INFORMATION SECURITY – WHOSE RESPONSIBILITY IS IT?

by

Guillermo L. Ortiz-Caceres

A Graduate Term Paper Submitted to Dr. Philip Lunsford, DTEC 6865
College of Technology and Computer Science
in Partial Fulfillment of the Requirements of the
Degree of Master in Science in Industrial Technology
Computer Networking Management

East Carolina University
Greenville, North Carolina
November 2006

ABSTRACT

Consumers of the global service we call the "Internet" are largely illiterate in the area of information security. The new order of global economy, open access to the Internet and a growing number of terrorist activities leaves us all open to a new kind of threat. The threat increases as more consumers gain access to the Internet and the number of radical groups with network security knowledge continues to grow.

Consumer reactions to the gamut of activities that ranges from the invasion of privacy to information espionage has resulted in the passing of thousands of legislative laws which have been largely ineffective in deterring those who know how to get around security controls and cause harm.

Information security breaches come in the forms of passive and intrusive attacks. The author establishes to what degree consumers are responsible for the protection of their own information as opposed to the entities that have been established to provide secure services across the Internet. The author shows that protection can only be accomplished through the education of information security managers on existing testing procedures that comply with establish laws combined *with* the education of consumers on security practices that mitigate the accidental release, or intentional breach, of restricted information. The target population of this paper is information security undergraduate students and graduate students.

INTRODUCTION

Consumers and organization worldwide of all sizes today have taken advantage of the proliferation of information sharing which has become an integral part of our society. Optimizing speed and access to information is just one common goal that organizations in both the public and private sector strive to accomplish. (Cho, 2003) Computer and network illiteracy is increasingly becoming a non-tolerable deficiency in our society. As our society becomes more dependent on the internet people are finding it harder to do without the internet. Worldwide organizations have to deal with computer illiteracy in underdeveloped nations which are struggling to become advance countries. (NPR, 2002). Baby boomer and pre-baby-boomer consumers in our society have been unwillingly or unknowingly thrust into the world of technological advancements with little or no preparation. As an example, millions of Americans are now expected to get most of their Medicare problems and questions answered on the internet through WebMD or MedicareINteractive.org. Medicare recipients are often the poor and elderly who have little, if any, knowledge of the internet and 76 percent of the seniors questioned by the Kaiser Family Foundation/Harvard School of Public Health survey said they had never been online. (ABC World News, 2005)

Because of this, it has become increasingly important for consumers, organizations and the information technology specialist to share responsibility in protecting information as well as the resources that facilitate the information exchange. It is particularly important when considering the sharing of information within government and military agencies that have to deal with the increase threat of internet crimes and terrorism. (Maney, 2004)

However, the author is in the opinion that the public consumer is at greater risk than large organizations and government agencies since they lack the knowledge and skills to adequately protect the dissemination of personal information across the internet. Personal information is the target of criminals seeking to steal a person's identity and relies heavily on the victims' social security numbers, financial institution account numbers, driver's license numbers, property deeds and medical history.

As computers become more common in consumers' homes and small businesses incidents of information security related breaches has grown proportionally. The United States alone has over 164,000,000 personal computers. (Aneki.com, 2006) Four-fifths of all home computers lack one or more core protections against virus, hacker and spyware threats and an eighth of identity thefts use information obtained directly from users over the Internet. (LaRose, Rifon, & Embody, 2006) Where once only large corporate environments were susceptible to attacks, individuals and small business networks are increasingly being targeted. However, most security breaches are caused by the computer users themselves.

Of all the security vulnerabilities that can be listed, large corporation and small business employees may be the most difficult problem to manage. Information technicians can set up firewalls and establish perfect intrusion detection protocols, but when trusted employees do something they should not, either accidentally or unknowingly, many information technology security controls become irrelevant. (Swartz, 2006)

Home computer owners are also plagued by the lack of knowledge on how to adequately set up bundled antivirus, anti-spyware and firewall software that come with their computers. More often that not, they allow the software registration to expire past the initial introductory period assuming that the software is still functional with the latest upgrades. Others take a step further in purchasing small office home office (SOHO) routers and wireless routers without really understanding that they can increase their vulnerability to attacks as a result of their actions. They rush in setting up their wireless home networks to get their Internet connectivity working as quickly as possible. Most local area network wireless products today come right out of the box without security measures enabled. Configuring security features is at best a slow process because it is non-intuitive. (Mitchell, 2006)

CORPORATE AND SOHO VULNERABILITIES

Wireless local area networks (WLANs) are rapidly becoming the perceived panacea to reduce cost in corporate and SOHO networks because they created a new level of productivity and

freedom both within and outside the organization. Many wireless applications have surfaced over the years to facilitate business operations in the form of inventory tracking, mobile printing, and point-of-sale terminals. Administrative functions which facilitate front office operations such as e-mail, Internet access, and voice over IP have become so crucial that without them a corporation could be crippled. (Haase, 2002) However, these applications bring with them new challenges to security. While securing hardwired LAN and WLAN mediums in themselves is something that IT technicians are quite familiar with there is yet another threat that quite often surprises IT technicians. Employees that have the need to take work home and bring it back to the office environment are increasingly becoming the newest of threat in a corporation. Traditional security boundaries are being diminished by remote-access and virtual private network users connecting from homes and public locations while outsourced information services contractors often need physical access to the internal network to accomplish their work. Rogue access points and transient storage devices, such as universal serial bus (USB) flash drives (UFD), are yet another threat to secured hardwired LANs.

A rogue access point is a wireless router that an employee has brought to the office without specific authorization from the corporation. These store-bought, low cost devices often don't conform to corporate WLAN security policies. They enable an open, insecure interface to the corporate network because they are behind the firewall and are not detectable by traditional intrusion detection or prevention systems. Anyone within the signal range could access the corporate network if no other security measures are implemented.

UFDs with high memory capacities up to 4GB bring new challenges for corporate IT environments concerned with data-access security. Every computer manufactured today comes with USB ports. The ports pose threats to the corporate environment ranging from information theft or data lost in the public domain because of the user's information security ignorance or negligence. For the most secure IT environments, this means the IT department will have to block all the physical ports which employees have access to and unwittingly encouraging employees to find other ways to move data over other mediums which are not authorized and on well controlled networks.

> "Complicating this situation is the new reality of mobile workers requiring access to the network while on and off premises. Employees regularly use their homes, hotels, airports, and other wireless hotspots to conduct business. These

> ‘unmanaged’ sites can act as a conduit for threats to the corporate network-laptops risk contracting viruses, spyware, and malware. Wireless clients can exacerbate the problem by connecting to wireless access points or other wireless clients without the user's knowledge.” (Cisco, 2006)

CORPORATE AND SOHO RECOMMENDATIONS

Educating the employee on network security is a key point in preventing security breeches. In a recent survey 574 IT professionals attributed 60 percent of their company’s 2005 security breaches to human error, 20 percent to technical malfunctions, and the remainder to a combination of the two. Of the companies surveyed 84 percent with security awareness programs credit it with reducing breaches. Yet only one-third of companies have security training programs. While 11 percent plan to implement one soon, one-third of companies have no plans to implement such training at all. (Schwartz, 2006).

Security program must focus on the human element as much as technical advancements. Many security awareness training programs are inadequate with typical training sessions detailing only on how to use e-mail, passwords, and Internet browsers safety. In 11 percent of companies, training session runs less than 30 minutes, and at 36 percent of companies, less than an hour.

The Cisco Network Admission Control (NAC) solution provides a powerful answer to today’s security challenges. Cisco NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access the network. Access is permitted only to compliant and trusted endpoint devices, which can include PCs, servers, IP phones, and printers. Cisco NAC can deny access to noncompliant devices or redirect them to a quarantine and remediation area. (Cisco, 2006)

One of the initiatives currently being developed by Institute of Electrical and Electronics Engineers (IEEE) to deal with UFD endpoint devices brought into the workplace by employees is a new standard, the IEEE P1667 "Standard Protocol for Authentication in Host Attachments of Transient Storage Devices". The standard defines methods for authenticating transient storage devices when they are connected to host computers in corporate, government, academic and other environments. The IEEE is an organization composed of engineers, scientists, and

students. IEEE is best known for developing standards for the computer and electronics industry. (Happich, 2005).

The standard would allow bi-directional authentication of UFDs and relies the operating system to authenticate the UFD when it is plugged into the corporate computer so the system can authenticate it according to the IT security policy and thereby mitigating immediate port shut down. The newest UFDs would incorporate U3 LLC, a joint venture that is backed by SanDisk and M-Systems. U3 is responsible for the development of a proprietary application design specification created for Microsoft Windows operating systems so that applications can be executed directly from a specially formatted USB flash drive. Applications are allowed to write files or registry information to the host computer, but this information must be removed when the flash drive is ejected. (Wikipedia, 2006)

UFDs termed as "U3 smart drives" differ from traditional USB flash drives because they come preinstalled with the U3 Launchpad which emulates the Windows OS start menu and controls program installation. The main difference between current UFDs and a U3-enabled UFS drives is a unique hard-encoded serial identification number, which, in combination with firmware, enables software vendors to license a special-purpose-made version of their products for use on U3-enabled storage devices. This would allow network security policies to force the drive into compliance before being allowed access to the network.

HOME COMPUTER USER RECOMMENDATIONS

The average computer user needs to be able to understand the importance Internet security and often a simpler explanation of what needs to be done goes further in getting security controls implemented.

Fifteen years ago, firewalls were something that the average consumer had a hard time understanding. They were complicated, expensive, and primarily utilized at corporate network perimeters. As technology improved and prices fell, these devices were made available to the consumers. The news media played an important role in disseminating the alarming rate at which successful computer hacks and attacks on corporate and government computers were increasing. Popular press accounts of online safety problems harped on the fear factor to promote personal responsibility in Internet security. These were often accompanied by hard luck

stories and warnings that it can happen to us. Since the threats posed by online hazards like spyware are still unknown to many Internet users, simply making them more aware of the danger is an appealing strategy to get the message out. Among students enrolled in business and computer science courses, awareness of the dangers of spyware was a factor in changing risky behavior and to take protective measures. (LaRose, Rifon, & Embody, 2006) Consumer concerns increased dramatically with the introduction of broadband Internet access, cable modems and most recently wireless-fidelity (Wi-Fi) which is best known as wireless networks. With the increase of security concerns, more and more computer network and computer security experts are recommending layered security.

Applying a good layered security system helps protects the consumer from the threats of Internet access. This method allows successive layers of security to cover security weakness developed in preceding layers or if they are configured incorrectly. This layering method for computer security protection will also lessen the criticality of selecting the best of each layer. The following layers provide the best approach to a good layered system

Layer 1, Antivirus Software

Most computers today come with some sort of free trial version of popular antivirus software. The problem lies when the trial versions are allowed to expire and the user fails to purchase the software. Having properly configured and updated antivirus software is the ultimate consumer responsibility. Without it the user can expect nothing in the form of security beyond the trial period. This is equivalent to leaving the key to your front door under the entrance floor mat.

Some antivirus software programs are free but they have limited configuration capabilities and the author recommends purchasing the full version. Software that has been certified by organizations such as the International Computer Security Association Labs, which is a security industry authority for setting standards for information security products, provide the consumer an added measure of authenticity. A list of the most popular software companies are listed in the links section of this paper.

Layer 2, Select a router with firewall or personal firewall software.

Today a consumer can purchase routers and firewalls software that closely emulates corporate routers with reflex access control lists, but doesn't require a certification to understand. While properly configuring firewall and consumer routers is not intuitive, vendors provide

sufficient costumer service support to ensure proper configuration. However, consumer purchased firewall software is often sold with many of the firewall featured turned off by default. A hacker could still gain access to the computer if not properly configured. Control of inbound and outbound traffic on the firewall software acts much like a gate guard controls access to and out of a property based on a set of access rules. Firewall software allows the user to decide which computers on a home network can have access to resources such as a shared printer. In a home router, the software can also be set to shut off ports thereby denying internet access to a user, such a minor in the home, during specified dates and times. Other settings act like reflex access control lists, allowing a port to open only when the user initiates the session or connection.

Firewall router users still have the responsibility to ensure the firmware is up to date and must make a conscientious decision to make this happen.

Layered 3. Update your operating system and applications

With all of the new security holes and vulnerabilities that continue to be found, users must update their operating system, no matter who the vendor. This also applies to their applications, including their browser. This process is relatively easy since most operating systems today allow them to set options so the browser or operating system updates itself periodically. Again, the user must be cognitive of the features available in the options or setting pull down menus available.

IT professional profess periodic updates of system software. They recommend that if the user accesses the Internet occasionally (one hour per day or less), they should update their antivirus software weekly. If they use the Internet daily (one hour per day), they recommend updating antivirus software daily. Even more aggressively, if they use the Internet extensively (more than one hour per day), or are involved with computer security, updating antivirus software should be done hourly. This aggressive approach can be made easier it the software allows changing its settings to real-time scans of all files. (Willert, 2001) While performance can be degrade when automatic options are turned on it is worth the tradeoff compared to losing, deleting, or corrupting data and having to take time to rebuild a system and make it functional again.

Layered 4. Constant education to keep skills and knowledge inline with the newest threats.

The best way for users who are illiterate in computers is to take classes available to them in their local community colleges or on-line training sessions such as those available at Microsoft.com. Unwary Internet users continue to be a threat to the network we all share, attracting spam, phishing and spyware. Improvements in technical and legal solutions are still not perfect. The huge increase in anti-spam and personal information filtering software along with the CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) attest to the public's reaction to the increase in privacy invasion attacks we are all now too familiar with. The CAM-SPAM Act of 2003 establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. These measures drive hackers to more insidious deceptions, even as vigilance is eroded by continuing waves of spam. With so many online threats perpetuated by the every day actions of Internet users, it is only logical that Internet users must assume more responsibility for protecting themselves online. (LaRose, Rifon, & Embody, 2006)

CONCLUSION

There will always be new threats to safe Internet use and corporate network security. Being aware of the threats should always be the first step in establishing a sound security policy. The more defenses, both in educational and technical advancement, we can place between would-be hackers and ourselves the more likely hackers will fail at their attempts. Layered defense works both at the corporate and home office level. Consumers are just as responsible for the protection of their own information as are the entities that have been established to provide secure services across the Internet. Internet and corporate network security can only be accomplished through the education of information security managers on existing testing procedures that comply with establish laws combined and the education of

consumers on security practices to mitigate the accidental release, or intentional breach, of restricted information.

LINKS

Norton Antivirus	<http://www.symantec.com>
McAfee VirusScan	<http://www.mcafee.com/us/>
Panda Antivirus Platinum	<http://www.pandasoftware.com>
Trend Micro PC-cillin	<http://www.antivirus.com>
Norman Virus Control	<http://www.norman.com>
F-Secure Antivirus	<http://www.f-secure.com>
Sophos Antivirus	<http://www.sophos.com>
AVG Antivirus	<http://www.grisoft.com>
Computer Associates Inoculate IT	<http://www.ca.com>
ICSA Labs	<http://www.icsalabs.com/icsa/icsahome.php>

REFERENCES

ABC World News. (Nov 2005). *Elderly Confused by Medicare Prescription Plan.* Retrieved October 2, 2006 from <http://abcnews.go.com/WNT/Health/story?id=1306814>

Aneki.com (2006). *Countries with the Most Computers.* Retrieved November 26, 2006 from <http://www.aneki.com/computers.html>

* Cho, M. (2003) *Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer.* Retrieved November 28, 2006 from <http://www.sans.org/reading_room/whitepapers/assurance/>

* Cisco Systems. (2006). *White Paper. Five Steps to Securing Your Wireless LAN and Preventing Wireless Threats.* <www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking_solutions_white_paper0900aecd8042e23b.shtml>

* Cisco Systems. (2006). *White Paper. Cisco Network Admission Control (NAC) Solution Addresses Today's Security Challenge.*

* Haase, J. (2002) *Building an Information Assurance Framework for a Small Defense Agency.*

Retrieved November 28, 2006 from <http://www.sans.org/reading_room/whitepapers/assurance/>

Happich, J. (2005). *Turn Any PC Into Your Trusted Workstation*. Retrieved October 9, 2006 from <http://www.epn-online.com/page/28649/turn-any-pc-into-your-trusted-workstation.html>

* Kadel, L. (2004). *Designing and Implementing An Effective Information Security Program: Protecting The Data Assets Of Individuals, Small And Large Businesses*. Retrieved September 29, 2006 from <http://www.sans.org/reading_room/whitepapers/hsoffice/1398.php>

* LaRose, R., Rifon, N., & Enbody, R. (2006). *Promoting Personal Responsibility for Internet Safety.* Retrieved November 2, 2006 from http://www.msu.edu/~isafety/papers/PromotingresponsibilityCACM.htm

* Maney, C. (2004) *Security Issues When Data Traverses Information Domains: Do Guards Effectively Address the Problem?* Retrieved September 16, 2006 from <http://www.sans.org/reading_room/whitepapers/assurance/>

Mitchell, B (2006). *Top 9 Tips for Wireless Home Network Security*. Retrieved October 28, 2006 from http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm

National Public Radio. (2002). *Arab Computer Illiteracy.* Retrieved September 15, April 2006 from <http://www.npr.org/templates/story/story.php?storyId=1146661>

Schwartz, M (2006). *Employees Cause Most Security Breaches, Yet Response Lags.* Retrieved October 9, 2006 from <http://www.esj.com/security/article.aspx?EditorialsID=1769>

Senior Citizens League. (Nov 2005) *Many Seniors Will Spend Far More Than Necessary On Part D Plans*. Retrieved September 20, 2006 from <http://www.tscl.org/NewContent/102560.asp>

* Willert, J. (2001) *Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters.* Retrieved September 15, April 2006 from <http://www.sans.org/reading_room/whitepapers/hsoffice/>

Wikipedia (2006). *U3*. Retrieved November 24, 2006 from http://en.wikipedia.org/wiki/U3