Global Information Assurance Certification Paper

Defending your Company from Home
By Marcial Antigua III
GSEC Practical v1.3

Introduction

The use of broadband Internet connections, like DSL and cable modems, for telecommuters and home office workers is gaining popularity in the business community. Telecommuting over broadband, however, brings about security issues and risks that both companies and employees must be aware. Vulnerabilities in home-based computers and threats coming from their high-speed and always-on Internet connections expose both the end user and company to tremendous security risks. This is forcing companies to re-evaluate the security of their IT infrastructure, systems and practices.

"Work-at-Home" computers need to be protected with a complete solution that involves the use of remote client firewalls and file-store encryption as well as the observance of secure home computing practices.

This paper presents the vulnerabilities of telecommuters and their home-based systems, their exposure to increasing Internet security threats, then discusses defensive solutions and home computing practices that companies and telecommuters can take to protect their enterprise network and systems.

Growth of Telecommuting

The number of people working remotely from a corporate office is becoming more prolific as advances in technology make telecommuting increasingly feasible. There are numerous research efforts that clearly illustrate that telecommuting is becoming a widely accepted practice within US businesses today.

According to a survey conducted by Cahners In-Stat Group (www.instat.com), a high-tech market research firm, in just the one-year period from 2000 to 2001, the number of employees that telecommute increased from 19 million to 32 million.

Other research organizations have conducted similar surveys that support this trend; People working from remote locations, whether from home or small office, are becoming commonplace and their numbers are increasing.

There are numerous reasons for telecommuting, most presenting a win-win situation for both the company and the employee. Companies are now realizing the benefits of this type of work arrangement. Salespeople, executives and home-office workers are more productive. They can work any time of the day or night. Teams can easily collaborate on evenings, weekends and holidays. This also allows part-time employees the added flexibility to work any time of the day or any day of the week. Job satisfaction levels in

these work arrangements or schedules become higher, which translates into more efficient and productive employees. Ultimately, this contributes to a company's bottom line as efficiencies in human resources are maximized.

Telecommuting Over Broadband Internet Connections

In the past, dial-up access was the only widely available and viable method to support a telecommuting workforce. These were implemented via dedicated and proprietary remote access devices accessible over plain old telephone systems (POTS). The challenges with this connection were slow data transfer speed, poor reliability in maintaining a persistent connection, and high communication costs.

More recently, significant advances in network connectivity over the Internet made telecommuting easy to implement and affordable. Of the 32 million telecommuters in 2001 indicated in the Cahners In-Stat survey, 70% have access to the Internet. This allowed more and more companies to provide telecommuting as a viable option for their workers. The Internet is becoming, if not already, the de facto standard for connecting telecommuters to the corporate network. Some factors that support this are:

- **Increasing availability of broadband Internet access services** - Estimates from Telechoice place the number of broadband subscribers to 5.7 million and is expected to rise to 14.5 million in 2003. The acceptance of this type of connection either via DSL or cable modems is quickly replacing dial-up as the primary method for remotely accessing the corporate network over the Internet. According to Cahners In-Stat Group, "No other broadband Internet-access technology comes close to cable modems and DSL in public acceptance" (Kirstein, Mark; et al., p.10).

- **Rising computer and Internet skill levels of end users** – More people are becoming more proficient in using the Internet, and the number of users is growing everyday. According to a study conducted by Cahners In-Stat Group, "of the 101 million households in the United States, roughly 52% were accessing the Internet from home by midyear 2000" (Kirstein, Mark; et al., p.13).

- **Acceptance of the Internet as a viable medium to conduct business** – The number of people embracing the Internet as a means for commerce and business is increasing daily. This is due to Internet accessibility from any location, convenience of using the Internet at any time, and reduced costs to both the end-user and business provider.

Vulnerabilities of Telecommuting Over Broadband Internet Connections

Unfortunately, as more and more businesses exploit and maximize the benefits of broadband Internet access technologies such as DSL and cable modems to support home-based workers, securing and defending these home-based systems begin to pose huge challenges for IT organizations. As the workforce fragments to their individual home office locations, the traditional network perimeter virtually disappears. Corporate IT departments now have to expand their security focus beyond the company's physical boundaries as "work-at-home" computers represent more "back doors" to the corporate network. The defensive perimeter now includes hundreds, or even thousands, of home-based computers connected to the Internet through broadband connections from a variety of ISPs. The vulnerabilities and security issues associated with this are as follows:

- **Always-on and always-connected access** - As a nice benefit of broadband, users can leave Internet connections constantly open throughout the day or night. This mimics the type of service available to office-bound workers. Unfortunately, this practice also provides hackers more opportunities to scan for system vulnerabilities and, once breached, use those for their malicious intentions at any time. Hackers can seize control of a number of these systems without the owners ever noticing for use in spoofing or distributed denial of service attacks (DDoS).

- **High-speed access** - Typical broadband speeds range from 384 kbps to 1 Mbps. With this much bandwidth, large amounts of data can be transmitted to and received from a variety of hosts over the Internet in a very short period of time. Hackers can use this to their advantage by being able to conduct their exploits quickly whether they are scanning for information or sending malicious programs.

- **Constant IP address** - With an always-on connection, a work-at-home computer may be continually using the same IP address for several days or weeks. This makes it easier for a hacker to acquire key information about the target computer to come up with a complete profile or identity, and then use these to conduct a directed attack.

- **Unmanaged and poorly secured computers and networks** - Typically, corporate IT groups relegate the responsibility for securing home computers to the end user. Work-at-home computers will not have the appropriate and sufficient security configurations. These systems will either not have the latest security patches applied or not have the necessary security software installed. To complicate matters, home networks are gaining popularity, allowing multiple computers for different members of a household to share a single Internet connection. According to an In-Stat/MDR survey, there has been a strong demand for broadband sharing devices designed for small or home networks. Linksys and NetGear are just two vendors with over 2 million cable/DSL routers shipped in 2001.

- **Unapproved software** – In addition to the standard business software and applications used by telecommuters, additional "unapproved" software are becoming more widespread as part of their arsenal of tools. These unapproved software can be file-sharing programs like Gnutella, Morpheus, Kazaa, as well as instant messaging applications from AOL and Yahoo!. Though efficient and helpful, these communication tools have known vulnerabilities that open up a number of security and privacy issues. The messages and files are mostly transmitted in unencrypted format and can be viewed or intercepted by almost anyone along the way. When using these tools for business purposes, they present risks of exposing confidential and private information to unsavory individuals on the Internet.

- **Non-secure computing practices** - Though more end users are better educated about the uses and benefits of the Internet, a huge gap remains when it comes to security and privacy. The typical end-user lacks the knowledge and awareness to protect his home computer and conduct a security-conscious behavior while connected online. They do not follow secure practices especially in relation to user accounts and password. Users easily fall victim to social engineering tactics leaving them and their home-based computers susceptible to attacks over the Internet. Examples are hoax email messages that carry dangerous payloads or Trojans.

Threats and Attacks Against Telecommuters

These home-based computers, in combination with their broadband Internet connections, pose significant security risks to a company's enterprise network. Since they can be considered as extensions of the corporate LAN/WAN, their exposure to threats and intrusions on the Internet are ultimately passed on to the corporate body.

A number of incidents have been reported and publicly disclosed in recent years that highlight the susceptibility of companies to security intrusions by way of work-at-home computers. No less than Microsoft has been attacked in this manner back in October 2000. Reports from various online and print sources indicate that the attack involved the use of malicious software from a worker's home computer.

Work-at-home computers with broadband Internet connections are especially prone to the following types of exploits and attacks:

Used as Zombies for Distributed Attacks

Zombies are unwitting computers on the Internet that have been compromised or hijacked to conduct attacks against other computers. Computer owners are unaware that their machines have been turned into zombies. Hackers typically form zombie computers into groups for a simultaneous and concerted assault on their intended targets. Poorly configured and unsecured work-at-home computers can easily be turned into zombies and used to launch distributed denial of service attacks (DDoS) or to scan other computers on

the Internet. In a recent article from BusinessWeek Online, security experts estimate that a significant number of zombie computers are home-based with broadband connections. This can cause public embarrassment for companies with the costs of losing credibility from their clients and any potential revenues. This can also have legal implications where companies may be held liable for any attacks originating from zombie systems connected anywhere on their corporate network.

Unauthorized Connections from Backdoors and Trojans

Backdoors are holes in operating systems intentionally created for legitimate purposes such as troubleshooting or maintenance; or unintentionally created as consequences of flaws in development or unknown programming errors. Backdoors also take the form of remote control programs covertly installed on computers that allow hackers to access affected systems with full administrative privileges. Backdoors render systems open to practically any type of nefarious activity and, unless detected, leave these systems open for repeated intrusions over extended periods of time.

Backdoor programs such as Back Orifice, SubSeven and NetBus grant successful intruders a lot of control over the breached systems. These programs permit the remote execution of programs, redirection of applications, logging of keystrokes, retrieval of cached passwords and editing of registry entries. They are usually distributed and installed on machines of unsuspecting individuals via Trojans, programs that appear harmless and useful but actually conceal other malicious software.

Backdoors have huge security implications for companies, especially in the financial and technology sectors. Security breaches in work-at-home computers could eventually lead to intrusions on highly sensitive corporate servers. This can result in the exposure of confidential and proprietary data, leaking of financial information, theft of user accounts and passwords, and vandalism. Losses of significant monetary value can be associated with all of these.

Infection and Replication of Worms

A worm is a malicious program designed to replicate itself automatically without any human intervention over computer networks. It copies itself on one computer and attempts to infect as many others as it can.

An example of this, reported in a Computerworld article (www.computerworld.com), is the worm called W32.Aphex@mm or W32.Aplore@mm, discovered in April 2002. Once computers are infected, this mass-mailing worm replicates itself by sending email messages from addresses obtained from Microsoft Outlook, by sending instant messages via AOL Instant Messenger or by connecting to an Internet Relay Chat (IRC) channel. Unlike previous worms, it does not carry a dangerous payload other than to replicate itself.

Another recent one, discussed in a number of articles in a TechTarget security site (http://searchsecurity.techtarget.com), is the Klez worm, which has reappeared in a number of variants since January 2002. In its latest form, it replicates itself by attaching to email messages sent to addresses gathered from the infected computer as well as by spreading over shared drives between computers on a network. As part of the email, it can also attach a file picked up from the infected computer potentially leaking confidential or sensitive information to other victims. It will also try to deactivate anti-virus programs and delete related virus signature files.

Though these examples of worms are not completely destructive to the infected computer, their impact to any company as a whole is still significant especially if hundreds or thousands of machines are affected. These worms can disrupt normal business operations by tying up precious bandwidth as it replicates itself across the entire network and by using up limited personnel resources as clean up and inoculation efforts are undertaken.

Defensive Solutions for Work-at-Home Computers

Traditionally, companies implement and use security solutions for their internal local and wide-area networks. Enterprise-class firewalls, intrusion-detection systems, anti-virus programs, and authentication mechanisms are now considered standard business software for most companies and have been deployed within the corporate perimeter to protect web servers, routers, switches, file servers and client computers. Usually, these are all part of an enterprise or corporate security strategy, which, for the most part, only cover company locations, buildings and offices.

In addition to these security solutions that are widely installed and in use today, there are additional measures that need to be implemented to address the specific security needs of work-at-home computers. A complete security solution for these systems is a combination of the following:

- Remote Client Firewalls to Protect Systems
- File-Store Encryption to Protect Data and Information
- Secure Home Computing Practices

These are described in detail below.

Remote Client Firewalls

It is important that users know and control what is coming in and going out of their systems, as well as with what computers and hosts out on the Internet they are connecting. Work-at-home computers need to be protected against unauthorized inbound and outbound connections and movement of data to and from the Internet. The use

ingress and egress filtering techniques will allow only packets with legal source and target addresses to move in and out of these systems. Most companies already practice this in the form of enterprise firewalls for office-bound computers. However, instead of relying solely on a single centralized firewall, companies can easily expand their defense perimeters via remote client firewalls for work-at-home systems. These types of firewalls protect home-based computers and networks from uninvited Internet traffic especially during periods when they are not connected to the corporate network.

In a study conducted by Cahners In-Stat Group, about 50% of over 1,000 households surveyed with broadband access do not have any form of protection like a software or hardware firewall. The group believes that intrusion protection will be a required component for any home-based system as more and more users embrace broadband access and as they become better informed about the associated Internet security risks with this type of connection. The Gartner Group also supports the use of client firewalls and states that they are necessary components for a secure computing environment for companies that employ telecommuters.

Remote client firewalls for work-at-home computers can be categorized as follows:

- **Personal Firewalls** - These are software-based products, which are widely available as free downloads for personal use. They are easy to install and use since they are typically configured with wizards or context-sensitive online help features. Examples of this are ZoneAlarm v2.6.362 from Zone Labs Inc. (www.zonelabs.com) and Tiny Personal Firewall from Tiny Software Inc. (www.tinysoftware.com).

- **Embedded Firewalls** - These are software-based products integrated with the operating system, anti-virus packages or VPN client software. An example of a firewall integrated with anti-virus is Norton Internet Security 2002 from Symantec Corporation (www.symantec.com). For a firewall integrated with VPN client software, an example is the Cisco VPN Client starting with version 3.5 (www.cisco.com).

- **Firewall Appliances** - These are dedicated hardware devices with preinstalled operating system and firewall software. Their models are specifically designed for small and home office environments, supporting 10 or fewer computers. Examples of these are available from Cisco Systems (www.cisco.com), NetScreen Technologies (www.netscreen.com), Sonicwall (www.sonicwall.com) and Watchguard Technologies (www.watchguard.com).

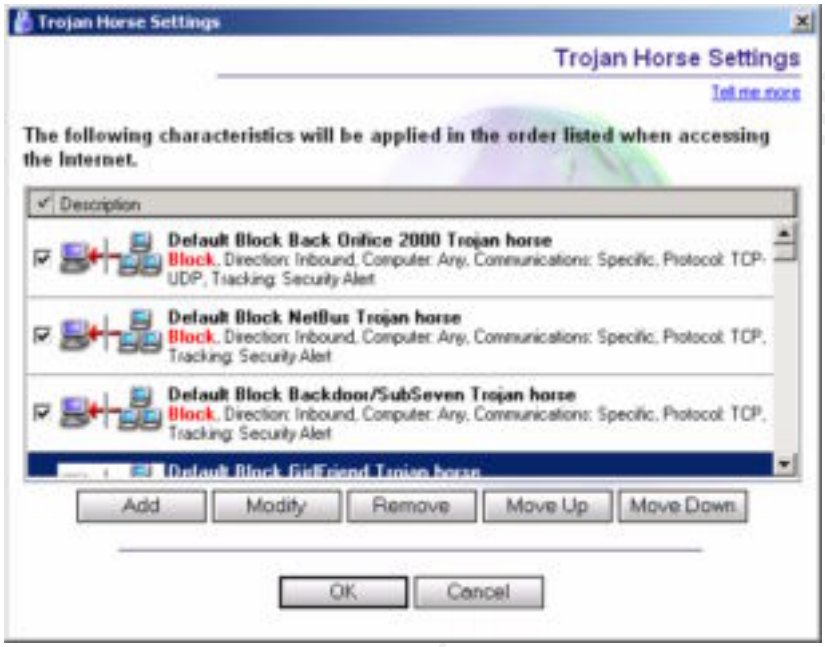
Most of the popular firewall products perform stateful packet inspection and repel common attacks like SYN, ICMP floods and port scans. The firewall appliances will have throughputs between 10 Mbits/sec to 200 Mbits/sec and provide front-end GUIs for administration.

Some of the advanced firewall features provide remote or central management, proxy capability for HTTP, SMTP, FTP and Telnet, integrated network address translation (NAT), privacy controls, blocking of active content (such as executable e-mail attachments), and malicious-code-scanning software.

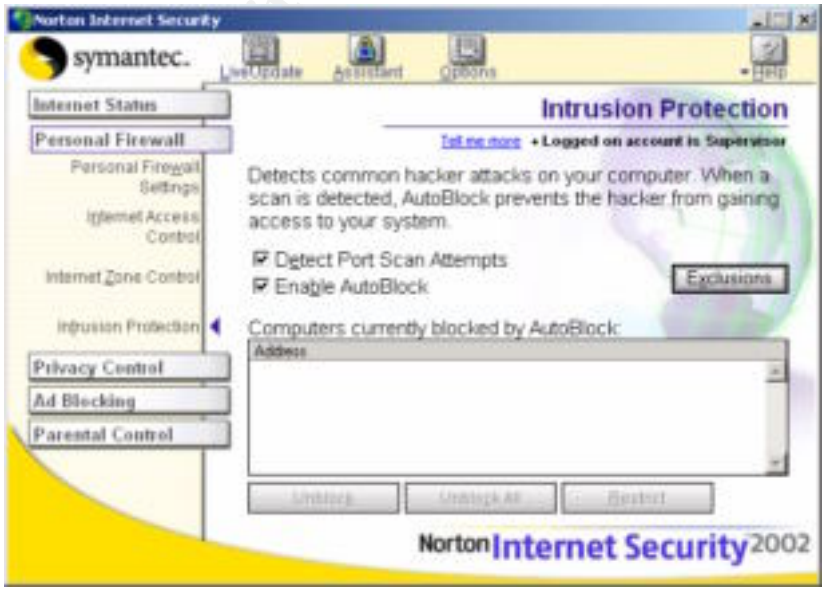
Below are some feature highlights from a popular firewall product, Norton Internet Security 2002 (NIS):

- NIS automatically blocks all file and print sharing capability on Windows computers upon installation. The figure below illustrates how computers that need to share files and other services, like in a home network, need to be explicitly defined via the Internet Zone Control section. Trusted computers have full access just as if NIS is not installed. Restricted computers, also definable especially for identified attack sources, have no access whatsoever. This allows the user to be selective in authorizing systems to communicate with while keeping unauthorized ones on the Internet from gaining access to any of these services.

- NIS comes with a number of built-in rules. The following figure shows how an important set of rules block and protect against Trojan horse or back door programs. These are kept current via updates using the LiveUpdate feature. NIS ensures that malicious programs do not communicate through the Internet connection.



- NIS has the ability to detect and protect against intrusions. It monitors Internet traffic patterns that indicate port scanning activity or connection attempts from Trojan or Backdoor programs. Upon detection, NIS automatically blocks all communication from the attacking source.



- NIS provides automatic rule configuration. As new applications are executed and recognized by NIS as low-risk, new rules can automatically be created. This assists users in configuring their firewall to allow authorized applications to pass.

File-Store Encryption

Telecommuting brings about widespread distribution and storage of company-related data on work-at-home computers. These can be sensitive files containing financial or confidential information, medical records governed by privacy regulations, business plans affecting multimillion-dollar decisions and proprietary technical designs for future product offerings. These are all very important and valuable corporate assets that need to be protected against exposure to outsiders, industrial espionage and theft. These are best secured by using file-store encryption while they are stored in local disks of work-at-home computers. For Microsoft Windows systems, file-store encryption can be implemented by either of the following methods:

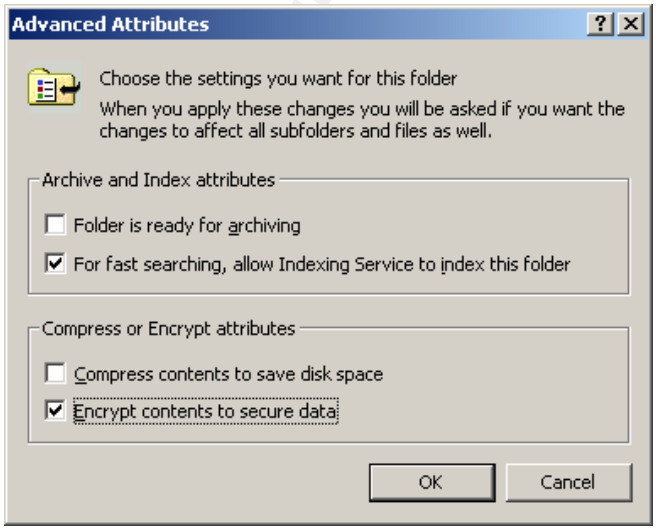
- **Built-in Encryption** - Windows 2000 comes with the Encryption File System (EFS) allowing files and folders to be encrypted dynamically. EFS works by encrypting and decrypting files and folders using symmetric encryption, then protects the symmetric key by using public key encryption.

- **Third-Party Encryption Tools** - There are a number of encryption products that can be purchased or downloaded for free. Examples of these are FileCrypto from F-Secure Corporation (www.fsecure.com) and Private File from Aladdin Systems (www.aladdinsystems.com).

The following steps describe how a folder is encrypted using Windows 2000 EFS:

1. Open the **Properties** dialog box for the appropriate folder.
2. In the **General** tab, click the **Advanced** button.

3. Check the box for the **Encrypt contents to secure data** option.



4. Click the **OK** button. All subfolders and files added to the encrypted folder will also be encrypted. Only the user who encrypted these files can open them. For recovery purposes, in case the encryption certificate and associated private key are lost, decryption can always be performed by the Administrator account.

Secure Home Computing Practices

The technical solutions discussed above present only one side of implementing a secure telecommuting environment. In order to implement a complete security solution, companies must also follow secure computing practices and train their telecommuters on how to keep their systems and data safe. Telecommuters or home-based workers need to be cognizant of the dangers of working from remote locations, and in turn have a defensive behavior while conducting business over the Internet.

Through training, users will learn that securing their systems not only protects their own property and information, but also protects everyone else's in the process. Companies also need to train home-based users to recognize and immediately report suspicious system behavior. Without the appropriate training, companies may find it difficult to enforce or convince telecommuters to secure their home-based systems.

Last November 2001, Ernst & Young International conducted a survey, which involved 459 CIOs and IT directors from different companies around the world. The survey results indicated less than 50% had IT security awareness and training programs for employees.

Here are other guidelines that should be established for telecommuters:

- Reduce the number of hours that remote computers are physically connected to the Internet. When not in use, shut down computers and turn off DSL or cable modems so that the chance of the computer being broken into is greatly reduced.

- Log off from high-speed Internet providers when not needed, because it forces the computer to obtain a new IP address the next time it logs back in.

- In extreme cases, physically unplug the network connection going into the computer (typically, an Ethernet connection) especially when suspicious activities are detected.

- Limit or control the applications installed and used on a computer. Keep up to date of any patches for all applications. For example, software products with security issues or known vulnerabilities are Kazaa, Instant Messenger and Outlook.

Implementation and Management Considerations

When implementing defensive solutions for work-at-home computers, companies must take into account the following important items:

- Consider home computers and networks to be extensions of the corporate computing environment. As such, these remote nodes, subnets and components have to be included in any enterprise security strategy.

- Decide whether or not to allow telecommuters to use their home personal computers for work. If the work-related data is highly confidential, it may be wise to provide a computer for work purposes only. In this case, companies can hold the employee responsible for the integrity and confidentiality of the data.

- Plan the deployment accordingly since it involves a huge number of home locations. This may number in the hundreds, or even thousands of geographic sites.

- Develop a process for on-going deployment of the security solution for new users. Security is not a one-time event. Companies must have a repeatable and reusable procedure to ensure consistency of protection across the enterprise. For example, for personal firewalls, these can be pre-installed and pre-configured as part of a standard image for company-issued home desktop computers.

- Provide home-based workers with a facility or process to notify the company of security breaches, detected intrusions or attempts, and other incidents.

- Determine how to remotely monitor and manage the continuous operation of the security solutions deployed on work-at-home computers. Consider locking down the system configuration to prevent users from disabling the security products installed like anti-virus programs and personal firewalls.

References

Danda, Matthew. Protect yourself online. Redmond: Microsoft Press, 2001.

McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions, Third Edition. California: Osborne/McGraw-Hill, 2001.

Dalton, Curtis. "Managing Remote Desktop Firewalls." Network Magazine. March 2001 (2001): 84 - 88.

Conry-Murray, Andrew. "Firewalls for All." Network Magazine. June 2001 (2001): 42 - 47.

Steinke, Steve. "Lesson 140: Cable Modem Systems." Network Magazine. March 2000 (2000): 38 - 40.

Farrow, Rik. "Distributed Denial of Service Attacks." Network Magazine. March 2000 (2000): 74 - 76.

McHugh, John; Christie, Alan; Allen, Julia. "Defending Yourself: The Role of Intrusion Detection Systems." IEEE Software. September/October 2000 (2000): 42 - 51.

Langhoff, June. "32 Million Telecommuters in 2001." 28 January 2001.
URL: http://www.langhoff.com/surveys.html - abc (12 April 2002).

Kirstein, Mark; Burney, Kneko; Paxton, Mike; Bergstrom, Ernie. "Moving Towards Broadband Ubiquity in U.S. Business Markets." April 2001
URL: http://www.instat.com/catalog/downloads/broadbandubiquity.pdf (10 April 2002).

Zone Labs, Inc.. "New Threats, New Solutions: Enterprise Endpoint Security." 2002.
URL: http://www.zonelabs.com/pdf/IntegrityOverview_final.pdf (29 April 2002).

Skedd, Kirsten. "Consumers Adopt Home Networks to Keep up with the Joneses." 10 April 2002. URL: http://www.instat.com/press.asp?ID=178&sku=IN020235RC
(11 April 2002).

Girard, John; Pescatore, John. "Home PCs Are the Weak Link in Enterprise Network Security." 2 November 2000.
URL: http://www3.gartner.com/DisplayDocument?id=316922&acsFlg=accessBought
(29 March 2002).

Salkever, Alex. “Broadband ISPs Shouldn’t Knock Down Firewalls.” 20 November 2001.
URL: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011120_6165.htm (27 April 2002).

Mainelli, Tom. “Tricky worm can spread via AOL’s instant message.” 10 April 2002.
URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,70002,00.html (11 April 2002).

Hurley, Edward. “Let Klez be a lesson to you.” 30 April 2002. URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci820435,00.html (2 May 2002).

Skedd, Kirsten. “"Always On" Broadband Drives Demand for Consumer Internet Security: Firewall Sales Lead Growth.” 10 July 2001.
URL: http://www.instat.com/pr/2001/rc0107hn_pr.htm (14 April 2002).

Verton, Dan. “Disaster recovery planning still lags.” 1 April 2002.
URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,69705,00.html (1 May 2002).

Salkever, Alex. “Scared of ‘Zombies’? You Should Be.” 30 May 2001.
URL: http://www.businessweek.com/bwdaily/dnflash/may2001/nf20010530_300.htm (14 April 2002).

Salkever, Alex. “IM Vulnerable.” 17 April 2001.
URL: http://www.businessweek.com/bwdaily/dnflash/apr2001/nf20010417_373.htm (14 April 2002).

Janss, Steve. “Protecting the homefront.” 14 May 2001.
URL: http://www.nwfusion.com/research/2001/0514feat2.html (25 April 2002).