In defining computer viruses Parsons and Oja wrote that the technical definition of a computer virus is a set of program instructions that attaches itself, and spreads to other files. Viruses corrupt files, destroy data, displays irritating messages, or otherwise disrupt computer operations. (185)

In continuing, Parsons and Oja explained that there is a common misconception that viruses contain program codes to spread themselves from one computer to another. They do not. The reason viruses spread is because people redistribute infected files by exchanging disks and compact discs, sending e-mail attachments and downloading software from the Web. (185)

For the book titled Computer Concepts, it is learned that a computer virus generally infects the files executed by your computer such as those with .exe, .com or .vbs extensions. When a computer executes an infected program, it also executes the attached virus instructions. These instructions then remain in the Random Access Memory, waiting to infect the next program that the computer runs or the next disc it accesses. (185)

In addition to replicating itself, a virus might perform a trigger event, sometimes referred to as payload. The resulting effects can range from displaying an annoying message to corruption of data on the computer's hard disk. Trigger events are often keyed to a specific date. The Michelangelo virus, for example was designed to damage hard disks on March 6, the birthday of artist Michelangelo. (185)

A key characteristic of viruses is their ability to lurk in a computer for days or months, quietly replicating themselves. While this is taking place, a user might not even know that his or her computer has a virus; therefore it is easy to inadvertently spread infected files to other people's computers. (185)

According to CNN.com Technology, there are thousands of variations of viruses, most falls into one of the following six general categories, each of which works its magic slightly differently.

The first category of viruses is the Boot Sector Virus. This virus replaces or implants itself in the boot sector---an area of the hard drive (or any other disk) accessed when you first turn on your computer. This kind of virus can prevent you from being able to boot your hard disk. Second is the File Virus which infects applications. These executables then spread the virus by infecting associated documents and other applications whenever they're opened or run. Third is the Macro Virus. It is written using a simplified macro programming language, these viruses affect Microsoft Office applications, such as Word and Excel, and account for about 75 percent of viruses found in the wild. A document infected with a macro virus generally modifies a pre-existing, commonly used command (such as Save) to trigger its payload upon execution of that command. Fourth is the Multipartite Virus. He virus infects both files and the boot sector--a double whammy that can reinfect your system dozens of times before it's caught. Fifth is the Polymorphic Virus which changes code whenever it passes to another machine. In theory these viruses should be more difficult for antivirus scanners to detect, but in practice they're usually not that well written. Finally there is the Stealth Virus which hides its presence by making an infected file not appear infected.

It must be noted that not all malicious codes are viruses. A common misconception is that other kinds of electronic nasties, such as worms and Trojan horse applications, are viruses. They aren't. Worms, Trojan horses, and viruses are in a broader category analysts call "malicious code." A worm program replicates itself and slithers through network connections to infect any machine on the network and replicate within it, eating up storage space and slowing down the computer. But worms don't alter or delete files. A Trojan horse doesn't replicate itself, but it is a malicious program disguised as something benign such as a screen saver. When loaded onto your machine, a Trojan horse can capture information from your system -- such as user names and passwords--or could allow a malicious hacker to remotely control your computer.

Daily many computer users participate in the spreading of viruses without knowing they did. Viruses can slip into your computer from a variety of sources. The most common sources of file viruses, boot sector viruses, and Trojan horses are floppy disks, homemade compact discs, and Web sites that contain games and other supposedly fun stuff.

A common misconception is that write-protecting your floppy discs by opening a small hole in the corner of the disc prevent virus infection. Although a virus cannot jump onto your disk when it is write-protected, you must remove the write protection each time you save a file on the disk. With the write-protection removed, your disk is open to a virus attack.

Another common source of viruses is e-mail attachments. A seemingly innocent attachment could harbour a file virus or boot sector virus. Typically, infected attachments look like executable files, usually with .exe filename extensions, although they can have .sys, .drv, .com, .bin, .vbs, .scr, or .ovl extensions. These files cannot infect your computer unless you open them, thereby executing the virus code that they contain.

In order to assist users in identifying whether their computers have a virus, there are some symptoms which they can look for. It must be noted that the symptoms depend on the virus. The following symptoms may indicate that your computer has contracted a virus, though these symptoms can have other causes.

(1) Your computer displays vulgar, embarrassing, or annoying messages.

(2) Your computer develops unusual visual or sound effects.

(3) You have difficulty saving files, or files mysteriously disappear.

(4) Your computer suddenly seems to work very slowly.

(5) Your computer reboots unexpectedly.

(6) Your executable files unaccountably increase in size.

(7) Your computer starts sending out lots of e-mail messages on its own.

It is important to remember, however, that some viruses, worms and Trojan horses have no recognizable symptoms. For example, a computer can contract a worm that never displays an irritating message or attempts to delete files, but which replicates itself through an e-mail until it eventually arrives at a server where it can damage a network communication system.

In looking at the history of the development of Computer viruses, Wang wrote that the first known PC virus was created in 1986 by two Pakistani brothers, Amjad Farooq Alvi and Basit Farooq Alvi, who ran a software company called Brain Computer Services. The brothers discovered that the boot sector of a floppy disk could contain instructions other than those used to load an operating system. Then, like now, software was being illicitly pirated. So, the brothers created a virus called the Brain virus that would infect any machine that used illegal copies of their software to punish the perpetrators. Prior to the Brain virus, there had been reports of viruses lurking on Apple machines in 1981. These Apple viruses were propagated through the exchange of pirated games (237).

Within the world today, Information Technology can significantly enhance the way businesses are conducted. This can be done in two different ways. First, it can simply be used to automate the processes already performed in an organization. Automating processes has many advantages, such as making the process faster, more reliable and less error prone, and allowing the organization to deal with many more cases. Second, information technology can be used by organizations to completely re-design the way in which they perform their business operations.

Today, the Internet ties together businesses and homes across the globe, and countless people depend on e-mail to communicate. In a CBS news report, Kevin Poulsen, a security analyst, explains, "These days, companies are so reliant on e-mail, that if they can't send or receive e-mail, it costs them money. (1)

The emergence of the internet has led to even more dramatic changes in the way business is conducted. Many commercial organizations have been attracted to the Internet and are using it for commercial properties often referred to as e-commerce, or e-business.

Companies have become involved in e-commerce for a number of reasons. First, the Internet enables them to significantly reduce their transaction costs. For example the cost of conducting a simple bank transaction over the Internet is less than 5% of the cost of conducting the transaction face-to-face and less than 25% of conducting that transaction using an Automated Teller Machine. Second, the internet has enabled companies to build new relationships with customers and suppliers. Many companies for example insist that potential suppliers wishing to reply to a request for tenders submit their proposals over the Internet. Finally, many companies have either set up entirely new businesses on the Internet while others have seen Internet businesses take a significant slice out of their market share and have therefore been forced to establish an Internet presence as well. A good example is amazon.com, which started as a company selling books over the

Internet, took a significant slice out of the market share of Barnes and Noble and so forced the latter company to set up an Internet site as well.

Many businesses are using the internet to conduct business between them. This type of e-commerce is known as Business to Business and it account for some 80% of the total value of all e-commerce operations. However, individuals have also been drawn to the internet for commercial reasons. For example, many individuals are using the Internet to buy directly from retailers in e-commerce. Examples include amazon.com and dell.com. The reasons for the emergence of such activity include convenience, greater choice and savings.

There's no doubt the adoption of Web technology provides a company with the opportunity to change its relationships with the organizations and individuals with which it does business--from trading partners to suppliers, from internal customers to end customers. Perhaps the greatest opportunity for change lies in the collaborative capabilities the Internet provides. The Internet supports the transition of transacting business through discrete, predictable, serial processes to a more cyclical, dynamic approach. The Internet provides a means to readily adapt technology that lets all parties work from the same system, using the same information, in a real-time environment.

Communication is integral part of businesses. Communicating status and changes regarding product-development schedules is just one way in which the Internet is changing business relationships. The Internet has given businesses the ability to increase their communication to their internal and external customers and break down perceived barriers to management. For example, business associates can receive updates from the chairman via the Internet, as well as talk directly with him through regular Web chats. Through broadcasts over the Web, we hear the message delivered at financial-analyst meetings at the same time the analysts are receiving it.

In addition, a manufacturer alerting everyone immediately of a delay and reflecting this delay on the shipment schedule in real time gives retailers, transportation companies, and importers the opportunity to take corrective measures.

The Internet also permits retailers to become more customer focused and responsive. External customers now have the power to determine when they shop, what they want to shop for, and how they want to receive the goods (by mail, by truck, or for pickup at the nearest store). At the same time, information directly collected about customers' buying habits assists retailers in tailoring product offerings and promotions to individuals.

Indeed, the Internet impacts all relationships. Easy access to timely, accurate, and targeted information by businesses and their suppliers, partners, and customers fosters relationships that are one to one rather than one to many. The personalization, communication, and functionality that are the outcome enhance and reinforce relationships in ways not possible in the past. Further implementation and extension of these principles will extend and enhance business relationships well into the future.

With the importance of computers to businesses in the world today, one wonders how they can survive without their use through a virus attack.

According to CBS.com, the first modern Internet virus supposedly caused millions, if not billions of dollars in damages. As users begin to use email to replace standard forms of communication like telephone and US mail, email becomes a prime vehicle for malware to spread. Communication is a part of every social being. Thus, the social impact of viruses is that they adversely affect the infrastructure people use to interact with one another. Another social impact related to viruses is the hysteria that they cause to society. A byproduct of this hysteria is hoaxes that are sent to people warning of dire consequences if the user opens attachment or runs files with a specific name. Many users naturally want to warn their friends and family of such electronic tragedies by sending out more email. This usually has the effect of congesting network traffic where everyone emails everyone.

Network congestion for businesses may lead to operational downtime. The rationale in business is that time is money, so downtime means the loss of money. The economic impact of either hoaxes or viruses can be detrimental to businesses across the globe. Many corporate systems communicate with each other across the Internet. If communication somehow comes to a screeching halt between these systems, money, goods, or service may not change hands. Ultimately, everyone may suffer from such electronic gridlock. Reports by ICSA.Net and Information Week portrays enormous economic impact of recent virus strikes on the US and global economy. From the report it can be deduced that the damage estimated from the "LoveLetter" virus costed as much as $10 billion whilst the damage estimated from the "Melissa" virus was $385 million. When including hard and soft dollar figures, the true cost of virus disasters was between $100,000 and $1 million per company. Furthermore viruses and computer hacking has cost U.S. businesses an estimated $266 billion. Globally, about 64% of companies are hit by at least one virus annually.(1)

The effect of computer viruses on businesses was exampled in an article in The Jamaican Observer entitled “Computer viruses hits local firms”. The article expressed how several Jamaican firms have been hit by one of the nastiest computer viruses ever to surface, and which have been creating havoc across computer networks in the USA and elsewhere. The viruses responsible were the Sobig.F and "Blaster Worm" that brought down computer systems by clogging their capacity with mass mails.

The article went on to explain that the Sobig.F virus -- aptly named because of its ability to infect computer operating systems without human intervention -- multiplies by using e-mail addresses it finds in computers it infects. According to computer experts, this virus has turned out to be the biggest mass-mailing computer program ever developed.

The other virus, Blaster Worm, began striking computers worldwide in early August. Its modus operandus was to exploit a known vulnerability in Windows XP, Windows 2000, Windows NT 4.0 and Windows Server 2003. The National Commercial Bank was one of the institutions that have been hit by the Blaster Worm version of the virus. The bank's director of transformation initiatives, Herb Phillips told the Business Observer that the worm shut down the systems at some of its branches for nearly half hour last week Tuesday, with the Kingston Street branch going down for nearly two hours. It took 24 hours, he said, to 'scrub' the bank's almost 8,000 different servers, download the patch, and rebuild a new firewall for the Kings Street branch. The viruses caused millions of dollars in losses to businesses affected.

In today’s uncertain environment, it is good advice to practice safe computing. The more practice measures you take, the safer you will be when your computer faces infection, as it almost certainly will. In order to protect your computer from infection from viruses, there are a few tips you can follow.

First, install anti-virus software on every single computer you use without exception. Anti-virus software is an absolute worthwhile investment for your computers, network and business. Without them a business is unprotected and open to many kinds of business interruptions.

Secondly, choose the anti-virus mode that scans your computer every time you turn it on, and every time you create move or copy files. The auto-run mode will catch viruses in the background; otherwise, protection will take place only when you remember to manually run the software. Many busy people may forget to manually scan their computers everyday.

Thirdly, keep your anti-virus software up to date by downloading the latest virus definition files or virus updates from your vendor. If businesses fail to update their anti-virus software frequently, they leave their network exposed to infection by any newer virus that were created or received since their last update. While many businesses update their definition files monthly, or weekly, others prefer to update their software daily. This mainly depends on the level of protection their businesses requires.

Fourthly, businesses must beware that many viruses propagate by sending copies of themselves to everyone in a user's e-mail address book. If they don't have updated anti-virus software, they could risk infecting every individual or companies on their mailing list. On the other hand, if their vendors or associates don't have, don't regularly use, or don't know how to update their anti-virus software then they can infect your business. It is necessary then, for users to talk to their friends, associates, vendors and suppliers in order to urge them to consider using updated computer virus software on every machine.

In addition, to anti-virus software, businesses will need to install personal firewalls. Firewalls are real time protection programs that can alert you instantly to any suspicious activities. They can also block that activity in real time as opposed to antivirus programs which usually scan for files that are already resident on a machine. Having both protective systems of firewalls and antivirus programs operating simultaneously is a good self protection measure especially for businesses that use the internet for long periods of time.

Also, businesses should be certain to back up all their important files often, so that they will not lose their data. Weekly or nightly backups are good safety measures. If a system in a business becomes infected by a computer virus, the business may need to delete every file, program or data base in order to clear out the computer properly. However it must be noted that a virus can store itself on a backup disk, therefore is necessary to run a virus check before backing up data or you may reinstall infected files.

In continuation, businesses which engage in e-business may find it prudent to engage in a full time, on staff security specialist. In addition, businesses should have access to, or contact with, firms that specialise in cyber security. Cyber security requires daily attention in order to keep up with and stay ahead of the threats that emerge almost daily.

In relation to e-mail viruses, users at businesses should consider deleting, unexpected or unrequested e-mail, or e-mail from someone they don't know. This is because many viruses are sent in e-mail attachments. It must be noted also, that if you receive a suspicious e-mail from someone you know, it is possible that their computer is infected with a virus.

Though many view viruses negatively, there are viruses that could be considered “good.” The Potassium Hydroxide (KOH) virus has the unique distinction of being a beneficial virus. The virus asks the user for permission to encrypt all the data on the user’s hard disk or floppy disk once infecting a machine. If the user chooses not to accept, the virus simply deletes itself. Aside from this beneficial behavior, the virus has the same infection methods as any other virus.

Currently, viruses like any other program need the intervention of a process or someone to run. Also, like any other program viruses usually contain bugs that could inactive their destructive behaviors. Viruses are limited to certain vehicles of transference like the Internet or a floppy disk. However, with improving technology, viruses can circumvent some or all of these limitations. Cellular phones, Pocket Personal Computers (PC), and other handheld devices that use wireless communication and email may become infected with a new strain. Because of the pervasiveness of technology, it encompasses much of the good -- and plenty of the bad -- of the whole wide world.