Global Information Assurance Certification Paper

What do I Put in a Security Policy?

William Farnsworth

August 10, 2000

O.K. I just finished a great security conference and I am headed home motivated to make some changes in my organization. The boss (one of those "decision makers") is skeptical. He barely signed my travel request and he is "pretty sure" that our network is fine.

After all, we have a firewall and our virus scanners are up to date. Even with a couple of mis-steps we were only down for a little over a day with a fairly significant infection from the I LOVE YOU virus. And we have no evidence of anybody hacking through our perimeter. So… why do we need a security policy?

I explain in great detail the difference between a virus and an aggressive attack from outside, but it seems to do no good…

And then salvation… we get an email from one of our salesmen in the field with a copy of a disaster plan *requirement* from one of our biggest customers! The pretty brochure indicates that since we are one of their primary suppliers, they want to understand our security practices as part of a continuation of delivery program they are pursuing. They want to make sure that all their key suppliers have a disaster plan and security plan to keep delivering product under adverse conditions. Boss says, "Well O.K. we need a security plan, is it done yet?"

Salvation? I am not so sure anymore. *Now I actually get to write one*. But… what does it look like? Sure I know our systems, I know how we connect to the Internet, I understand the email systems, I understand how our internal systems are connected and how fragile they are… but what goes into a security plan?

I bring up my word processor and I write "MyCompany Information Security Plan." Cool, now we are getting somewhere… but... where… What's next?

Back to the drawing board, and to the Internet for some information.

There are lots of samples of security policies on the web. Every college of any size has a published security manual, or parts of it, on their web site (1-8). Well I don't know… University computer security policies? How well will they relate to my business? Think about it a little.. An environment where you have users on your network that may have little or no loyalty to your organization (how long will they be part of the organization? Weeks? Months? A few years?)… Users that may have little fear of retribution (after all what can you do to a college freshman?)… Users that are striving to attaint the peak of peer recognition… users that are (at least) self-styled techno-dweebs… sounds like a pretty rough security environment. Perhaps we *could* learn a little bit from them.

But… it seems like a formidable task to review each of these and develop a plan for MyCompany. I wonder if there is a template file or we could develop one from some site.

Sure enough, the National Institute of Standards and Technology (NIST) has a couple of articles on how to build a security policy. Cool. The boss will understand that.

"*Guide for Developing Security Plans for Information Technology Systems*" (9) is almost exactly what we want. Well almost, it was developed in 1988 so the majority of the security emphasis is directed toward large systems and physical security, including emphasis on floppy distribution of viruses. There are only two mentions of firewalls in the document and then more in passing than anything else. It is a very informative document, but in many ways it misses the mark for a company whose greatest vulnerability is email viruses. And email is not mentioned once in the document.

So… here we are almost back at square one. Ms Swanson authored another document two years earlier with Barbara Guttman; "*Generally Acceptable Principles and Practices for Securing Information Technology Systems*." This document has perhaps a better overview of the process but still lacks specific relevance in today's world.

Off to the web again… and we find our favorite source of technical documentation, the RFC's. Sure enough, the original RFC1244 "*Site Security Handbook*" (11) and it's replacement RFC2196 "*Site Security Handbook*" provide more great information and we start to see an outline forming.

The final outline is attached at the bottom of this discussion, but our overall approach deserves some attention.

It was clear that each of the organizational units of our company and even our central Information Technology division needed specific policy and procedure flexibility. The central organization (CIS) provides telephone, network, web server and some financial services. Each business unit, organized by vertical market segment may have slightly different security requirements. The outline allows for a definition of this flexibility in the General Information section, and each of the operational units in the CIS organization has a section of the policy and procedure manual outline below.

Business units and the international organizations are free to write additional policies for IT areas for which they have responsibility, but the corporate document will cover sections that they do not touch.

There are a few common sections that are used by each department, but each department is not an exact match to all the other departments.

Authentication of the user is critical for most of the departments. User password requirements are especially important for the domain administration section, and for the legacy systems. We continue to support legacy systems on VAX hardware and some of our new ERP systems require separate login administration.

Intrusion protection is required in all sections. Monitoring attempted (and real) access is of importance to make sure that confidential information is not compromised, and the systems are protected from malicious attacks.

Physical access to the data center, the Network Operations Center, cable closets on the campus and the telephone switch rooms is specified in this section. Who has access and who needs to be escorted during visits are all specified here…

Almost all of our equipment has backup requirements. The data center with its financial systems is our primary concern, but we shouldn't forget the network routers, switches, and even the phone switches have magnetic media that needs backup policies. Firewalls, intrusion detection systems, content filters all require consistent backup policy. Offsite storage is also a consideration. We live in a tornado area and offsite backup is very definitely part of our daily procedures.

Disaster planning is part of each of these areas as well. Taking the time up front saves time and money when the tornado wipes out the data center, or the NOC, or any of the buildings on campus.

Auditing of all our systems is necessary to provide evidence and clues to diagnose and document problems after an incident. In addition clear usage policy is included to protect the authorized network operations folks when it is necessary to scan various machines and ports on the network. At the same time the sections on intrusion protection and acceptable use policy include restrictions on who can monitor and probe the network.

Some of the special topics that need to be covered in any comprehensive security policy are policies for modems, dial-in, dial-out, employee departure procedures and a section on incident handling.

Incident handling is described in significant detail with roles and responsibilities, and a step-by-step procedure from identifying the incident to the final forensics.

I encourage you to look at other practices and procedures for guidance for your own policy documentation and adapt them to fit your implementation requirements.

Bibliography

(1) Various. "*Texas A&M Computer Security Policy*." Texas A&M Computing and Information Services. November 1999. http://www.tamu.edu/cis/qapcm/SecurityPolicy.html. (August 10, 2000)

(2) Various. "*ITS Lab Support Policies & Guidelines.*" Information Technology Services, University of Colorado at Boulder. January 1998. http://itsweb.colorado.edu/docs/policy.procedure.html. (August 10, 2000).

(3) Fritchley, David. "*Computer and Network Use Policies.*" Policy and Procedure @ Ohio University. February 1997. http://www.ohiou.edu/policy/91-003.html. (August 10, 2000).

(4) Various. "*Policies and Responsibilities for Use of Campus Computer and Network Resources.*" Academic Computing and Network Services, Florida State University. February 2000. http://www.acns.fsu.edu/docs/policy.html. (August 10, 2000).

(5) Various. "*Information Technology Security Policy*." Office of Information Technology Services, Murdoch University, Perth, Western Australia, 1997, http://wwwits2.murdoch.edu.au/security/policy.html. (August 10, 2000).

(6) Various. "*Proposed Network Security Policy*." Computer Security Administration, University of Toronto. July 31, 2000. http://www.utoronto.ca/security/policy/. (August 10, 2000).

(7) Various. "*Information Technology Computer and Network Security*." University of California, Davis. May 14, 2000. http://security.ucdavis.edu/text/index.html. (August 10, 2000).

(8)Masse, M. "*Information Security Policy for Administrative Information*." Administrative Information Technology Services, University of Illinois. April 1999. http://www.aits.uillinois.edu/security/securestandards.html. (August 10, 2000).

(9) Swanson, Marianne. "*Guide for Developing Security Plans for Information Technology Systems*." NIST Special Publication 800-18. December 1988. http://csrc.nist.gov/nistpubs/Planguide.PDF. (August 9, 2000).

(10) Swanson, Marianne and Guttman, Barbara. "*Generally Acceptable Principles and Practices for Securing Information Technology Systems*." NIST Special Publication 800-14, September 1996. http://csrc.nist.gov/nistpubs/800-14.pdf (August 9, 2000).

(11) Holbrook, P. and Reynolds, J. editors. "*RFC1244 Site Security Handbook*." July 1991. http://www.faqs.org/rfcs/rfc1244.html. (August 9, 2000).

(12) Fraser, B. editor. "*RFC2196 Site Security Handbook*." September 1997." http://www.faqs.org/rfcs/rfc2196.html. (August 9, 2000).

Sample Security Policy Outline

1. Introduction
    - *1.1.1. General Information*
    - *1.1.2. Objectives*
    - *1.2. Responsible Organizational Structure*
        - 1.2.1.1.1. Corporate Information Services
        - 1.2.1.1.2. Business Unit Information Services
        - 1.2.1.1.3. International Organizations
        - 1.2.1.1.4. Tenants
    - *1.2.2. Security Standards*
        - 1.2.2.1.1. Confidentiality
        - 1.2.2.1.2. Integrity
        - 1.2.2.1.3. Authorization
        - 1.2.2.1.4. Access
        - 1.2.2.1.5. Appropriate Use
        - 1.2.2.1.6. Employee Privacy
2. Domain Services
    - *2.1.1. Authentication*
    - *2.1.2. Password Standards*
    - *2.1.3. Resident Personnel Departure*
        - 2.1.3.1.1. Friendly Terms
        - 2.1.3.1.2. Unfriendly Terms
3. Email Systems
    - *3.1.1. Authentication*
    - *3.1.2. Intrusion Protection*
    - *3.1.3. Physical Access*
    - *3.1.4. Backups*
    - *3.1.5. Retention Policy*
    - *3.1.6. Auditing*
4. WEB Servers
    - *4.1.1. Internal*