Creating a Security Plan...Getting Started

By Jean Driscoll, Holiday Retirement Corporation

Editor's Note: Jean is our Associate Editor for CNC, but this month she tackles a less technical subject: Security. Jean may be reached at Jean.Driscoll@hrc-cc.com. If you have suggestions for future technical articles, please let her know.

As IT professionals, we have all seen destruction caused by the wayward virus (or badly written program), and most of us have restored data that had been inadvertently destroyed by an inconspicuous user, trying a function just because it was there. We all realize that these problems eventually become our problems. How should we go about putting in the security structure to protect ourselves?

This article will cover the steps for creating a security plan. As additional resources, White Papers will be available on the JDETips website to help with the specifics of setting up security on the AS/400 for both WorldSoftware™ and OneWorld®. (The WorldSoftware White Paper will be available November 1, 2002, and the OneWorld White Paper will be available January 1, 2003.

The steps to any plan for security will include:

a) Getting sponsorship from Management

b) Picking your security team

c) Determining security policies that will support your security needs (at a detailed level, this means determining what needs to be secured and from whom)

d) Determining what security measures are needed to support your policies and how to audit the security once it is in place

e) Testing a security setup in a test environment

f) Implementing the security measures

g) Auditing the system once the security measures are in place

Management

It is in the very nature of a security project that a security implementation will affect everyone in the company. A security project will involve time. Testing the implementation of the plan will involve a number of users whose time needs to be allocated. A testing environment needs to be set up. Disk space or other system resources may need to be fortified. Someone needs to set guidelines for system security for your company. For a well-rounded security plan, the network and other database administrators should be involved from the outset. All of these resources, hopefully, can be acquired through your management.

The Security Team

A team should be formed that can communicate well and often. Whom you invite to be on your team will depend on the level of knowledge of your department, your management, and your user group in regards to systems and security.

Depending on the size of your organization, you may want to have separate teams for deciding policy and another team for implementing the security measures and policy.

The company I am working for is small enough just to have one team who does everything. We are a small company that is just migrating out of the mainframe environment of the 80's, and where only application security has ever been implemented (and this by Andersen Consulting). Our security team consists of the IT Director, the Operations Manager, the Network Administrator, and the CNC Administrator. The IT Director states the overall direction for security policy and communicates the need for a security project and policies to the rest of the company so that the policies are supported. Everyone else on the team comes up with the policies and determines how to implement the security to support the policies. With a company that is more technically advanced, or further along in its security implementation, members of the user community would also be asked to serve on a policy determination team. In a larger company, telecommunications specialists, Web-masters, System Performance or Work Management specialists as well as security administrators would be part of the team.

Security Policies

At Focus 2002, Erik Hjelmstad from PoliVec outlined many different types of policies that should be

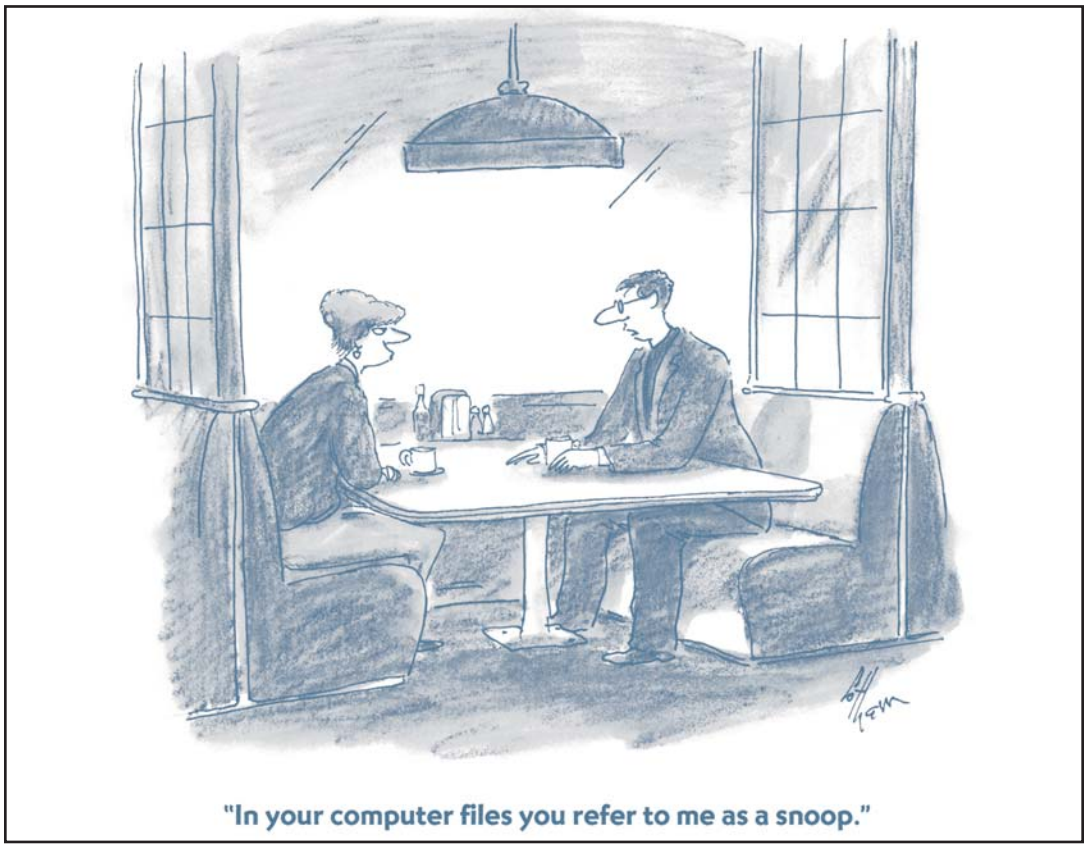
setup, documented, and implemented. Erik defines a Security Policy as "A set of documents that describes, at a high level, the security controls that will be implemented in the company," "A set of rules that states what actions are permitted and which actions are prohibited," and "may include procedures that will be performed and how often certain items should be done."

He cites many policies covering the areas of Business Continuity Planning, Physical and Environmental Access, Personnel Security, System Development and Maintenance, Industry Compliance, Asset Control, and the Security Policy itself. He mentions different types of businesses that may already have standards that a security policy should follow, like the Government Information Security Reform Act and the British ISO10799.

I learned from this topic that there is a lot to learn about policies. The Security Policy is the "foundation of your security infrastructure – which can help to guard your company against potential lawsuits," it gives you a starting point for a security plan, it helps employees start understanding why security is necessary, and some industries are required by law to have one in place. Here's a Web address that will show you different policies on which to base your policy: ***www.sans.org/newlook/resources/policies/policies.htm***

For this article we will discuss more of an overall policy that can help guide our efforts in determining the security measures or implementation standard for a company. As I mentioned before, the company with which I work is just learning about computer systems and security, so the pervading thought here is that the security policy will be implemented in stages. The first stage is just putting guidelines and implementation standards together that will stop the user community from being able to hurt itself. Hopefully we can accomplish this with minimal input and effect on the user. The next stages of security implementation will take into account external hazards to the company and disaster recovery.

For this first stage, I foresee the creation of password, acceptable use, and anti-virus policies, and then the implementation of measures that will stop the user from being able to delete or modify data via programs unrelated to the data's specific application, stop the users from having command line access from any applications including FTP, and secure any sen-



"In your computer files you refer to me as a snoop."