Planning Intranet Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A reader writes, “I am looking for a template for a security Plan for an Intranet that we are developing. Can you point me to a template for a security plan for an internet or intranet?”

***

The most important piece of advice is that templates are a good tool for policies, but nothing can substitute for a sound analysis of your own situation. No one published plan can suit all possible network designs, applications, and threats. As always, you have to

* Gain upper management support for developing security policies and procedures;

* Form an information protection working group with representation from all sectors of the organization, including technical staff, production workers, public relations people, legal staff, facilities security and so on;

* Evaluate your functional requirements;

* Define the value of protecting the different kinds of information your users will work with (valuation will include the costs of unavailability, errors, unauthorized disclosure, forgery, excessive security and so on);

* Evaluate the most important threats in your particular business and technical environment;

* Define an acceptable strategy for safeguarding information resources without crippling productivity, wasting money, or frustrating employees in their work;

* Review and adjust proposed policies so that all sectors of the organization agree to work towards effective implementation;

* Include awareness training and ongoing programs to maintain and publicize changing security policies as needed;

* Assign responsibility for keeping security as a living component of everyday work.

Ho-hum, but you knew that, right? OK, here are some resources for you. In the space available, I am listing just a few good starters, and omission of a resource is in no way to be construed as criticism.

(1) Let’s get the shameless plug out of the way first. Several chapters in the CSH4 provide useful preparatory reading:

35, & 37 come to mind as most relevant <g>.

(2) Take a look at the text below; I haven’t seen it myself, but the blurb includes positive notes from well-respected security experts:


(3) _Intranet Journal_ has an extensive list of articles about intranet security at <http://www.intranetjournal.com/security/>.

(4) The English edition of the German _IT Baseline Protection Manual_ has a number of relevant sections in the Network security chapter (#6) at <http://www.bsi.bund.de/gshb/english/etc/k6.htm> but see the site map at <http://www.bsi.bund.de/gshb/english/etc/navie.htm>.

(5) The CERT/CC "Security Improvement Modules" are available online (and free) in Acrobat PDF and in Postscript formats from <http://www.cert.org/security-improvement/#modules>. This information is also available in the textbook,


(7) The SANS Information Security Reading Room is full of useful materials. Start at the home page <http://www.sans.org/newlook/home.php> and click on the Reading Room icon at the top of the screen. You’ll be asked to register if you haven’t yet done so.

(8) For help in precise wording of policies, I recommend


and also


* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.