Reasonable Security Safeguards For Small to Medium Organizations

by Dr. H.B. Wolfe

Introduction

In today's world most businesses, large and small, depend on their computer(s) to provide vital functions consistently and without interruption. In many organizations the loss of the computer function could mean the difference between continued operation and shutdown. Reliability and continuity, therefore, become the critical aspect of any computer system(s) currently in use. This paper attempts to describe some of the most important issues any organization should address in order to reduce their risk where it relates to computer related failure.

Computer Security - What is it?

Computer security covers a myriad of areas but basically it entails the protection of the physical plant (hardware, wiring and other related equipment); creation, implementation, update and enforcement of security policies and procedures; software protection where appropriate; and backup. You might ask yourself why I have included backup as a category by itself. The simple fact is that no matter what type of incident might occur, if you have the appropriate backup the likelihood of a successful recovery is dramatically increased. Conversely, without that backup the likelihood of an unsuccessful recovery is also dramatically increased. Therefore, backup and its appropriate storage is vital to the successful continuance of any computerized operation.

Physical Security - What do we protect?

The first thing that anyone asks when we begin to talk about security is how much is it going to cost me. That will vary based on how tightly any organization decides to make their protective measures. The costs can be as little as nothing in the case of a procedural change and big bucks in the case of serious hardware and/or building modifications. The answer is undoubtedly somewhere in between and inevitably whatever the organization can economically justify. What we must address are the risks and their respective likelihood of occurrence and then assign a value to preventative measures.

First of all the hardware must be protected from unauthorized access. Access has two different aspects - physical and procedural (we'll discuss the procedural aspects later in the paper). Physical access refers to being able to get to the machinery to damage, destroy, or to make unauthorized use

of it. To reduce that type of risk equipment needs to be located in a place that is not open to the public or to persons who are not authorized to use it. Larger organizations have guards and barriers. Smaller ones rely on their own people and procedures as a deterrent during working hours.

Hardware must also be protected from being damaged outside the normal hours of work. This can be accomplished by normal physical security that might be used to protect any other capital items - locks, intruder detection, video surveillance, fire and smoke detectors, alarms, etc. *Acts of God and vandals do not occur at convenient times.*

Another aspect of physical security deals with storage of vital records, software and backup copies of data, software and documentation. In the event of a catastrophe, the given hardware configuration can always be rebuilt - insurance will generally cover those costs. The installation of site specific software may be time consuming but for the most part that too can easily be accomplished where standard software was in use. However, where software had been customized or created specifically for the organization affected, it is not easily reconstructed unless proper backup is available. That backup needs to be stored in a secure storage facility preferably two copies in two places. One copy stored on site in a proper data storage cabinet (these often look like safes but have added dust and fire protection that a safe does not). The other copy stored off site at a local bank or other secure site. Where original or customized software exists current copies of the respective documentation also needs to be stored in the same way. All the backup in the world isn't much good if you don't know what to do with it. It goes without saying that **data backup is a must for any organization**.

Many organizations are making use of data communication in one way or another. For those folks it is important to understand the vulnerabilities. Networking and other kinds of data communication usually make use of either public land lines (telephone company cables) and/or their own cabling for those communications. One of the basic things I learned when becoming familiar with administering a network is that if anything goes wrong the first place to look is the cables, the second place is the cables and the third place is the cables. Cabling is probably the most vulnerable part of a network and therefore, we need to take particular care to insure that the cabling is protected from accidental or deliberate damage. This technique costs little to reduce a significant risk.

Another risk in data communications is the possibility of interception. A simple rule of thumb to follow is to consider the value of the information being transmitted over your communication links. If that information/data deals with capital items or their movement (money, property, goods, etc.) or with sensitive information (confidential or proprietary) it would be a good idea to make use of data encryption to protect that communications traffic. That can be accomplished by using either software (which requires processing from the host system) or hardware encryption (which takes

place within its own processor). Incorporating data encryption into your overall communications security strategy can be very cost effective. There are several products created and produced right here in New Zealand that provide a good level of security.

One computer product has a particular risk associated with it that all of the others do not and it's worth singling it out for some discussion here. The increasing popularity of notebook computers adds a downside risk to everyone and every organization that officially makes use of them. The first consideration is the fact that individuals will take confidential and/or proprietary information with them off site stored on their notebook computer. This is a real risk. In America there are documented cases of groups targeting corporate executives and deliberately stealing their notebooks not to sell the machine but to sell the data and information contained thereon. During the Gulf War a British officer who had the plans for the invasion of Iraq on his notebook had it stolen from the locked boot of his limousine. Luckily, in that particular case the thieves were patriotic and returned the machine as soon as they realized what they had taken.

The issue is how to protect sensitive files on such a machine. The computer and software can easily be replaced and that cost absorbed by insurance coverage. But what of the data? The only protective measure that delivers reasonable safety is data encryption. Fujitzu has a product that works on the Windows (3.x and '95) platform called TeamWare CRYPTO. This appears to be a non intrusive application that allows the user to encrypt individual files on their system. It is but one example of such products that are available. We have tested several access control products (programs which either allow or deny access to the use of the computer based on password control) and in every single case we were able to by pass those controls and gain access to the data contained on the system. Some notebooks have such controls built into their systems but these are not reliable and can also be bypassed.

Security Policies and Procedures

Security begins at the top. If top management does not consider computer security to be important, no one else within the organization will think it important. Therefore, a policy needs to be created at the top addressing the importance, safety and continuity of the Information Technology function. This policy should foster and encourage the notion of an accountability culture making everyone within the organization responsible for security issues. As organizations get larger the security function should have a formal structure, authority and responsibility of updating policies and overseeing in general the security activities and measures practiced within the organization.

It makes no sense at all to issue edicts and then not enforce those policies. Enforcement is vitally important to the success of any security policy and strategy designed and put in place to protect an organization. In order for security policies to be enforced someone has to take responsibility for that enforcement. Moreover, everyone needs to know exactly what the penalties are for infringement. I am not a policeman nor am I advocating that type of environment. I am, however, suggesting that all staff receive training in security issues regularly throughout their employment with an organization. Part of that training should include the complete description of the consequences of the various kinds of breaches that could occur and how each employee can participate in protecting their organization and ultimately their job.

It is easy to forget security once you have created a policy and/or put protective measures in place. The fact is that organizations change and the computer configuration (both software and hardware) is constantly changing. Because of these changes, new risks arise. Therefore, computer security policy needs to be reassessed regularly and updated as necessary. Additional training would need to be done as new threats and safety measures are also put into place. This is an ever changing ongoing business.

Software Protection

This type of protection can be further broken down into specific areas. First, where access is controlled by software (password protection) it is important to educate users in the formation of their passwords as well as in their responsibility not to make them available to others deliberately or by other means. Deliberate is fairly obvious but other means can vary. In almost every installation you can find someone's password written down and taped to the bottom of their keyboard or in their desk drawer or in another obvious location. Normally explaining these risks will help to reduce them.

Programs that control the use of passwords can usually determine the size of the minimum length of the password (larger is better - 6 characters minimum) and whether or not it has been used before. Some have the capacity to check a potential password against a master list of common nouns and any password found in that list would be rejected. In educating staff about passwords, for example, it would be worth mentioning that the use of names of familiar people and things that are important in the user's life can usually be easily guessed by an average hacker attempting to gain access to your system.

Over the past several years, with the increasing popularity of PC's, computer viruses have become a significant and real threat to all organizations. A virus is a program that attaches itself to another

program or in special cases (like the Microsoft Word macro viruses) to specific types of document files. When the virus code is executed it takes control of your computer (without your knowledge or approval) and appends a copy of its code to other executables on your computer whenever it can and it watches for whatever trigger conditions its creator designed into it. When those conditions exist it carries out its payload directive. That may be as simple as displaying an innocuous message on your screen or as devastating as reformatting your hard disk. This is a very real risk that is not going to go away for the foreseeable future.

There are more than 7,000 viruses currently identified and described covering several environments including MS/DOS, Windows '95, Windows NT, Macintosh OS, etc. That means that if you use any of these operating systems in any computers that your organization relies on - they are at risk. Viruses travel from machine to machine in several ways. Many of these can be cut off by taking reasonable care and following simple procedures. For example: booting up from a floppy disk should either be prohibited or the capability should be disabled within organizational machines. This simple measure would virtually eliminate the potential of being infected by a boot sector infector (a significant portion of those 7,000 plus viruses).

There are software products that you can purchase that will help to protect your equipment from virus infection. These are referred to as anti-virus products and they come in many flavors. The most common are scanners and there are several that are freely available from the Internet (if you have Internet access). Scanners look for a unique string of characters that most viruses also use (these are used by the virus to distinguish whether a target file has already been infected so that it doesn't repeatedly infect the same file) and if found identify that specific virus. Of course, you must (on a virus free system) scan an application program PRIOR to executing it to find out if it is infected. Virus recovery is another example of where **good backup pays for itself**.

The Internet is a two edge sword. On the one hand, it makes available a significant amount of useful information services (including security alerts and protective software), and the ability of users to cheaply communicate on a worldwide basis. At the same time it opens the door for two other major risks. In the first instance the Internet also contains information and software deliberately designed to do damage to others. You can find instructions for hacking into almost any family of computer and almost any operating system. You can find source code for programs that probe computers attached to the Internet to find and identify their vulnerabilities. You can find source code for building viruses. These examples are but a few that demonstrate that the bad guys are communicating - constantly.

In the second instance the Internet itself is a risk. If your organization's machine(s) are attached to the Internet, they are liable to attack from outside your organization. The current hot topic in computer security circles is firewalls. This term refers to a technique to protect Internet users from outside attack. This technique has been defeated in several different ways. The bottom line here is that most systems connected to the Internet are vulnerable in some way. So far, as new methods are employed to defend against those vulnerabilities, those methods have all proved to be only temporarily effective.

Conclusion

Computer security is a very specialized business. This short paper has highlighted a few of the kinds of risks that computer users face each day and then only superficially. There are a significant number of books written about each of the areas I have addressed. Some of the more esoteric threats, such as TEMPEST and technical surveillance, have not been discussed since those risks may be considered non existent in New Zealand at this time, however, that does not mean that these risks do not exist. Everyone would probably agree that bugging surveillance only really happens in the movies or in places like Washington, or New York, or Paris or Moscow, etc. The simple fact is that it occurs right here in little old New Zealand.

On Good Friday 1995 an associate was installing an alarm system in a local business and in so doing had to get into the space above the ceiling. While he was up there he noticed a device and immediately talked to the owners about it. Apparently it must have been put in place prior to their purchase of the business (just a few weeks earlier) and they just wanted it removed. That was in sleepy Dunedin.

Additional Sources of Useful Information:

Cryptography:

Schneier, Bruce, *Applied Cryptography*, 2nd Edition, New York, John Wiley & Sons, Inc., 1996, **ISBN 0-471-11709-9**.

Viruses:

Ludwig, Mark, *The Giant Black Book of Computer Viruses*, Show Low, Arizona, American Eagle Publications, Inc.,1995, **ISBN 0-929408-10-1**.

Networks:

Cheswick, William R., Bellovin, Steven M., *Firewalls and Internet Security*, Reading Massachusetts, Addison-Wesley Publications Company, 1994, **ISBN 0-201-63357-4**.

Electronic Mail:

Schneier, Bruce, *E-MAIL SECURITY: How to Keep Your Electronic Messages Private*, New York, John Wiley & Sons, Inc., 1995, **ISBN 0-471-05318-X**.

Document Security:

van Renesse, Rudolf L., *Optical Document Security*, Norwood, Massachusetts, Artech House, Inc. 1994, **ISBN 0-89006-619-1**.

Periodicals:

Computers & Security, Oxford, England, Elsevier Advanced Technology, 8 issues per year, **ISSN 0167-4048**.

Computer Fraud & Security Bulletin, Oxford, England, Elsevier Advanced Technology, 12 issues per year, **ISSN 1361-3723**.

Network Security, Oxford, England, Elsevier Advanced Technology, 12 issues per year, **ISSN 1353-4858**.

INFO Security News, Framingham, Massachusetts, MIS Training Institute Press, Inc. 6 issues per year, **ISSN 1066-7822**.

Privacy and Security 2001, Sterling, Virginia, Ross Engineering, Inc., 12 issues per year.

Internet Sites of Interest

http://ciac.llnl.gov/
CIAC Security Web Site

http://www.sei.cmu.edu/technology/cert.cc.html
CERT Coordination Center

http://www.cdrom.com/pub/security/coast/
F-PROT Zip files

http://www.ifi.uio.no/pgp/download.shtml
How to download PGP 2.6.3I

http://www.ifi.uio.no/pgp/PGPfone.shtml
PGPFone

http://www.tscm.com/
TSCM.COM Counterintelligence and CounterTerrorism Home Page

http://www.enter.net/~chronos/cryptolog.html
Welcome to Crypto-Log: Internet Guide to Cryptography

ftp://ftp.win.tue.nl/pub/security/
Directory of /pub/security

http://www.thecodex.com/
The Codex

http://www.nwfusion.com/
A Flurry of Firewalls

http://www.isecure.com/newslet.htm
SECURE NEWS

http://www.netsurf.com/nsf/v01/03/nsf.01.03.html
Netsurfer Focus on Cryptography and Privacy

http://www.engin.umich.edu/~jgotts/underground.html
The Internet Underground

NOTE: The Internet is a fluid living thing. What is valid today may not be valid tomorrow. One or more of these addresses may no longer active but give them a try.