Lake County Contractors Association
Professional Practice Report
May, 1996

Computer Security

by Bill Zeigler, V/H Associates

With the advent of a more inclusive community in computing, systems and users are interacting on an unprecedented level. More systems are networked or connected by modem, more users are learning to develop information, more procedures are incorporating a group approach to developing data. Banks are disseminating account activity, goods and services are being transacted with increasing automated procedures. E-mail has become commonplace only in the last few years, growing to 90 million users by the end of 1995, about double the level from just one year earlier. Remote server access is expected to grow 35% per year through at least 1998. The total amount of the world's accumulated and recorded information has doubled in less than five years - in 1950 it took decades.

The mass quantity of events and activities being distilled into some electronic form demands a medium that provides increased access. Certain information coming to the attention of unintended people in or out of the organization can lead to undesirable or unproductive responses. The introduction of some control over data access has thus become more important and simply good business practice, similar to data backup procedures. And similar to data backup, even a small effort toward procedure can go a long way to making security a non issue. The tools to do the job are often available in added features in software programs (network security features, passwords on files), even option settings on hardware (screen blankers, passwords to access disks).

So what does this mean to you? As in most decision paths with innumerable impacts: analysis first, planning next, and then action consistent with a designed purpose increases the chance of intended results with less effort than a "Ready, Fire, Aim (OOPS)" response.

Analysis - This means analyzing the body of information within your organization, how it is developed and by whom, who needs it, who wants it, and consequences to crossing over that access. This includes samples of sensitive information that typically come to mind such as payroll, policy analysis, crisis events and related info. But also consider competitive data that takes time and money to develop such as customer lists or results of new approaches to problems or situations. Hot Spot examples, either sensitive data or thin access points, are:

- Payroll and personnel data
- Customer lists - these can benefit competitors
- Sales and Marketing data - either you bought this info or you paid your own forces or squeezed margins to develop it
- Written / coded procedures - this information often is the product of much effort to identify efficient methods of production, product formulas, equipment cost history - many things that took plenty of your time and expense to develop
- E-mail systems and contents
- Outside access points such as communications or Internet servers
- Internal server locations - data access and possibility for system disruption [e.g., intentional virus]
- System communications tools such as modem pool capabilities

Planning - With a clearer picture of information hot spots in the organization as well as where, how and by whom it is developed, it is easier to formulate where you would like to introduce controls to access. Don't initially consider techniques or procedures for doing so, but focus first on points of concern. This step sets down the action that will be taken, considering available techniques and features, cost of loss vs. cost of protection, etc. All the conclusions drawn here leave execution to the Implementation step.

Consider the practical aspects of required action to plug a potential leak. This can include political or personality aspects of those who might currently have access when you determine they should not. Procedure changes and additions usually have a measurable effect on productivity and possibly moral. While it may be theoretically possible to plug every leak, it may not be feasible or advisable (translation, cost effective) to reach that goal. The cost of compromising the integrity of the data in question can be assessed.

Passwords are a common tool and implemented at many levels and ways. One protection technique is to avoid words found in the dictionary, a source used by decoding programs. Another technique is to require the user to change the password at specified intervals. Another published approached is to focus security at an access point to a network or sensitive point as the most effective - once in the system, no more effort is devoted to limiting access. At this level, times of access may be designed into the system which are

consistent with the user's role and approved activities. Timecards are probably not going to be loaded at 2 AM, but an intruder may attempt access at that time.

Internet servers are usually outfitted with third party protection schemes called ‘firewalls’. Encryption technology for Internet merchants and buyers has received extensive attention in the last few months. In elaborate networks, a server can be installed dedicated to routing users to other servers after following an authentication routine.

Implementation - After Analysis and Planning, it should be easier to execute the decisions made previously. This is the easiest step particularly if it is not attempted first. The steps should be documented and users oriented in advance of the changes. Implement available steps in balance with practical aspects of procedure (ways to introduce security without making a career of the process) and technical feasibility (our members are not in the market for retina scan systems).

Monitoring - This is helpful to continue to refine and diagnose the procedures put in place. Many systems include features that record failed login attempts or require privileged user intervention after a specified pattern of attempts.

Conclusion
In a quickly changing world of computers, systems and information management, technology advances have raised the value of attention to appropriately designed security. As often is the case, common sense and even basic steps can keep the process smooth.

***Professional Practice Repor*t** is a publication of LCCA’s Professional Service Committee. LCCA is not responsible for the content of this article which only expresses the opinions of the author. For more information, contact LCCA at 1312 Washington St., Waukegan, IL 60085 Phone: (847) 623-2345 e-mail: PPR@LCCA-IL.org.