21 Myths About Computer Security

Myth: *The worst computer security threats are from the Internet and hackers.*

Reality:

No, employees pose the biggest computer security threat. It is estimated that between 50% - 80% of all computer security problems are "inside jobs". Former employees, unhappy employees and poorly trained employees are the greatest computer security threat. Make sure you have a policy to remove computer privileges for terminated employees. Computer security starts with good internal policies. The best firewall and anti-virus system won't protect you if the "barbarians" are already inside the gates!

- Wen Ho Lee, a US nuclear scientist, may have either given away by mistake or stolen very sensitive information via his computer.
- In September, 2000, a laptop that had confidential information was stolen from Qualcomm's CEO.
- In February, 2000, a laptop with "highly classified" information disappeared from the US State Department.
- John M. Deutch, former CIA director, used an insecure home computer to draft confidential documents.

If a bad guy has unrestricted physical access to your computer, it's not your computer anymore. Microsoft's Scott Culp.

Why invest in a firewall if you let your computer walk out the door?

Myth: *Only open email attachments from known senders.*

Reality:

That is a good start. There are viruses that propagate themselves through the Microsoft Outlook Express address book. Thus, if someone that you know has you in their Outlook address book and has been hit by the SirCam or the Magistr viruses, their computer (without your friend's knowledge) will send you a friendly email with an interesting attachment. If you open that attachment you will send the same virus to those in your Outlook address book. When you finally get a call from someone who used to trust you, you will probably have to reinstall Windows to fix your problem.

Myth: *Security experts don't get hacked.*

Reality:

We are familiar with an organization that gives excellent seminars on security. They admitted to being hacked a minimum of two times.

Steve Gibson, a well known computer expert, indicated that his Web site was a victim of a Denial of Service (DoS) attack. The hacker that did that was a 13 year old.

Myth: *You don't need to be concerned about new viruses until you get an email from your virus scanner provider. That is because developers of virus scanner software send email to customers when a bad virus has been discovered.*

Reality:

Anti virus software developers usually notify customers via email when they have a solution to detecting a bad virus. There is a critical difference between being notified that a bad virus is spreading quickly and being notified a day or two later that there is finally a definition file that will help block the virus.

Get on a mailing list of a service that will notify you when there is a new, damaging and active virus on the loose. Your anti virus software developer might send you that email hours or several days too late.

Myth: *You only need a good virus scanner.*

Reality:

This really depends on needs of the business. What if the hacker works (or once worked) with you. They might be able to walk up to a machine, put a floppy in the computer, and walk away with sensitive information.

Virus scanners usually don't stop hackers from gaining access to your system via the Internet. If hackers get that far, they might be able to remotely access, view and even change information on your system. A break – in is not a virus, and virus scanners look for viruses.

Myth: *You can't get a virus from plain text email.*

Reality:

Email that contains html code usually looks like a Web page. Email that has html code can contain a virus. That is because of ActiveX, JavaScript and other components that can be hidden in email that looks like a Web page. So, what does this have to do with plain text email? Email with html code can be designed to look as if it is plain text, but invisibly contain the virus threat. If it appears to be a plain text email, you really don't know for sure that it is plain text.

Myth: *If you buy and install the best virus scanner, you won't get viruses.*

Reality:

In 1998 that could have been a true statement. In 1998 it took about a year from the time that a virus was discovered to the time when it could infect lots of systems. Viruses (we are including computer worms with viruses) are spreading at a faster rate than before. It is critical to periodically update the scanner's virus definitions. In 2000 updating definitions monthly was prudent. In early 2001,

weekly definition file updates made sense. Towards the end of 2001, daily virus definition updates are barely fast enough.

On September 18, 2001, the Nimda virus spread throughout the Internet in a matter of hours.

Needless to say, it is best to schedule daily virus definition downloads to run automatically every night.

Myth: *The greatest computer security threat is that of a hacker trashing my system and network.*

Reality:

The data on the system is usually more valuable than the system itself.

The worst threat is to have something stolen from the system, and have no idea that it was stolen. The hacker breaks into your system; the hacker steals your important information; and the hacker doctors the logs. The information is gone or duplicated, and there is no trace that the system was hacked.

What would happen if your identity was stolen? Possible financial ruin. What would happen if your customers' credit cards were stolen from your system? Possible financial ruin and loss of reputation.

Myth: *Buy the most computer security that you can afford.*

Reality:

The cost of computer security must be justified. Your business needs more security than a kid's home computer but less security than one of the FBI's computers. What could a computer security problem cost you? What are the most likely computer security threats that you face? How much does it cost to close security vulnerabilities?

Some of the best computer security measures are inexpensive. Locks on doors and hard to crack passwords are inexpensive and fairly effective.

Myth: *If you hire a security "expert," you don't need to get involved with security yourself.*

Reality:

At a minimum, you need to know enough about security to get a feeling if something is going wrong. A security consultant should be enough of an "expert" to explain to you what she is doing, and what you need to look for.

Myth: *Windows NT4, 2000 and XP® are secure systems since they have achieved high Federal government security ratings.*

Reality:

It is true that Windows 2000 and NT4 (with Service Pack 6a) have received the NSA (National Security Agency) C2 rating. A C2 security rating is more security

than most business need. However, Windows NT4 and Windows 2000, as they come typically installed, have plenty of security holes. You have to take the time to plug the security holes. We don't yet know how secure XP really is.

Myth: *Only machines that host Web sites might run Microsoft® Internet Information Server (IIS).*

Reality:

If you are using Microsoft's FrontPage® on a Windows® NT4 or 2000 system, chances are that you are constantly running IIS in the background.

What if you are running IIS? IIS takes some work to make it secure. Microsoft has been good enough to make security patches available for IIS. If you are running IIS, and you have not taken advantage of those patches, you probably have been hit by the Code Red and Nimda virus (worm).

Myth: *Microsoft Windows XP is the most secure version of Windows yet.*

Reality:

We don't know that, and would you bet your business on a Microsoft promise? New Microsoft operating systems often need to go through one or two service packs before most of the security holes have been fixed. Windows XP might be the most secure Windows operating system, but do you want to be the guinea pig?

It takes time for hackers to discover security problems, and it takes time for security experts to figure out the solutions. Books that describe how to close some Windows 2000 security problems were published only months before the Windows 2000 replacement (XP) was released.

Myth: *A strong password can't be broken.*

Reality:

A strong password contains upper and lower case letters, numbers, one or more special characters. A strong password is typically seven or more characters long. A strong password does not contain the username, words or names. If possible, passwords should contain non printing characters.

A strong password can be broken or cracked with commercially available software. A strong password takes much more time to crack than a weak password. Breaking a strong password takes a "brute force" attempt to crack, but it definitely can be done.

Myth: *Since a router is attached to my DSL line, I am safe from hackers.*

Reality:

A router can help with computer security, but its primary purpose is to move packets of data to appropriate destinations as fast as possible. Don't mistake a router for a firewall. The purpose of a firewall is to block unwanted access to a

network and to stop certain types of information from leaving a network. A properly configured firewall usually provides better security than a router.

With an always on 24/7 DSL line, a firewall should be used. A 24/7 DSL line is much easier to hack than an Internet connection that is only turned on when needed.

Myth: *The best rated firewall installed by an expert will protect a system or network.*

Reality:

Yes and no. Security holes in firewalls are discovered frequently. On occasion check to see if there is an update available for the firewall.

Also, firewalls are setup to permit various types of Internet traffic. It is possible for a hacker to get into the network using a permitted type of connection.

Think of computer security as an ongoing process rather than a one time project.

Myth: *If you have an Intrusion Detection System (IDS), you don't need a firewall.*

Reality:

Think of an IDS as a motion detector in a home security system. Think of a firewall as a solid door with a deadbolt. Would you leave your door wide open so the motion detector could warn the family? No, you would make sure the door is closed and locked. The IDS like a motion detector is useful, but it is neither the first line of defense nor the first security measure to consider.

Myth: *There is so much information going over the Internet that it is next to impossible to have someone eavesdrop on me.*

Reality:

There is something called a Man – In – The – Middle attack were someone "listens" to email or file transfers between two parties. There is actually software that can automatically read other's email and data transfers. When the software detects something that it is supposed to watch for, it saves the information for the hacker.

Targets could be email between lawyers, accountants and their clients. Targets could be businesses with new critical products.

Myth: *Security is about protecting your computers and data.*

Reality:

Computer systems security is more that protecting computers and data. For accounting firms, computer security is also about image, trust and confidentiality. An accounting firm is in trouble without a good image, trust and confidentiality. If someone steals client identities, an accounting firm can be in deep trouble. A business that relies on transmitting information to its business partners is in

trouble if those partners cannot trust that the information is accurate and confidential.

Myth: *Hackers work alone while chain smoking and drinking Jolt or Code Red.*

Reality:

We have a problem with the “work alone” part of that statement. There is lots of free or inexpensive software that can be used to break into systems or create viruses. The Senna Spy Worm Generator 2000 can create email viruses where you enter some information, and it will create a virus for you. You might be surprised at the source of some software used to hack systems. Some of this software is pretty easy to use.

Microsoft has made available software to trouble shoot network problems. That same software can be used to gather information about a hacker’s target.

Myth: *We have never had security problems before.*

Reality:

1)Are you sure of that? 2) So what! If you haven’t had problems before consider today’s economy. Lots of technically talented are now out of work. A very small percent of them want to prove to the world that they are too smart to be in the predicament that they find themselves in. How are some going to show you that they have been wronged? They are going to hack your system and infect your system with nasty viruses if you give them a chance.

There are documented situations where hackers have been using other people's computers for there own benefit. The computer owner is not even aware that their computer is being used by someone else.