Global Information Assurance Certification Paper

Michael Johnston
GSEC Practical Requirements version 1.3

Making the Case for Security at a Nonprofit Institution

The Internet is a marvelous, wonderful tool. In the last 5 years, the use of the Internet for business and personal purposes has grown to the extent that it has become a part of our lives we could not easily do without. On an individual level, and as people working for businesses both large and small, the Internet has created positive opportunities for education, business, and communication that have never existed before. In the last several years, it has also become a breeding ground for new problems that had not been envisioned by the founders of the Internet when they created it. The problems have grown up along with the opportunities, mostly without our conscious awareness of them until the last year. In order to continue to enjoy the benefits of the Internet, we must now take measures to safeguard our selves and our businesses from the problems. It will take educating ourselves about the nature and resolution to the risks now inherent in use of the Internet.

Nonprofits have started to make use of the opportunities that the Internet opens up for them, through organizations like the Center for Excellence in Nonprofits, and Compasspoint. Thus far, however, there has been far too little emphasis on the role of security and the necessity for it at a nonprofit. In general, nonprofit institutions, by their nature, their purposes and the ways that they grow, do not tend to have a great deal of technical expertise on their staffs. The technology "hat" in a small to medium sized nonprofit may be worn by someone who has many other responsibilities, and not enough time for all of them. Although many staff members may contribute to resolving technical problems, this does not necessarily produce the same results in a timely manner as would hiring a professional to address the issues. Also, having a small or non-existent budget for technology tends to emphasize more self-reliance on internal resources, i.e. those staff members who have some experience with technology but little time to be concerned specifically with the subject. Since, by definition, a nonprofit is an organization not established for the purpose of making money, but to serve a good purpose, there is also a general attitude that the resources that exist should be spent on furthering that purpose. Spending money on anything else may seem like stealing from the ones which the organization exists to serve. Outside consultants tend to be hired for focused, short term projects. So an attitude of ignoring potentially expensive problems may be a part of the organizational culture, to the degree that trying to find an inexpensive alternative may be taken to such an extent that it winds up taking much more time, and costing much more in the long run than a straightforward solution would have cost.

This attitude may extend to security, as well. Unfortunately, taking an attitude that what can be ignored will not harm you, is likely to result in disastrous

consequences in today's world of computer viruses, hackers, and the theft of valuable information from an organization's computers. There are so many clever ways that information can be stolen today that it is tempting to throw up your hands and not want to deal with it. After all, the amount of news appearing every day about computer theft is overwhelming! It comes down to examining the issues in terms of *risk management and defense in depth*, (as defined by Eric Cole in his book, Hackers Beware) so as to reduce the likelihood of an attack succeeding. It is not that you will not be attacked; you will. But it is not an impossible task to discover what the risks are, simply one which must be addressed a piece at a time, until you have a workable plan, and know what can be done about each one of them. The purpose of this practical is to show what some of the risks are and what can be done about them, in many cases without spending a lot of money. The answers to the threats will vary somewhat depending on the size of the organization. It is not my purpose to go into fine detail in this presentation on all the aspects of every security threat, but to give enough background to create an awareness of what some of the threats are, and point to the resources that will help you to find the detailed answers that you need. In my explanations of the issues, I will be trying to explain them in the simplest terms possible, given a subject that is inherently complex and technical.

Introduction - The Background

What does security mean in this context? The Random House Unabridged Dictionary defines security as 1) freedom from danger, risk, etc; safety. 2) freedom from care, apprehension, or doubt; well-founded confidence. 3) something that secures or makes safe; protection; defense.

Security is not an absolute, but a relative condition; there are degrees of security, based on the risks taken. Once we know how we are at risk, and from what or who, we can manage the risk to create a real sense of security and safety. To put this into perspective, because of the growth of the Internet and the services that most businesses (considering a nonprofit as a business) use on the Internet, the risk is for all practical purposes unavoidable. When the Internet was in the formative stages, no one thought about security - it was a whole new world opening up and trusted automatically. But with no built-in security (and Microsoft has paid little attention to security, historically) we have no built-in safeguards to our Internet access. If you could completely do without any connection to the Internet, if you could do without email and online services, most of this conversation would be unnecessary. But how many of us can do without email or online services today? Unless an organization cuts itself off from the Internet completely, it will need to deal with these issues.

Most nonprofits fall into the category of small to medium sized businesses. Along with the passion and idealism that many nonprofit employees bring to their jobs, there can also be the assumption that they are less likely to be

subject to hacker attacks and other attempts to gain entry to their systems and the data on them. This assumption may be based on the belief that since 1) a nonprofit is an institution dedicated to a good purpose, and 2) most nonprofits do not have much in the way of funds, who would harm them? Why would anyone bother?

These beliefs might give a false sense of security. As the Nimda virus/worm showed, everyone is vulnerable to virus attacks; viruses do not care about the kind of organization you may have. Similarly, hackers who are attempting to gain entry to a network have no idea that the IP address belonging to the server they are trying to hack into belongs to a nonprofit, and probably would not care if they did know. The point is simply that nonprofits are no less vulnerable, and no less likely to be attacked and penetrated, than any other business. And like any small business, it would not take much to damage it.

Defining what is at risk

So what are the risks? Although it might seem that a nonprofit does not have much that a hacker might want to steal in the way of data, this is almost certainly not true. Examples:

1. Do you take donations?
2. Do you have a web site that will allow donors to make donations?
3. Do you have software to track donors and donations?
4. Do you have accounting software that contains bank account numbers?
5. Account numbers of vendors?
6. Do you keep records of employees? Clients? Do these records have Social Security numbers, addresses, phone numbers, credit card numbers?

Even if you are a very small scale nonprofit, you are likely to have some or all of the above. If you have not taken some logical steps to protect your data, you are at risk of having that information stolen. And you may be liable if it is stolen. These are therefore the core of what needs to be protected.

How is the foregoing at risk?

Following are a few of the greatest issues, from the point of view of an attacker looking at your systems:

Issue 1. If you send and receive email, you are at risk of receiving and re-sending viruses, including what are known as trojans that may open up your system to other misuse. You can even pick up a worm virus by browsing a web site that has been infected, as happened with the Nimda virus.

Issue 2. Assuming that you have a connection to the Internet, you are at risk as long as your connection is open, whether it is a dial-up connection or an always-on connection such as a DSL, cable, or other high-speed connection such as a T1 or T3 line.

Issue 3. As small as this risk may seem, you are at risk if you have a server (or a workstation with critical data on it) in an unprotected area where anyone

not on your staff can access it for even a moment.
Issue 4. If you have installed a wireless network, or a wireless access point within a reasonably secure network, you have put your network at risk since wireless networks are not, yet, very secure.
Issue 5. If you have a network with a firewall, but still have PCs on the network that have modems, a hacker can get access to your network by using that modem.
Issue 6. If you do not have a good network security policy that specifies secure passwords and limited access by anyone who does not need more than minimum access, you are at risk. This is called the principle of least access. Too many companies - not just nonprofits - start out with a network that allows everyone to have access to everything because it is the easiest way to get started, not realizing how much danger they put themselves in. And almost every operating system in use today has a default installation that leaves all the access wide open to everyone. A integral part of a good network security policy is educating your network users and having their support. If you do not educate your network users about security, a result may be that they keep their passwords on yellow stickys on their monitors or under their keyboards.
Issue 7. Your key personnel have not been informed about the dangers of social engineering by persons who might want to penetrate their systems.

These are some of the more obvious potential security holes. It is not an all inclusive list, just the most often employed to penetrate networks and obtain data. I will discuss them one at a time. For definitions of the many of the terms please see the section on definitions at the end of the practical.

Issue 1. - Email
Everyone who sends and receives email is a target for email viruses, including worms and trojans, that arrive via your email server. This is the same whether you have your own server such as a Microsoft Exchange server or some other variety such as sendmail on Linux, or use a service which simply delivers email to you on demand such as AOL.
- Viruses are probably the best known, generically, because they have been around the longest. A virus is usually an attachment to an email, which in the beginning had to be an executable which you would run independently of the email itself. Virus technology has now progressed to the point where a macro virus can be included in the body of the email itself, and runs itself when you open up the email. They can infect a Word document or an Excel spreadsheet that someone sends you, whose computer is already infected. Viruses can be quietly resident on your PC for quite a long time, then suddenly become destructive on a particular date that it is set to go off.
- A Trojan can come into your system very quietly, masquerading as an innocuous program such as a game or a screen saver. The holidays are particularly dangerous for this - remember the cute joke someone sent you that they enjoyed so much they had to send it on to you? Once you open and run the program, it can have an entertaining quality that amuses you - all the while it is

installing itself on your computer and doing any of several things such as sending itself to everyone in your address book. It may also create a 'back door' on your computer, and send the information on accessing the back door off to the original creator of the Trojan.
- Worms, particularly mail worms, spread rapidly once activated. They are usually email attachments but can be embedded in the email itself and run when the email is opened. They will then search your address book for adresses, and email themselves to all your addressees. If there are mailing list addresses in your address book it may go out as a mass mailing.

Issue 1. Resolution Your main protection against viruses, worms and trojans is to obtain a good antivirus program like Norton Antivirus or McAfee, and subscribe to the updates. Then run the remote update program to keep your virus data files up to date, *every day*. And configure the antivirus program to check all your email as it comes in, and do *on-access scanning* as well. This will have the software check all your emails on arrival, and scan all files you open as you open them. There are several levels of antivirus software purchasing, depending on the size of your organization. For example, individual workstations can be covered by individually purchased packages of Norton AntiVirus (NAV) if you only have a few computers to cover and no network or a peer-to-peer network, or a single server. If you have a server on your network, do not forget to put antivirus software on the server! If you have a network with 50 or more PCs, several servers, and perhaps more than one site, you may want to look into a corporate licensing program. At that point, it will save you a some money to buy licenses that way. If you have grown to the point where you have your own Exchange server on site, you probably need to invest in the Norton Corporate Edition, which covers not only all your workstations, but your servers and your email server as well.

Issue 2. - The Internet Connection
Your Internet connection is the window of your PC to the world, but to a hacker, it is a door with few and weak locks that are for the most part easily bypassed. There is a lot of hype circulating about hackers. If you pay attention to the network news, from time to time you will hear about some hacker's exploit, and how vulnerable our computers are. The truth, unfortunately, is much worse than the mainstream media tells us. At this point in time, hackers have such an easy time about breaking into systems that it is truly scary. This is not a permanent condition, but one which needs to be addressed until the majority of the problems are dealt with. The reasons for the problem are many, but here are a few.

a. The default installation of almost all operating systems in use today - Microsoft, Unix, Linux, Mac (with the exception of Mac OS 10) - is to leave them wide open to anyone who wants to come in. And it is not a part of the installation of any of them, at this time, to give you a choice about what to leave open and what to close up tight, that the majority of us would understand. *You*

have to do it after the installation, and almost no one does. Recently, Bill Gates pronounced that Microsoft would now make security the top priority. But that simply admits to the world that MS operating systems have never been really secure. What you should understand about this is that up until recently, almost NO one has really thought in terms of security when the operating system is being manufactured, nor what to educate technicians about so that they can set up a PC to be secure when they install it. This is true for workstations, and it is true for servers. It is also true to a lesser extent for the equipment and software that controls our access to the Internet, no matter what the size or speed of the connection may be or the type of equipment.

Two examples from Microsoft will illustrate this.

1) When you install Windows 9x, the default installation leaves file and printer sharing turned on, which means that anyone who browses a network that machine is connected to can see everything on it if you do not set password protection. It is always best if you turn this off entirely.

2) The default installation of Windows NT will install IIS, or Internet Information Server, which is a web server. It installs it as a service on the server, which means that the service is running in the background and you won't know that there is an open door to your server - even though you may not be using it for anything. You have to at least shut down the service, and ideally eliminate it entirely from the server if you are not using it. By default, it is wide open to anyone who knows the password to get into the default installation.

b. Your PC, server, and firewall communicate through what are called ports. These are the doorways or windows through which communication takes place. For example, when your web browser inititiates a connection to a web site, it picks the first available port. Each computer has 65,536 ports to do this with, as does a firewall. The first 1024 ports are reserved for "privileged use", meaning that services the server (and your PC is a server in this regard) provides, such as HTTP, FTP, and so on, use these ports. But any hacker can also try to gain entry to your PC or server, and then to your network, through these ports. To put this into perspective, a hacker who gains entry quietly by a port you are unaware of, then installs a backdoor program that allows him to remotely control your server. This is exactly as if you had installed PCAnywhere on the computer and allowed anyone to dial into it. In fact, Gator, the digital wallet program, was reported by Symantec in March 2002 as having its installer, GatorSetup.exe, infected with the Backdoor.Trojan virus.[Footnote] This allowed unauthorized access to the infected computer - just as if you had PCAnywhere installed.

How do hackers do it? The tools to do it are all out there on the Internet. In simple terms, they use a port scanning tool, easily available on the Internet, to perform a port scan of your firewall (and/or your PC/server if it is directly connected to the Internet with a DSL or cable connection) to find what ports are

open. Then they use a combination of other tools to attack that port, in various ways, until the machine with the port open says, OK, you are legitimate, you can come in. The hacker then installs a backdoor program, and he is in. But it is much easier for the hacker if he can send you an email that has a cool game attachment containing a trojan, that will set up the backdoor from the inside, as soon as you run it. Another way for hackers to get in is by means of the services running on your server, which you are not using, but which were installed initially in the server or workstation setup. Both HTTP and FTP are examples of this. Think about it - if a hacker discovers that port 21 (FTP) is open and the FTP service is running on your machine, without any configuration beyond the default installation, he can gain access to your machine, upload a backdoor program using FTP, and he has access to your machine.

Issue 2. Resolution

1. Microsoft established an Incident Response Center, to handle security issues with its operating systems, and continuously issues patches that need to be applied to their servers. There is even a program they recommend you install on your servers that will alert you to the latest patches, called BigFix, which will go out and check for the latest patches, by category, and put a message on the server screen to tell you that there is a fix that needs to be applied. It may be time consuming, but these fixes are your security updates and should be applied. Similarly, your Windows 9x, ME, 2000 Pro, and XP machines have a Windows Update utility that will start your IE browser, take you to the Microsoft web site, and when you select Product Updates, it will do a check on your operating system. It will then determine which, if any, of the available updates you need to download and install to close security holes. While not the entire answer, it is a definite help, and needs to be done regularly as new security holes show up.

2. A firewall is a necessity, though it is not all the answer. For single home users with DSL lines, as well as small offices, there are inexpensive devices such as the Linksys Cable/DSL Router series (and there are many brands with similar functionality) that has Network Address Translation (NAT) built into it. Briefly, what NAT does is to take the external IP address that the ISP assigns to you, and translates it into something on the other side of your router (where your server and PC are connected) so that there is not a direct connection to the Internet. The potential attacker only sees the external address, and can't get to your PC directly. Larger networks have more complex routers that are more configurable, but the Linksys and its cousins will do a good job. Other, better equipment includes the SonicWall routers, and of course Cisco.

3. A desktop intrusion detection system, in addition to antivirus software, is highly recommended for small networks. Several good ones are BlackICE and TripWire, which are inexpensive. Larger networks need to have more complex - and therefore more expensive alternatives, such as Cisco's Secure IDS, or NetIQ's Security Manager. You may think that this is not necessary, but it is

most likely that your network is being scanned frequently. Eric Cole of the SANS Institute, stated in the Security Essentials course recently (SANS Darling Harbor, Security Essentials Track) that even if you have an intrusion detection software set up, if you are not seeing 12 to 24 scans and attempts to penetrate your network every day, you are probably not looking in the right place. And he went on to say that prevention is ideal but detection is a must.

4. Lock down your servers! Shut down unnecessary services, and close ports that you do not need. As in item 1 above, keep the patches up to date. There are several good guides for doing this. I have directed my comments at Microsoft operating systems, because the majority of the smaller businesses use their products, but the guides apply to Unix and Linux systems as well. One such is available on the InformIT.com web site; it is an article entitled The Dirty Work: Maintaining Basic Linux Systems Security, by Jon Lasser. It can be found at InformIT.com in the Articles section. Login is free, by entering your email address. Other material on locking down your Microsoft servers can be found on the Microsoft web site. See also Building a Windows NT Bastion Host, but Stefan Norberg, at http://people.hp.se/stnor/. His articles are downloadable from that site. He is also the author of Securing Windows NT/2000 Servers for the Internet
A Checklist for System Administrators, available by clicking on the link on the above web site.

5. Make use of the resources available from a search of the Internet to help you secure your network. A very good white paper entitled Principles of Secure Network Design is available for download and printing from Netscreen Technologies, Inc. web site. It explains the terminology, and what you need to do to protect your networks in relatively plain language. It is available at this URL: http://www.netscreen.com/solutions/index.html. You will need to login to download the paper, but login is free.

6. Do not rely only on one firewall to safeguard your network. This is the principle behind Defense in Depth. Consult Hackers Beware! by Eric Cole, regarding Defense in Depth. Also see Software security principles: Part 2 Defense in depth and secure failure Gary McGraw (gem@cigital.com), Vice president of corporate technology, Cigital, and John Viega (viega@cigital.com), Senior research associate and consultant, Cigital, at http://www-106.ibm.com/developerworks/security/library/s-fail.html?dwzone=security

Issue 3. Physical Security.
This is a topic that is not paid much heed. Your servers and your workstations can be compromised by a person who walks in the door, strikes up a friendly conversation with you or your receptionist, and asks if he can use the bathroom. When he walks down the hall, he sees your server in an unlocked room that has the door open. He walks in, closes the door behind him, and if the server itself does not have a strong password, or even more likely, is already logged in, he has all your data to do with as he wants. This scenario may be all too likely

since the space a small nonprofit has to devote to a server may be small indeed. The server may be in a corner of an office, for lack of a small room to lock it up in. Does this sound familiar?

Issue 3 Resolution There are a few obvious answers to this problem. First, if you have a server, never leave it logged in. That will avoid the simplest issues. Second, If you have the space to assign to your server, lock it up! A corner of a locked, air conditioned supply closet would do as well if you can't give it a space of its own.

Issue 4. Wireless Networks

Wireless networks are a relatively new topic, and which keeps cropping up as a great new technology for people to use that allows a great deal of flexibility. While that is true, wireless technology, like most new technology today, does not have very good security built into it. What this means is that a hacker could sit across the street - or in some cases across the San Francisco Bay on a hilltop, with a directional antenna - and hack into a wireless network. The most popular protocol 802.11b uses a security algorithm called WEP (Wired Equivalent Privacy) is not secure at all according to several researchers at the University of California. You can see their article on the Internet at: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
Also, in the last several weeks, the first wireless exploit tool was released on the Internet for hackers, called AirSnort. After monitoring transmissions until between 100mb and 1gb of data has been gathered, it AirSnort can guess the encryption password in less than a second. See the following URL for this article on this tool: http://www.vnunet.com/News/1124818

Issue 4 Resolution The easiest resolution is, of course, don't use wireless. It is not yet securable enough that it will not compromise all your other security measures if you put a wireless connection into your secure, wired network. Remember that while you may think that you don't have anything that you care if anyone else sees, that may not be true when you consider what you have on your PCs and servers in the way of financial and personal data. As neat a technology as wireless is, it bears watching for future developments. But as of now, I would not recommend it for use in conjunction with networks that have any critical data on them.

Issue 5. Modems

As most small nonprofit organizations have grown over the last few years, they have started out with modems for connection to the outside world, and only lately have they begun to get faster Internet connectivity in the form of DSL, cable or T1 lines. But often when they get the faster connection, they forget about the modem line, and it is still there with a modem attached to the PC. And the odds are about even that the modem is set up with autoanswer on. This means that if a hacker calls that number, and gets an answer, he may have instant access to your PC. If your PC is connected to your network, and logged

in, he has access to everything that you have access to. Your firewall will not keep that person out.

Issue 5 Resolution The answer is obvious - if you have a fast connection now to the Internet, disconnect all the modems and terminate service to the lines. If you do not have a fast connection and still depend on a modem, make sure that the autoanswer function of the modem is turned off.

Issue 6. Network Security Policy
A network security policy is necessary if you are going to set up planned, working organizational security. A good deal of the foregoing issues are covered in a good network security policy. Do your users understand the implications of network security for the organization, beyond their own jobs? Have they been informed about security issues and why they should support security? Does management understand the impact of a security policy, or its lack? These are critical questions to the adoption of a security policy, because implementing such a policy will call for all users to make changes to the way they work. That is in addition to the volumes of work that will be called for by the IT person or persons, to create, and then implement, a network security policy. This will be the most challenging part of instituting security for an organization. But it is also the most necessary.

Issue 6 Resolutions There are a number of resources available to support you in creating a network security policy. A search of the Internet turned up some interesting ones, from free to relatively expensive. The free ones are simply Adobe Acrobat files you can download and print. The expensive are combinations of software and lists which you can interact with to create your own security policy that is tailored to your organizational needs. Also available is software to help you implement the policy.

The free paper, available from a web site, is called Why Should You Enforce a Network Security Policy? and is available from the usenix.org web site, in the December 2000 issue of the ;login: magazine, the magazine of usenix and sage. as a article listed on their index at:
http://www.usenix.org/publications/login/2000-12/index.html
The ones you might want to buy may be found at the web site at the Information and Security Policies World, at:
http://www.information-security-policies-and-standards.com/
And another one that may be different, is found at:
http://www.network-and-it-security-policies.com/

Issue 8. Social Engineering This is fairly simple in concept, if you remember that it is basically about a confidence man trying to gain admittance to your network by 1) talking you into letting him get access that he is not supposed to have, or 2) getting sufficient information from you to get in without your overt permission and help. While nonprofits may not be targets for social engineering as much as

a commercial enterprise, it is worth mentioning to alert you to the possibilities. It could be as simple as a story told by Eric Cole of SANS, about a person who researches a company, finds out that they are hiring a lot of people for various positions, and guesses that they are staffing a new site. Because the multiple advertisements for staff have the name of the same hiring person, say Joe, on them, he guesses that the person is probably too busy to keep track of ever detail. So he calls up the main number for the company, and asks to be transferred to the help desk, thereby getting an inside line rather than a call coming from outside. He tells the help desk person he is a new hire, just brought on board by the Joe, and asks the help desk for a login and password, saying he has just arrived and wants to do some work. He also knows that the Joe is not available, so the help desk will not be asking him awkward questions. By creating a relationship with the help desk person, eventually he gets a login and password, and he is in to their network. He also asks for, and gets, a remote dial-in number.

This is only one example; there are many more. For more detail, you can see Eric Cole's book, Hackers Beware, on the topic of Spoofing.

Issue 8 Resolution Although not easy, there are some key things you can do to protect your network and users from social engineering attacks. It mostly comes down to educating your users, especially the ones in key positions such as the receptionist, administrators, and the help desk personnel on the network security policies, which should have material on what is allowed and what is not regarding giving people access to your network. Make sure that the policy is advertised and given support by management - it will make all the difference.

Conclusions

Nonprofits have a rich variety of resources available to them to not only obtain technology through donations and price reductions available to them, but because of the Internet, they also have the information available to begin to secure their networks and the data they need to safeguard. I have tried to show some of the vulnerabilities that nonprofits may not be aware of, so as to make a wake up call. I also have tried to give some direction to the search for answers to the issues I have raised. As I stated in the beginning, I have not tried to give a detailed explanation of every security threat; that would take a book in itself. I have tried to pick out the issues that seem to me to be most likely to not get addressed by nonprofits. As organizations, nonprofits may be paying more attention to their missions and simply trying to obtain the resources to further them. Security, in that context, might be taking a distant back seat, and the day has arrived when it must be addressed.

Definitions Used

Hacker - this is a much overused and misunderstood term. Originally it meant simply someone who was proficient at programming code. Now it is confused

with negative connotations, and everyone sees the hacker as the boogieman. To differentiate between good and bad hackers, we now have other terms, such as:
White Hat - a good hacker who is most often a security specialist, and uses security tools to both test network security from the outside and inside of the network, but to catch attempted exploits before they become damaging.
Black Hat - a bad (criminal) hacker. Spends time attempting to break into your system so as to steal information from databases, deface your web sites, create chaos and generally cripple your network (and along with it your business).
Cracker - a hacker who is a black hat, but is mostly interested in slipping quietly into your systems and networks, taking what he/she is looking for, and getting out again - without your ever knowing they were there. Causes little or no overt damage because does not want to alert you to the fact that you have been compromised. The good ones already have your data and you don't even know it happened.
Script Kiddie - a newbie who has just started into hacking, has found some tools out on the Internet, and puts together an attack using them. Does not really know what he/she is doing, just wants to see if can do something. This kind of hacker is most likely to do overt damage to your systems. As an old hacker presenting at DefCon 9 2001 stated, he would be much more afraid of 25 script kiddies than of a single cracker, because the script kiddies would destroy your networks and systems, where the cracker would not. Though the cracker quietly stealing your data would be a longer-term problem if it was used or sold to someone else, your systems would still be working. That might not be much consolation in the long run, however!
Virus - a computer program that is designed to infect your computer as a biological virus infects a live organism, replicating itself and spreading through the computer and often broadcasting itself via email to other computers. May have consequences ranging from trivial (a simple splash screen with a cute message) to catastrophic (wipes out the computer's hard disk). See Reference 4.
E-Mail Worm - similar to a virus, but more independent. Email worms were originally spread by being a message attachment that had to be opened (try the neat screen saver or joke program!), but evolved into a program that could be embedded into an email message so as to be run when the email is opened and read. Usually sends out email messages to everyone in the recipients' address book, containing a copy of the worm. See Reference 4.
Pure Worm - a worm that does not depend on human interaction like an email worm, but spreads by attacking always-on, internet connected servers. Examples would be the Code Red worm that attacked Microsoft IIS (Internet Information Server) machines. Since IIS machines are essential to Exchange email servers as well as being the machines that host web sites, the Code Red worm did (and still does) a lot of damage. See Reference 4.
Trojan - a virus program that is effective by being deceptive, having an overt and a covert function. An example would be an email message from a friend with an attachment that they think is a neat screen saver, but in reality is a trojan that will install a program on the computer for the benefit of the virus creator. Often

this will be a back door to allow the creator to access the computer remotely, without the owner ever knowing it was done until it is too late. See Reference 4.
Polymorphic Virus - a virus that changes its own code to avoid detection. See Reference 4.

REFERENCES

1. Center for Excellence in Nonprofits, www.cen.org
Compasspoint Nonprofit Services, www.compasspoint.org

2. The Random House Dictionary of the English Language, Unabridged Edition, copyright 1979, Library of Congress Catalog Card Number: 74-129225, p. 1290.

3. OMB Watch
http://www.ombwatch.org/article/articleview/600/1/77/

4. F-Secure Corporation, September 2001 white paper, "Computer Viruses - from an Annoyance to a Serious Threat"

5. Hackers Beware, Eric Cole, copyright 2002, New Riders Publishing.

6. What is the risk to Windows 9x from Dedicated Internet Connections?
SANS Security Resources Intrusion Detection FAQ
http://www.sans.org/newlook/resources/IDFAQ/DIC.htm

7. DShield.org Incidents Detection
Internet Primer - Definitions of Internet terms
http://www.dshield.org/primer.html

8. Microsoft OS Product Updates are found at:
http://windowsupdates.microsoft.com
Click on Product Updates and follow the prompts.

9. Principles of Secure Network Design, by Netscreen Technologies
http://www.netscreen.com/solutions/index.html
Login is necessary but free.

10. Software security principles: Part 2 Defense in depth and secure failure Gary McGraw (gem@cigital.com), Vice president of corporate technology, Cigital, and John Viega (viega@cigital.com), Senior research associate and consultant, Cigital, at http://www-106.ibm.com/developerworks/security/library/s-fail.html?dwzone=security

10. Washingtonpost.com Newsbytes, 07 March 2002

Gator branded a Trojan Horse Despite Security Fix,
http://www.newsbytes.com/news/02/175046.html

11. Security of the WEP algorithm, by Nikita Borisov, Ian Goldberg, and David Wagner, University of California at Berkeley. Contact at wep@isaac.cs.berkeley.edu. Article may be found at: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

12. IT Security Policies and Network Group.
http://www.network-and-it-security-policies.com/

13. Stick to the Essentials: Configuring Servers Securely
by Julia Allen, the Author of CERT® Guide to System and Network Security Practices, MAR 22, 2002