

# Security Risks You and Your Family Impose on your Companies' Computing and Networking Assets.

By: Colin S. Thomas, Network/Data Engineer  
Thomasc.ctr@mfr.usmc.mil

## Abstract

Computer and Network Security is quickly becoming Information Technology's hot occupation. After the colossal disasters of the September, 2001 terrorist attacks and the more recent natural disasters companies have looked long and hard at how to better protect their computing and networking assets from the numerous hackers, natural disasters and foreign terrorists. This includes spending more resources on hardware, upgrading software, and relearning Information Technology priorities. Unfortunately, a grand majority of the greatest minds in Information Technology Security are overlooking the one element that can stroll right up to a companies computing asset and destroy it in one or two clicks. It's you the employee, your family or family friend.

This article is designed to expose the little advertised threat to your companies computing asset. We discuss how employees that either work from home (telecommuters) or the person who just randomly checks their companies email off hours are leaving their companies crucial data unguarded and at risk of attack within the safety of their home. We will bring to focus some of the growing Information Technology Security concerns of corporations when it comes to their data in your home. We will showcase some past security incidents to bring to light various security loopholes at the employee's home. We will offer some fundamental advice to avoid damage to your companies computing assets and to keep your family safe from the dangers of the Internet.

## Introduction

In almost every article in today's computing and networking security environment, all the experts exude the same message highlighting "must-do" rituals on your company's computer and network. Lock down the network, install intrusion protection devices, keep the anti-spy ware up to date and constantly run anti-virus on all email and system environments. What these experts fail to mention in their numerous articles is the unknown cohorts of the hackers, malicious code writers and software pirates is the All-American Family and their neighbors. "We have focused on protecting your children from others in cyberspace, dangers exist to you and others as well. And these dangers may be caused by our children and their friends, inadvertently or intentionally" (Aftab, 2004). The dangers are usually not obvious to the everyday computer user and today's corporate environment fools the user into believing they are inherently safe. This entire extracurricular internet searching and downloading activity being done on your companies computing asset over a network connection kindly provided by your boss. We will discuss these concerns and prepare the computer user to take accountability of their actions before a hacker takes accountability of their computer.

## So, What is the Big Deal?

Some people may say what is such a big deal about losing some business letters and some old, stale emails to a curious hacker through an incorrectly configured insecure network connection? In the '80's and '90's computer and network security was not a priority when a lot of the crucial data corporations created was still in paper form and internet usage was medieval. This is not the case in today's market with the new computers, the popular software packages and internet service providers available. To take advantage of the growing number of customers using computers, financial institutions are making it more comfortable for their customers to download or visit their financial accounts online. As evidenced during a recent poll, "[A large] number of respondents, 86 percent, acknowledged keeping sensitive health, financial or other personal data on their home computer." (Network, 2003) This new demand of computing resources has strained the average American family. Today's average family cannot afford more than one computer per household. This creates a bottleneck for information technology. Even in this technological age, a large number of families depend on one computer for all their computing needs. An Australian Statistics firm, Nation Master lists computer ownership in the United States as 544.408 [computers] per 1,000 people, [which roughly translates into 1 computer for every 2 people] (Nation, 2005). The computer you may depend on for your work doubles as your family financial center or kids for homework assignments. The computer is quickly becoming the data depository for your all your family needs. Old pictures of family members, taxes, and personal contacts are kept on computers. These same computers are also being transformed into the home entertainment centers. Where the problem gets complicated is when the person needing the computer for a particular task doesn't have one readily available to them. A larger number of employees are bringing their computers home in the form of the lightweight laptops and using them for personal reasons.

According to Family Guide Book, half of all the people that have access to internetworking connections are doing it for official business. Many of these same people let their children and other various family members use their "official business" computers for non-official tasks i.e.: homework, online calendars, downloading music and the newest internet commodity, online movie downloads. Hackers know this changing trend and are customizing their attacks to conform to the new computer usage. "In addition to holes in security and backup programs, critical vulnerabilities in instant messaging programs, Web browsers, file sharing applications, and media players are all listed among the Top 20 [Critical Internet Security Vulnerabilities]" (Twenty, 2005). The people that play the biggest role in these sorts of attacks next to the hackers themselves are careless family members and their neighbors. The kids doing homework and quickly chatting with friends or mom looking for recipes to impress the family and discovering a sale all on your companies computing asset. People are under the assumption that since their computer is locked in their house that the computer is safe.

New age hackers take advantage of security lapses by others to creep into your secure computing home environment. A recent example is Sony's recent CD/DVD release. Sony distributed, only in the United States, a number of CD/DVDs with an embedded

copyright protection tool. In Sony's underlying attempt to contain its copyrights on music with this hidden tool it exploded a new storm of controversy. If you or your family plays a CD/DVD containing this copyright tool your company's computer becomes instantly vulnerable to outside attempts of control. "The poorly written software leaves a PC wide open to hackers, and attempts to remove it can disable the CD drive" (Orlowski, 2005). The simple act of listening to a new CD/DVD vilifies your companies efforts of paying and installing all the latest security software and hardware to protect it's data integrity.

It's 5 o'clock; do you know where you kids are browsing?

"Knowing a lot about computers doesn't always prepare you for what your kids, or their friends, will dream up next".

Author, Perry Aftab, Esquire 2004

The average American child is online for several hours a week and is usually not attended by his or her parents. The following categories are just some of the places kids "hang-out" now with their friends.

- On The Web
- Chat rooms
- Instant Messaging
- E-Mail
- Peer-to-Peer Services
- Newsgroups, Forums, and Bulletin Boards.

Unfortunately, thieves, hackers, sexual predators and software pirates are using the same places to possibly make contact with your child to bring their devious plans to life.

The father or mother is working diligently on the companies internet connection in their effort to meet a deadline. The parents get called away to help with the kids or to get dinner ready. In their hurried exit, the computer remains unguarded and unlocked. In too many cases, there was never any security installed by the company. If security software was on the computer it may have been turned off, not kept up to date, or de-activated to avoid the nuisance. "Only 11 percent of those surveyed were deemed to have securely configured systems, though 86 percent said they felt their computer is very or somewhat protected from online threats" (Aftab, 2005). In the absence of the parent, the child begins looking for his or her favorite websites and starts clicking away. A malicious code writer notices activity on the computer via a "bot" loaded earlier. He employs social engineering via an official looking pop-up alert. Your child is suddenly alerted by the fake but official looking "system alerts" pop-up window demanding immediate action. With the coincidental appearance of this warning, the child is concerned that he or she has accidentally damaged your system files. In an effort to cover up the damage to the computer, the child quickly clicks the pop-up to start the repair and by doing so, loads the virus or Trojan horse on your hard drive.

Your computer is now a recruit of the malicious code writers army of “bots” and the child, not knowing what they have just done, closes the window and continues with their search of their favorite website. You return to your computer the next day and do not know what has occurred.

One new virus that is smart enough to make its way unto your computer may be just one of the “bots” posed to launch an attack against a federal government agency, local city web site or a credit card company in another state. This targeted financial institution may have millions of peoples consumer identities electronically stashed away on a server waiting for the next billing cycle. “The [DDos- Denial-of-Service] attack is the latest example of a growing trend, says Tom Corn, a vice president at Mazu Network, a Cambridge, Massachusetts-based vendor of DoS-mitigation technologies” (Jaikumar, 2004). These hackers are out recruiting your computer by attempting to place a “Bot” on your file system. At a time of their choosing, the hacker signals the “bot” to flood the target web site with requests for information. In most cases, the web site is not designed for this unpredicted amount of traffic and is temporarily out of service.

All too common news headlines report the results of DDos attacks that several files were compromised at a financial institution and approximately how the attack occurred. It may take hours or days for the Information Technology experts to delve through the logs and corrupted files for any evidence of intrusion. The one item the news report often does not mention is the “Bot” on your company’s computer that assisted in the attack.

Then there is the teenager, home from school for the summer with nothing to do. His or her parents are at work and tell the youth to stay out of trouble. To these young people the computer is a way out of the doldrums of everyday life and the confines of the home. They can keep up with their friends, learn the latest band gossip and poke around with some file sharing software. They quickly learn the simple tools of hacking and out of their search for fun and excitement try a couple out. “The importance of tech-savvy teens being able to make such judgments has been highlighted in recent months by the arrest of a Canadian teenager known as “Mafiaboy” for February’s widely publicized distributed denial-of-service attacks, which lasted almost five days, slowed the Internet by 20% and crashed many of the world’s most popular e-commerce sites. In another incident in May, a teenager reportedly pleaded guilty in a Montreal court to illegally penetrating the computer systems of several Canadian and foreign institutions, including NASA, Harvard University and the Massachusetts Institute of Technology (Infosec, 2000). The burden of the child’s ill-driven foray on the internet will ultimately fall back on the parents. In a number of these cibercrime cases, companies will want some sort of restitution for the millions or perhaps billions lost in revenue due to the child’s poor behavior. Unfortunately, the computer used by the child may have belonged to the parent’s employer and as a result may be confiscated for evidence. This type or new online fraud and abuse by young people may leave the parents employer open to lawsuits and the parents without a job.

## Adults Contribute to the Problem

Not all problems discovered on your companies computing asset is the fault of your kid downloading the latest game or your wife uploading family digital snapshots to a distant friend. “The far greater danger lies not in Internet-passed viruses, but through sharing infected floppy disks and by running infected programs” (Aftab, 2004). Adults may remember the “Sneaker-Net” of the ‘80’s and how one would run around with a floppy disc to share small programs and client files. It still exists today but with a twist, the floppy is now the CD/DVD you borrowed from your friend to share the recent client updates or a bootleg movie. In the excitement of the exchange came a hidden extra file the previous owner retrieved from a file-sharing program. “91 percent of users have spyware on their home computers, often placed surreptitiously by file-sharing programs” (Network, 2003). Unfortunately, the co-worker didn’t mention the other files he burned on the CD/DVD like the new rogue program he discovered while searching the web. “Don’t send others the programs you’ve received in email. Often, malicious code arrives embedded in a seemingly innocuous program such as a holiday greeting”(Aftab, 2004). You were in such a hurry to finish the clients work you didn’t complete an anti-virus scan of the CD/DVD before copying the files and a new noxious virus found its way onto another file system. “Not only is using copied software against the law, the work product and consequently, a company’s competitive edge is at stake” (Kruger, 1994). Now the company may inherit a “back door” into their secured network due to the virus shared via the CD/DVD. The rogue program that was also residing on the CD/DVD is downloaded onto the remaining office computers and the chance of becoming a candidate for a software audit became more likely.

## It Adds up

During a child’s unsupervised time on their parent’s computer official email is accidentally sent or crucial client files erased. Enough damage may have occurred to set the parent 8 or more hours behind on a particular project. They may find themselves trying to explain why an email got sent to the wrong person or, worse, the wrong client. Parents may not recognize this as a crime but to the company paying this employee it is a crime and a misuse of company property. The negligence of leaving the computer unsecured the child unknowingly becomes the thief. “Fortune Magazine reports that financial losses from computer crimes run about \$10 billion per year. What’s even scarier is that more than 95 percent of them, according to FBI estimates, go undetected” (Aftab, 2004). A Large number of companies may not report the crime due to pride or the company did not have a policy in place to handle this loss to intellectual property. Companies are losing large amounts of money paying for computing resources and network bandwidth that is being used for illegitimate web browsing or file downloads. “Online piracy is when someone illegally copies and shares copyrighted materials for business or personal use. This includes when someone downloads music, movies, games, or software without the permission of the copyright owner or when you share music, movies, games, and software copies that you own” (Using, 1994). What is even more discerning is that in an effort to prevent online crimes by their employees these companies may be watching what your downloading via the provided company network

connection to your house. “If your kids pirate digital files, you could be subject to steep fines or other penalties, and this practice can expose your computer to viruses, spyware, and other unwanted software” (Teach, 2004). Giving an employee the right to take home computing assets and using company network bandwidth comes with inherent risks.

Only now are employers catching on to the problem of poor computer security and illicit usage. Due to the recent flood of liable suits and damage to company file systems companies are planning more secure networks and re-training employees. “With more and more employers being held liable for actions of their employees online (Cybertots), many employers are setting up Internet use policies to regulate their employees' Internet access. Most of those policies prohibit the use of the account by non-employees, and substantially restrict the online activities of employees” (Aftab, 2004). Companies are becoming more proactive by purchasing monitoring software and writing properly written internet usage policies into hiring documents. Upfront, companies are spending double for security technology and more for employee training. They want to know where every security loophole exists and what they need to do to close it. “Big Brother may be watching you. All but a small minority of states permit an employer to monitor electronic communications of their employees, if the employer supplied the equipment and access or the employee consented to the monitoring. (E-mail policies contained in your employee handbook may be deemed consent.) That means that they are permitted to intercept and monitor your e-mail and where you go online. (Or your kids, for that matter.) If employers discover a misuse of their Internet accounts, they may be able to discipline or fire you. So be careful” (Aftab, 2004). Employees need to understand that they need to be accountable for EVERY transaction that happens on their company’s computer and how to can ensure it is safe from illicit use.

## Options to the Employee

First, talk with your family and discover what their needs are for computing resources. When the children are done describing their needs, explain how dangerous the internet can be. Print out examples of internet crimes committed by other young people and the punishment the kids and their parents experienced and gauge their response. “In order to make kids understand how bad hacking is, they'll need to identify with the victim, since to them hacking is a victimless and faceless crime. If you try to "bring it home," showing your kids how horrible it would be if a hacker got into your computer at work and destroyed all the work you've done, or got into your home computer and destroyed their files or destroyed their favorite websites, they may be able to appreciate the seriousness of the crime” (Aftab, 2004).

Second, Several county libraries offer free computer use at various branches. If the child is old enough, they will not need your presence to use the computer. The operating systems and associated software on a number of county library systems are locked down and make it complicated for the most curious teen to circumvent. These same facilities may have some sort of monitoring to keep kids in line with internet usage policies. Ever since it was discovered that some of the 911 terrorists used libraries to assist in

communication of their plans to their cohorts, libraries have made some great strides to keep this tragedy from happening again.

Third, a number of professionals with experience with this kind of home intrusion of their computing resources will tell you “don’t let your children or other family and friends use your companies computer or their network interface”! Computers are going to be a crucial part of every life from this point forward. Spend the extra money to buy the 300 dollar computer that can be used by your children or visiting relatives. Learn to lock down the software on that computer and create separate accounts with unique passwords. Getting your family into the practice of computer security will make them realize the importance. An anonymous author on a forum discusses how he combats his grandmothers computing needs when she arrives for a visit. “So I looked on Dell Outlet, which sells preconfigured computers that have been returned and reconditioned, and found a similar computer for \$356....the fact that this computer will probably do all she needs it to do far into the foreseeable and unforeseeable future. And she is about as demanding as the average computer user; she browses the internet, checks her email, uses Word and Excel, and keeps track of finances using Quicken and TaxCut. And she plays Solitaire and Minesweeper” (“thefultonhow”, 2005). If your company supplies you with a home modem line or cable buy the extra \$19.95 monthly account from a local ISP and separate your computing resources from those of your families.

## Conclusion

We have learned what may happen should an employee misuse or become negligent with their companies computing and network assets. Listen to the experts and learn to lock down the network, install intrusion protection devices, keep the anti-spyware up to date, and constantly run anti-virus on all email and desktop environments. Then take it a step farther, discover the actions you need to take to protect you and your family from online activities that will harm your family or submit you or your company to legal action.

It is not always the fault of the employee that their computing resources are compromised. A great number of these employees are starting to get a false sense of security concerning computer cibercrime. They feel that their company “has gone the extra mile” to ensure their data integrity. Unfortunately, a large number of corporations and educational, governmental institutions are lacking even fundamental policies concerning computer use and data protection at home. Discovering what policies exist can help the employee understand what actions they can take now, what they need to plan for tomorrow and what they need to learn the day after.

Divide your working environment from your families and secure it. After sitting down with your family and discussing how the family’s commuting habits will be revised your family may be upset with you. This kind of family “outing” will be better then telling them your out of work and facing legal action to boot.

Contact your human resources representative and become part of the solution before a hacker makes you part of the problem.

Infosec Outlook Volume (June 2000, Volume 1, Issue 3)  
<[http://www.cert.org/infosec-outlook/infosec\\_1-3.html](http://www.cert.org/infosec-outlook/infosec_1-3.html)>

“Using copied software: your work product at risk” Journal Kruger, R.  
Business Software Alliance, Washington, DC, USA; (1994, September)  
<<http://ieeexplore.ieee.org>>

Aftab, Perry Esquire (2004) “The Bad Stuff Goes Both Ways . . .Protecting Others and Yourself From Your Kids and Their Friends”  
<<http://www.familyguidebook.com/book/11.html>>

Thompson, Tyler (2005, March) “VNC - Control your computer from a far.”  
<<http://www.pcmec.com/show/opensource/759/>>

Ney, Robert W. Chairman, House or Representatives (R-OH) Chairman, (Unknown Date) “Committee on House Administration”  
<[http://www.house.gov/cha/tr\\_policy.html](http://www.house.gov/cha/tr_policy.html)>

State of Virginia, Department of Human Resource Management (Revised 2005, September) <[http://www.dhrm.state.va.us/hrpolicy/policy/telecommute1\\_61.pdf](http://www.dhrm.state.va.us/hrpolicy/policy/telecommute1_61.pdf)>

“thefultonhow” anonymous (2005, November) “The Cheapest Computer is Enough”  
<<http://pcmech.com/show/kudos/859/>>

Stay Safe Online and Get Wise Organization (2003) “A Young Person’s Contract”  
<<http://www.staysafeonline.info/basics/family.html>>

Jaikumar Vijayan, Computerworld (2004, September) “Hackers Hit Credit Card Company”  
<<http://www.pcworld.com/news/article/0,aid,117897,00.asp>>

“Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus” (2005, November) Copyright (C) 2005, SANS Institute  
<<http://www.sans.org/top20/>>

Erik Larkin, PC World (2005, November) “A New 'Malicious Marketplace' for Internet Attacks”  
<<http://www.pcworld.com/news/article/0,aid,123651,00.asp#>>

Network World Fusion Staff (2003, June) “Report: Broadband Customers Not Playing It Safe”  
<<http://www.pcworld.com/news/article/0,aid,111056,00.asp>>

Andrew Orlowski, (2005, November) “Sony unsinged by rootkit CD fiasco”<<http://www.theregister.co.uk/2005/11/22/analysis/>>

Nation Master, (2005) Australia  
<<http://www.nationmaster.com/country/us/Media>>

Gerhard Eschelbeck, CTO & Vice President of Engineering, Qualys (2005)  
< <http://www.qualys.com/company/management/>>

“Teach your kids not to illegally download or share movies, music, and software” (2004, December) <<http://www.microsoft.com/nz/athome/security/children/kidspiracy.mspx>>