AltiusIT

Viruses and Electronic Threats
Frequently Asked Questions

Introduction
More than ever before, companies are relying on the Internet to assist them with their day-to-day business activities. As more and more employees require access to the Internet, firms are encountering greater threats to their "information assets".
Questions

1. In the simplest of terms, what are viruses, worms and trojan horses?
Viruses, worms, and Trojan horse programs are various types of hidden, and unwanted, electronic threats. For the most part, they don’t damage your computer hardware, only your software, system configuration, and valuable data files.

2. What's the difference between the three?
Malware (malicious software) - Specifically designed program to disrupt or damage your systems.

Trojan Horse - a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.

Virus - A program or piece of code loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. They may damage your systems by deleting files, corrupting documents, and using the computer's memory and processor.

Worm - a special type of virus that can replicate itself and uses memory. Unlike other types of viruses, it cannot attach itself to programs.

3. Should businesses be concerned about them? Especially businesses without an IT department?
Electronic threats such as viruses, Trojan horses, and worms have the ability to destroy the internal software configuration of a computer system. In addition, these threats also have the ability to completely destroy any data that exists on the machines. Unfortunately, many businesses don’t have adequate protection. Since the threats are hidden, firms may not take appropriate steps to protect their organization from a disruption in their business operations.

4. What should businesses be concerned about?
Many businesses know about the visible threats such as vandalism, theft, and fire. Harder to evaluate are hidden threats such as hackers and viruses, worms, and Trojan horses. We recommend that businesses determine the impact to their organization should they experience a failure in their computer systems. For

example, what is the impact over time if computer systems are unavailable for one day, two days, one week, two weeks, etc. Since each business is different, each organization will have a different answer. The organization should take the appropriate steps, depending upon the criticality of the information to be protected, to get their systems up and running again within their required timeframe. Obviously, preventing downtime is preferred.

5. What could happen? What could businesses lose if they are targeted?
Viruses, worms, and Trojan horses all have the ability to damage your system configuration and destroy your data. In many instances, you won't know the system has been damaged until you try and use it. There are often no advance warning signs.

6. How can businesses prevent from being attacked? And what can businesses without IT departments do to prevent it?
The first step is to establish a reliable method of backing up your system configuration and your data. A reliable backup plan includes storing media off-site. This way you will have your information available to you even in the event of a disaster such as a fire. The frequency of backing up your systems depends upon the criticality of the information to be protected. The more valuable the information, the more frequently it should be backed up and stored off-site. Once you have a backup solution in place, the second step is to acquire anti-virus software. Major vendors such as McAfee and Symantec provide affordable software protection. Since new threats emerge on a weekly basis, most organizations should have the anti-virus software configured to automatically check for new updates.

7. If an attack does happen, how can businesses fix the problem?
Threats come in all shapes and sizes. Some viruses only delete certain types of files while others may wipe out your entire hard drive. I'd recommend the business contact a computer professional to assist them in restoring their systems to full functionality. The professional can determine the extent of the damage and minimize the time it takes to restore normal operations. The goal is to minimize disruption to the business operations. As a last resort, the computer professional may need to restore the entire system from the backup media. Unfortunately, this may mean that the business has to re-create any transactions or documents that were created since the date of the most recent backup.

Summary
Each organization has a unique environment that makes it difficult to protect against new and emerging threats. Network security audits help organizations identify, manage, and reduce their risks.

Publication Information
Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.