

# THE AUDITOR'S REPORT

## NEWSLETTER

*A Publication of Nearman & Associates, CPAs, P.A.*

### **Monitoring and Testing for Intruders**

Is your credit union at risk?

A majority of companies believe their computer networks are safe. This could be true, but what if it's not? The question then becomes what liability do you face if your network is not secure. Perhaps you believe that since your credit union does not perform transactions on the Internet the credit union's systems cannot be at risk. Let me give you a few quick statistics that will discount that theory.

1. The 2001 Computer Crime and Security Survey reveals that security breaches resulted in more than \$377 million in losses to the 186 corporations, government agencies, and other institutions surveyed. That relates to an average loss of over 2 million dollars per company. Are you prepared to deal with that loss?
2. A survey from the research organization, Computer Economics, revealed that in the year 2000 malicious viruses cost businesses and organizations worldwide an astounding \$17.1 billion, up from \$12.1 billion in 1999.
3. International Data Corporation estimates as many as 30% of a company's approved users are no longer employees. Why are they still on the approved list?
4. The FBI estimates the cost of the average insider attack at \$2.7 million. Insiders have the access to violate your computer network even if you aren't connected to the Internet. Can you afford to ignore this risk?

We are not implying that your IT staff is not doing their job. The day-in and day-out administration of a network is very time consuming. Just keeping up on the changes to the operating system, daily maintenance, and user problems is a full time job. Now add on the security side of the job and the task is overwhelming for most IT departments. New viruses are found almost daily. Unknown people are monitoring network traffic over the Internet. There are people who will try to break into your system and some of them may succeed.

Do you believe that security measures are built into the operating system? Most of us believe that these measures are sufficient to keep our networks secure. Let's look at one of these built-in security features: Almost everyone who uses the network logs in using a password. How secure are these passwords? A credit union we recently audited allowed us to evaluate the passwords on their network. We knew 80% of their network passwords in less than one minute. The remaining 20% were known within a few more minutes.

Physical security is another issue. Most companies lock up their servers, but what about the rest of the network? You work with the general public and most of them have some access to your building. Can you safeguard each of your computers from the casual intruder? What about your credit union's cleaning crews? Are they alone in the building at night where they have access to network connections? The risks are everywhere, so what can we do to help you?

Let's begin with a little bit of education. There are two levels of protection. The first is penetration testing. During penetration testing, your network security is analyzed against hundreds of known attacks to determine the network's weaknesses or vulnerabilities. The results are organized based on risk: high, medium, and low. The test results let you know how your network stands on security issues. Penetration testing, however, only evaluates your network at one moment in time. While the testing is valuable in helping to improve your security defenses, if you make changes to your network or add additional services at a later point in time, you will probably need to re-evaluate your network security at that time.

The second level is network monitoring or intrusion detection. All the network traffic into and out of your credit union is monitored on a 24 hour, 7-day per week basis. If unusual activity is occurring on the network, action can be taken immediately to halt the intrusion. Monitoring allows for proactive responses to attacks as they occur. How many credit unions have the resources to do 24 hour per day, 7 days per week monitoring? Can you afford to man your computer network around the clock? Your staff is already busy doing the day-to-day work of keeping your system up and running. Do they also have time to watch the network traffic?

In summary, the risks are everywhere. Attacks can come from inside your credit union or from the outside. Upwards of 80% of attacks come from within an organization and are performed either by employees or people working in or around an organization's computer system. Take a pro-active stance. Don't wait until it happens to you and then try to fix the problem. Prevent an attack on your credit union today; tomorrow may be too late.

*Brian Langan, President/CEO  
Langan Enterprises, Inc.*