to help them succeed.

Summary

The security plan has become a required and important part of the U.S. federal government toolset for improving security. Prospective IA professionals can be given a good education about how to write a security plan if they have the appropriate educational background. In addition, the learning experience can be improved with a little careful planning about how the security plan assignment is handled. NPS has had positive experiences, and the students have produced professional-quality security plans. By following the NIST Guide, the workload on the instructor is reduced, and the student is given additional tools for success.

References

1. Swanson, M., Guide for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18, December 1998.
2. Circular No. A-130, Revised, Office of Management and Budget, November 28, 2000.
3. 100th Congress, Computer Security Act, Public Law 100-235, 1987.
4. National Training Standard for Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011, National Security Telecommunications and Information Security Committee, June 20, 1994.
5. Irvine, C., Warren, D., Clark, P., "The NPS CISR Graduate Program in INFOSEC: Six Years of Experience", *National Information Systems Security Conference, NIST / NCSC*, Volume 1, pp. 22-29, October 1997.
6. Protecting Sensitive Compartmented Information (SC) within Information Systems, Director of Central Intelligence Directive (DCID) 6/3.
7. Information Assurance (IA), Department of Defense Directive Number 8500.1, October 24, 2002.
8. Information Assurance (IA) Implementation, Department of Defense Instruction Number 8500.2, February 6, 2003.