In discussions of computer crime, attention inevitably has to turn to what happens when our security perimeters fail. How do we respond to _successful_ attacks on our systems.

I’ve been teaching a Cybercrime course for the last couple of years, and one of the texts I use is by my friend and colleague Peter Stephenson. In this and several future columns, I’ll be basing my writing on key issues raised by Stephenson in his book on _Investigating Computer-Related Crime_.

First of all (Stephenson writes), one must define the goals of what he calls “intrusion management.” These are to prevent intrusion in the first place; to recognize an intrusion as quickly as possible; to delay damage as long as possible; to respond to the intrusion so as to prevent, reduce and repair damage; and to collect evidence for decisions on whether and how to engage in legal proceedings under civil or criminal law.

Intrusion avoidance starts with policies, standards and procedures. Policies are global statements about the desired level of security such as “Prevent unauthorized access to our mainframe computers.” Standards are recognized methods for achieving appropriate security; e.g., “Use RACF on IBM mainframes.” Procedures are specific steps to take in implementing standards; e.g., “Set the access-control list by default to account-only for all new accounts.”

Testing is an essential component of preparing for the failure of security barriers. Because good security methods reduce the frequency of security incidents, there is a paradoxical reduction in the feedback that would encourage good security. In the absence of any obvious problems, employees and managers tend to become lax in their commitment to security. Testing has many benefits:

* It keeps interest in security high;
* Tests can become a contest or a game, generating positive feelings about what can otherwise become viewed as onerous and dull;
* Frequent testing serves as a kind of drill, increasing the likelihood of good responses in a real attack;
* If properly analyzed, test results can point to weak areas that would benefit from rethinking and better training;
* Tests can provide a measurable proof of effectiveness.

***

In the next article, I’ll continue with more on testing security.

***

For further reading:
NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


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@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

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.