BACKDOOR LIABILITY FROM INTERNET TELECOMMUTERS

by
*Mark J. Maier**

I. INTRODUCTION

Internet telecommuters work from home and access their employer's internal network over the Internet.[1] This relatively new style of work has increased in popularity through the years, with an estimated 4.5 million workers Internet telecommuting in 1999.[2] While employers enjoy compelling benefits such as reducing overhead costs, Internet telecommuting raises new security concerns for employers by exposing their internal networks to "backdoor attacks" that exploit the telecommuter's connection. The recent backdoor attack on Microsoft's source code illustrates the extent to which such attacks threaten confidential information.[3] If such confidential information belongs to a client or

---

* Mr. Maier is a technology attorney in Mayer, Brown & Platt's Washington D.C. Information Technology Practice. Previously, he served as a manager of systems integration services with Compaq Computer Corporation. Mr. Maier thanks Professor Michael Rustad for his advice on this article and John Downing, a Compaq colleague, for his assistance in identifying this issue.

1. *See* U.S. DEP'T OF LABOR, GLOSSARY OF COMPENSATION TERMS (1998) (defining "telecommuting" as work "at satellite offices or at home using a computer and related equipment that links the telecommuter to the employer's main office" and noting that the telecommuter may still be required to spend some time — one or two days a week, for example — in the main office), *available at* http://stats.bls.gov/ comhome.htm (last visited July 9, 2001).

2. *See* THE COLUMBIA ENCYCLOPEDIA (6th ed. 2000) (indicating that in 1999, about ten million people regularly worked as telecommuters in the U.S.), *available at* http://www.bartleby.com/65/te/telecommut.html (last visited July 9, 2001); Telework America, *Employers Save $10,000 Per Teleworker in Reduced Absenteeism and Retention Costs: Teleworkers Increase to 10 Percent of U.S. Adults* (Oct. 27, 1999), *at* http://www.telecommute.org/ twa/1999_research_results.html (last visited July 9, 2001) (reporting that over 19.6 million people indicated that they were telecommuters in 1999); *see also* Kathleen Murphy, *Web Fosters Telecommuting Boom, and Many in the Industry Take Part*, INTERNET WORLD MAG., Feb. 9, 1998, at 50 (estimating that 30% of telecommuters use the Internet to connect).

3. *See* Ted Bridis et al., *Microsoft Says Firm Detected Hacker Quickly, Monitored Activities Throughout Attack*, WALL ST. J., Oct. 30, 2000, at A3, ("[T]he notion that a family's home computer could pose such a serious risk to a giant company's computer network reveals a largely unrecognized threat

third party, then the telecommuter's employer may face significant liability for damages. In such cases, employer liability will probably hinge on whether the employer provided adequate protection from such an attack.

This article considers whether, and to what extent, an employer should protect itself and others from security threats introduced by Internet telecommuting. It describes the factual setting and technology of telecommuting over the Internet. It explains the mechanism of a backdoor attack, through which a hacker accesses the computer of a telecommuter as an avenue to invade the employer's computer system. The article also discusses the potential contract and tort liabilities that a company may face if, through such a backdoor attack, a hacker is able to obtain confidential client information stored on the company's system. Further, the article considers the possible duties and the standards of care that may be imposed in this relatively new area of potential legal liability.

Throughout the article, various risk–benefit analyses are provided using statistics from previous years and estimates of potential harm to client or customer information. These analyses focus on the probability of various attacks, the possible harm threatened by them, and the burdens to protect against them. If, however, the proposed methods are used as a basis for an actual risk–benefit analysis, then the analyst should substitute current statistics and should carefully tailor the analysis to the circumstances of the company at issue and the information at risk.

II. OVERVIEW OF BENEFITS AND RISKS

A. General Benefits of Internet Use

Many varied companies find the Internet beneficial in conducting business.[4] The most popular uses for employees are employer-provided Internet access and personal e-mail accounts. But companies that use the Internet for marketing purposes reap significant savings through new, efficient methods to contact potentially wider customer bases. Businesses also use the Internet to

---

to many corporations."), *available at* 2000 WL-WSJ 26614912; *see also* Jaikumar Vijayan & Carol Sliwa, *Analysis: Home Workers Can Imperil Systems*, IDG (Nov. 7, 2000), *at* http://www.cnn.com/2000/TECH/computing/11/07/home. workers.idg/ index.html; Jerry Loew, *Telecommuters' Security Looms as New Concern*, MASS HIGH TECH, Oct. 4, 1999, at 22.

4. DON TAPSCOTT, GROWING UP DIGITAL: THE RISE OF THE NET GENERATION 209-16 (1997). *See generally* Mark J. Maier, *Affordable Internet Access for All Americans*, 6 RICH. J.L. & TECH. 8 (1999), *available at* http://www. richmond.edu/jolt/v6i2/article3.html (last visited July 9, 2001).

provide information to the public, to manage orders and inventory, and to take automated orders.

Some businesses are particularly likely to profit from the use of telecommuting employees. Internet telecommuting is useful for manufacturers and retailers with traveling sales representatives[5] and for companies that must otherwise lease expensive office space for all their employees.[6]

Companies typically provide their employees with computer access to network services from inside company buildings.[7] These internal network services include access to shared data and use of common resources such as printers and data storage devices.

Internet Service Providers (ISPs) are the main avenues into the Internet for most parties, including businesses.[8] An ISP provides services similar to those provided by telephone companies, with businesses typically connecting their internal networks to the ISP with a permanent, high-speed connection.

Companies using the Internet have relationships with various entities and individuals outside the company. These relationships include contractual relationships with other businesses, with temporary workers, and with advisors such as outside lawyers and accountants. They also include commercial relationships with customers or clients.

Most companies commonly obtain and store valuable client information on their internal computer networks. For example, companies in service businesses often obtain sensitive client information, including credit card and bank account numbers. Similarly, companies that manufacture parts designed by other businesses may obtain and store a client's specifications that might be classified as trade secrets. Such easy access to centralized information generally benefits a business and its employees.

---

5. *See* About.com, *Telecommuting: Telework Centres & Flexible Option* (Aug. 27, 1999), *at* http://telecommuting.about.com/smallbusiness/telecommuting/library/ weekly/aa082799.htm (last visited July 9, 2001) (providing general information concerning telecommuting advantages).

6. *See* Paul C. Boyd, *Six Organizational Benefits of Telecommuting*, *at* http://pw2.netcom.com/~pboyd/orgbens.html (last visited July 9, 2001).

7. *See* Jennifer C. Dombrow, Note, *Electronic Communications and the Law: Help or Hindrance to Telecommuting?*, 50 FED. COMM. L.J. 685, 689 (1998) (discussing generally the costs of providing employee workstations).

8. *See ISP*, *at* http://www.sharpened.net/glossary/definition.php?isp (last visited July 9, 2001).

B. General Risks of Internet Use

1. How Does the Harm Occur?

Before Internet telecommuting, a typical company used a handful of Internet connections, and hackers[9] targeted these connections because they provided direct access to the company's network. Firewall systems,[10] however, commonly defeated hacker attacks by blocking access to the internal network.

With the increasing use of Internet telecommuting comes an increased number of connections that expose a company's internal network to attack from access points that did not previously exist. These new paths are "backdoor" alternative-access points through which a hacker might attack.

Generally, to connect with an employer, an Internet telecommuter must first install a tunnel client,[11] also known as a Virtual Private Network[12] ("VPN"), on a home computer.[13] The VPN first encrypts[14] all information destined for the

---

9. *See* Whatis.com, "Hacker," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (defining hacker as "a clever programmer" or "someone who tries to break into computer systems").

10. *See id.* at "Firewall" (defining "firewall" as "a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks").

11. *See id.* at "Tunneling" (defining "tunneling" as "using the Internet as part of a private secure network" and noting that a tunnel "is the particular path that a given company message or file might travel through the Internet").

12. *See id.* at "Virtual Private Network" (defining "Virtual Private Network" as "a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures"). A VPN can be contrasted with a system of owned or leased lines that can be used by only one company. A VPN gives a company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one.

13. *See* Mark Levine, *Telecommuting Safely — Remote Node or Remote Session?*, The SANS Institute (Feb. 19, 2001), *available at* http://www.sans.org/infosecFAQ/encryption/telecom.htm. *See generally* RSA Security, *Implementing Secure Virtual Private Networks*, *at* http://www.rsasecurity.com/_products/securid/whitepapers/vpns/ (last visited July 9, 2001) (discussing the structure and connectivity of VPN systems and the security concerns and protective measures associated with remote access communications through VPN systems that tunnel calls through the Internet).

14. *See* Whatis.com, "Encryption," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999)

employer's internal network. Next, the VPN communicates the encrypted information over the Internet and delivers it to the employer's firewall using a set of communication rules called point-to-point tunneling protocol.[15] The firewall recognizes the encrypted information as trusted information and routes it to a tunnel server, which then interrogates the packets, decrypts[16] the information, and forwards the packets into the employer's internal network.[17]

Backdoor attacks exploit the additional access points that the Internet telecommuter uses to communicate with the company's internal network. Unlike conventional attacks, backdoor attacks reach the company's internal network indirectly through the telecommuter, rather than directly into the company's main Internet connection. If the telecommuter uses an "advanced tunnel"[18] client that has firewall-like features, hacker access to the telecommuter's computer can be blocked. But if the telecommuter uses only a "basic tunnel"[19] without the firewall-like blocking ability, then the hacker has a much better chance of gaining access to the telecommuter's computer.

After gaining access to the telecommuter's computer, the hacker uses that computer to issue commands over the Internet and to the employer's network. The employer's firewall intercepts the packets before they reach the internal network.[20] But since the firewall recognizes these "hacked" packets as trusted information from the telecommuter, it routes them to the tunnel server, which then forwards the "hacked" packets into the employer's internal network.[21]

(defining "encryption" as "the conversion of data into a form, called ciphertext, that cannot be easily understood by unauthorized people").

15. *See id.* at "Point-to-Point Tunneling Protocol" (defining "Point-to-Point Tunneling Protocol" (also called "PPTP") as "a set of communication rules that allows corporations to extend their own corporate network through private 'tunnels' over the public Internet").

16. *See id.* at "Decryption" (defining "decryption" as "the process of converting encrypted data back into its original form").

17. *See* Mark Maier, *Setting New Duties and Standards of Care for Internet Telecommuters*, Appendix A *at* http://www.law.suffolk.edu/academic/hightech /students/maiertelesec.html (last visited July 9, 2001).

18. *See* Whatis.com, "Tunnelling," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (explaining that an advanced tunnel provides both encryption (information protection) and a firewall (access prevention)).

19. *Id.* (noting that a basic tunnel provides only encryption (information protection)).

20. *See* Maier, *supra* note 17, at Appendix A.

21. *Id.*

Using a backdoor attack, the hacker can circumvent the strongest firewall security and gain access to the employer's internal network. At risk, then, are any trade secrets and any other confidential or proprietary materials that are on the network and accessible by the telecommuter. Moreover, if a client or other party owns the information, then the employer itself may be liable for losses resulting from the hacker's security breach.

2. What Type of Harm Occurs?

With the advent of Internet business, information theft has become a significant business risk.[22] Information theft and subsequent dissemination have devastating effects on trade secrets, which derive their worth from their secrecy. For example, a software developer's source code is typically highly secret and protected. But once placed in the public domain, anyone can readily copy and integrate the source code into other products.

Information disclosure can also destroy the practical value of confidential information that is normally unavailable to competitors. Written works in electronic form are also vulnerable to copyright infringement by hackers who could unlawfully copy and distribute these works. Ultimately, such harmful attacks could result in millions of dollars in damages.

Unfortunately, information theft is not a risk borne solely by the business whose system is invaded. Successful hackers may gain access to information and data belonging to the clients of a business that stores such client information. Under those circumstances, the business itself could be liable if a hacker compromises a client's information and causes the client harm. And if the business is found grossly negligent in storing or protecting the client information, then the business may be liable for punitive damages as well as actual damages.[23] Such increased damages may likewise be assessed if a company was holding the information as a fiduciary for the client.

III. INTERNET ENVIRONMENT BEFORE TELECOMMUTING

A. The Mechanism of Frontdoor Attacks

Connecting a company's internal network to the Internet exposes it to attack through unauthorized access by hackers.[24] Computer virus attacks have

---

22. Arthur Andersen, *Business Risks and the Virtual Office, Part 2, at* http://www.itaudit.org/forum/riskmanagement/f212rm.htm (discussing risk of information theft and various methods of information theft) (last visited July 9, 2001).

23. *See* DANIEL S. KLEINBERGER, AGENCY AND PARTNERSHIPS 133 (1995).

24. *See* Whatis.com, "Hacker," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999).

become common,[25] and some have made international news due to their widespread destruction of data and systems.[26] As a result, companies have increasingly recognized the need for anti-virus software. In 1999, businesses reported 9,859 Internet attacks to the CERT® Coordination Center.[27]

Before Internet telecommuting, hackers targeted a company's internal network through "frontdoor" attacks aimed at the company's Internet access points. Frontdoor attacks by hackers include obtaining user passwords and planting harmful viruses on computers.[28]

Hackers have also launched frontdoor attacks using "Trojan Horse"[29] programs. With such a program, data enters an employee's computer by posing as trusted data, such as an e-mail attachment.[30] The Trojan Horse applet is included in the attachment. When the attachment is viewed, the applet transparently installs itself in the employee's computer. Once inside, a Trojan Horse can monitor passwords, launch resource-intensive activities, and even destroy data.[31] A Trojan Horse can also transmit passwords to the hacker.[32]

---

25. *See* Ross Kerber, *Safe Surfing*, BOSTON GLOBE, Apr. 27, 1999, at C1, *available at* 1999 WL 6059502.

26. *See* Stan Miastkowski, *How to Protect Yourself Against Melissa*, CNN.com, *at* http://cnn.com/TECH/computing/9903/29/melissa.02.idg/index.html (Mar. 29, 1999) (describing the Melissa virus that appeared on Friday, March 26, 1999, as "the most wide-spread [virus] we've seen to date"); Cameron Crouch, *I Was Bitten by the Love Bug*, CNN.com, *at* http://www.cnn.com/2000/TECH/computing/05/08/love.bite.idg/index.html (May 8, 2000) (describing the "Love Bug" virus that swept around the world).

27. *See* CERT Coordination Center, *CERT/CC Statistics 1988-2000*, *at* http://www.cert.org/stats/cert_stats.html (last updated Apr. 26, 2001).

28. *See* Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 216-30 (1995).

29. *See* Whatis.com, "Trojan Horse," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (describing a Trojan horse as "a program in which malicious or harmful code is contained inside apparently harmless programming data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk").

30. *Id.*

31. *See* Michelle Delio, *Viruses? Feh! Fear the Trojan*, *at* http://www.wired.com/news/infostructure/0,1377,43981,00.html (May 24, 2001).

32. *See Beware the Trojan Horse*, Wired News Report, *at* http://www.wired.com/news/technology/1,1282,13477,00.html (July 7, 1998).

Hackers also gain frontdoor access by stealing authorized access passwords without using a Trojan Horse.[33] Because such passwords are stored in commonly known locations in computer operating systems such as UNIX, they are easily located by hackers.[34]

Hackers may also gain access by "spoofing" their own addresses. In a spoof, the hacker makes his actions look as if they are coming from a trusted location or from a safe e-mailer.[35]

B. The Probability of a Frontdoor Attack

According to the Computer Emergency Response Team (CERT) at Carnegie Mellon University and the SANS Institute, businesses in 1999 reported 9,859 Internet attacks.[36] In 20% of these reported attacks, the hacker obtained full access to target computers.[37] In another study of 4,299 attack incidents[38] reported to the CERT Coordination Center between 1989 to 1995, 57.9 percent of all typical Internet domain attacks succeeded.[39]

---

33. *See* WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER 159-61 (1994).

34. *See id.* at 159.

35. *See generally* Steven A. Heinrich & Roxana Dastur Malladi, *News of the Wired: Security, the Internet and the Networked Office--Problems for Law Offices*, 56 OR. ST. B. BULL. 15 (Dec. 1995) (discussing security concerns generally and indicating that problems from hackers are amplified by (1) the wide availability of hacking tools on the Internet, and (2) the sometimes-limited expertise of computer administrators).

36. *See* CERT Coordination Center, *supra* note 24, *at* http://www.cert.org/stats/cert_stats.html (last updated Apr. 26, 2001); *see generally How To Eliminate The Ten Most Critical Internet Security Threats*, The SANS Institute, *at* http://www.sans.org/topten.htm (June 25, 2001).

37. *See* John J. Fialka, *Computer Hackers Cost Big Business $800 Million in '95*, WALL ST. J., June 6, 1996, at B2, *available at* 1996 WL-WSJ 3105739 (reporting that 20% of the reported incidents evaluated by CERT during the first quarter of 1996 involved "total compromises" of the computer systems).

38. *See* John D. Howard, An Analysis of Security Incidents on the Internet: 1989 - 1995 (1997) (unpublished Ph.D dissertation, Carnegie Mellon University) (noting that an incident involves "a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing"), *available at* http://www.cert.org/research/JHThesis/Chapter1.html (last visited July 9, 2001).

39. *Id.* at Chapter 7 (noting that the 57.9% of attacks were comprised of 31% root break-ins and 26.9% account break-ins; 42.1% of attacks were unsuccessful).

C. Precautions Against Frontdoor Attacks

1. General Security Procedures

Solid security policies and procedures are the first line of defense against hackers.[40] Physical defenses include reliable building security such as keycard access and human guards at all entrances and exits. And for information that is considered extremely valuable, the strongest precaution is to keep the information off any network computer.

Another general security procedure is to require all authorized users to use nonobvious, frequently changing passwords.[41] Anti-virus software installed on all company computers also increases security. Such a software program scans information that enters a computer and warns the user if a virus is detected.[42] The user then opts to have the program either clean or delete the infected files.

But the strict policies that protect information may also inhibit access to that information. As more security is put in place, information becomes less available because it is more difficult to access. This result is not always preferable in today's fast-paced business world. Thus, each business that uses the Internet must strike a balance between the conflicting goals of information availability and information protection.

2. Encryption (Information Protection)

Encryption technology is a specialized security measure that protects information, even if an unauthorized user obtains the information. While encryption scrambles information with a key, decryption[43] allows those with the correct key to decode and use the information.[44]

Standard encryption methods include the Data Encryption Standard ("DES"); Rivest, Shamir, and Adelman encryption standard; and the Pretty Good Privacy process. The DES is a widely used standard, including use by the U.S. government.[45] DES was originally based on 40-bits of encryption for

---

40. *See* Rustad & Eisenschmidt, *supra* note 28, at 238.

41. *See* CHESWICK & BELLOVIN, *supra* note 33, at 159.

42. *See* Symantec Corporation, Reference Area, *at* http://www.symantec.com/avcenter/refa.html (last visited July 9, 2001) (discussing Norton Anti-Virus from Symantec, a leading product in the anti-virus software market).

43. *See* Whatis.com, "Encryption," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999).

44. *See* CHESWICK & BELLOVIN, *supra* note 33, at 211.

45. *See* JAMES ADAMS, THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE 215-16, 219 (1998).

private and business use, with stronger 128-bit and 156-bit encryption more commonly used today.[46]

3. Firewalls (Access Prevention)

An Internet firewall, which is placed between a company's internet network and the Internet, prevents unauthorized access to such a network. Individual firewall products typically cost between $5,000 and $20,000,[47] with Cisco's PIX Firewall, for example, costing about $7,000.[48]

The underlying way in which firewalls operate is to inspect traffic that is divided into small units called packets or frames. Each packet has a source and destination address similar to the "To" and "From" addresses on a package sent in the mail. These Internet addresses are referred to as Internet Protocol ("IP") addresses. More specifically, an IP address has a network portion (which is analogous to a street name) and a host portion (which is analogous to a street number). For example, in the IP address "20.10.30.100," "20" is the network number and "10.30.100" is the computer's host number.[49]

Firewalls can be set to filter incoming packets by reading each packet and rejecting anything not coming from a trusted location. In the preceding IP address example, the firewall could be programmed to exclude anything that is not part of the "20" network.

Firewalls may also filter data based on the port number — a number that identifies and organizes network activity on a particular computer. For example, much of the Internet's traffic is transferred with HTTP[50] text, which typically

---

46. *See* Robert Moskowitz, *DES Is Dead. Long Live . . . Well, Um, What?*, NETWORK COMPUTING, Mar. 22, 1999, *available at* http://www.networkcomputing.com/ 1006/1006colmoskowitz.html (along with its wide use have come numerous successful competitions to break DES's encryption).

47. American City Business Journals Inc., *In Depth: Security: Q & A: How Much Does It Cost to Set Up and Maintain a Firewall?* (May 5, 2000) *at* http://sanjose.bcentral.com/sanjose/stories/2000/05/08/focus4.html.

48. *See* CDW Computer Centers, Inc., *Cisco Entry Level 233MHz PIX Firewall 520*, *at* http://www.cdw.com/shop/products/default.asp?EDC=132767 (last visited July 18, 2001).

49. *See* Howard, *supra* note 38, at Chapter 2.

50. *See* Whatis.com, "HTML," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (explaining that Hypertext Markup Language ("HTML") — a set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page — tells the Web browser how to display the words and images).

uses a port number of 80. Another common traffic type is SMTP[51] e-mail, which typically uses a port number of 25. Firewalls can be used to filter all traffic except e-mail port number 25. Thus, this firewall filter would allow only activity destined for port 25 and would reject everything else.[52]

Port filtering is most effective when used in conjunction with content filtering.[53] This combination allows greater precision in screening incoming messages. The combination filter is set to allow only the proper type of content headed for the proper type of port. For example, a packet will identify whether it is carrying HTTP traffic or SMTP e-mail. Firewalls can be used to exclude all traffic except SMTP e-mail. If used in a port/content filter combination, firewalls can be configured to exclude all traffic except SMTP e-mail destined to port 25. If HTTP traffic is destined for a computer on port 25, the firewall will reject this packet. Similarly, if a SMTP e-mail request comes in destined for a port other than 25, it will also be rejected.[54]

Firewalls also can counter "spoofing" — in which a hacker uses a trusted source IP address in a packet that actually comes from the hacker.[55] Firewalls counter spoofing by identifying the actual owner of the address with a Domain Name System (DNS) lookup and asking if any packets were sent to the network. If the actual owner replies in the negative, the hacker's packet will be rejected.[56]

---

51. *See* Whatis.com, "Simple Mail Transfer Protocol," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (noting that Simple Mail Transfer Protocol ("SMTP") is "a TCP/IP [Transmission Control Protocol/Internet Protocol] protocol used in sending and receiving e-mail").

52. *See* CHESWICK & BELLOVIN, *supra* note 33, at 85.

53. *Id.*

54. *Id.*

55. *Id.*

56. *See* Whatis.com, "Domain Name System," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (explaining that the Domain Name System ("DNS") is a system of locating Internet domain names and translating them into Internet Protocol addresses).

IV. INTERNET ENVIRONMENT AFTER TELECOMMUTING

A. The Growth of Internet Telecommuting

Internet telecommuting developed when businesses realized that they could save money by allowing employees to work out of their homes.[57] This approach decreased the need for expensive office space.[58] Sales representatives, customer service professionals, corporate officers, and attorneys are good candidates for telecommuting because their work commonly allows them to work at home, instead of in a central business location.

As of 1999, there were an estimated 13 million telecommuters in the United States.[59] An estimated 30 percent of these telecommuters operate through the Internet.[60] Based on these estimates, in 1999 there were about 3.9 million Internet telecommuters in the U.S.[61]

A typical Internet telecommuter needs access to the company's internal network resources such as e-mail and data storage. For many years, these resources were available only from within the company's physical buildings. At that point, telecommuters initially dialed directly into the business's internal network using telephone lines. While this method allowed telecommuters to access the company's resources, the company had to invest in, and maintain, complex and unreliable telephone access equipment.[62]

The increased cost of the telephone access method prompted a search for a better way to connect telecommuters. Simultaneously, telecommuters began to purchase their own computers and home Internet access from local ISPs.[63] Eventually, it became clear that the Internet could be used to provide access into

---

57. *See* U.S. DEP'T OF LABOR, GLOSSARY OF COMPENSATION TERMS (1998), *available at* http://stats.bls.gov/comhome.htm (last visited July 9, 2001) (discussing Internet telecommuting).

58. *See* International Telework Association & Council, *at* http://www.telecommute.org/ (last visited July 9, 2001); http://telecommuting.about.com/smallbusiness/telecommuting/mbody.htm (last visited July 9, 2001).

59. *See* Press Release, U.S. Telecommuting Trend Surpasses 11 Million, Find/SVP, *at* http://etrg.findsvp.com/prls/pr97/telecom.html (Apr. 10, 1999).

60. *See* Kathleen Murphy, *Web Fosters Telecommuting Boom, and Many in the Industry Take Part*, INTERNET WORLD MAGAZINE, Feb. 9, 1998, at 50.

61. For figures and estimates of the number of Internet telecommuters, see *supra* note 2 and accompanying text.

62. *See* Cubix Employer, *Solving Business and Computing Problems*, *at* http://www.cubix.com/corporate/solutions/solutions.htm (last visited July 9, 2001).

63. *See e.g., ISP, at* http://www.sharpened.net/glossary/ definition. php?isp (last visited July 9, 2001).

the business's internal network through ISPs and tunneling products. Thus, telecommuters could connect to the Internet through their local ISPs and then tunnel into the company's internal network. With this method, the ISP, rather than the company, maintained the telephone access equipment.[64]

ISPs also offer higher-speed Internet access through cable television modems[65] or high-speed DSL[66] phone lines. Such access methods are up to 50 times faster than traditional telephone dial lines.[67]

But such high-speed Internet users are prime targets for attack. The reason is simple: cable modems and DSL allow perpetual "always on" access to the Internet, while dial systems provide only intermittent connectivity. And if a hacker succeeds in attacking and controlling a high-speed remote computer, then the computer can become a powerful tool to launch attacks such as "denial of service" attacks.[68]

B. The Mechanism of Backdoor Attacks

Internet telecommuters create additional vulnerability for employers because each telecommuter provides a connection point to the Internet. Unlike a company's main Internet connection, which is usually firewall-protected against frontdoor hackers, most telecommuters do not use firewalls when connecting to the Internet.[69] Hackers can thus circumvent the company's

---

64. *See generally* International Telework Association & Council, *at* http://www.telecommute.org/ (last visited July 15, 2000).

65. *See* Whatis.com, "Cable Modem," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (explaining that a cable modem is a device that enables you to hook up your PC to a local cable TV line and to receive data at about 1.5 Mbps.).

66. *See id.* at "DSL Guide" (noting that Digital Subscriber Line ("DSL") is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines).

67. *See* TechTarget.com, "Cable Modem," *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211726,00.html (last modified Oct. 20, 2000).

68. *See* Whatis.com, "Denial of Service," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (indicating that a denial of service ("DOS") attack is an incident in which a user or organization is deprived of the services of a resource that would normally be available).

69. *See* Bridis, et al., *supra* note 3, at A3; *see also* Vijayan, et al., *supra* note 3, *at* http://www.cnn.com/2000/TECH/computing/11/07/home.workers.idg/index.html; Loew, *supra* note 3, at 22; Kelly Jackson Higgins, *Bell Canada Secures the Last Frontier, Network Computing*, *at* http://www.networkcomputing.com/1214/1214centerfoldtext.html (July 9, 2001).

firewall by first compromising a telecommuter's computer and then using the connection to access the company's internal network. Such a backdoor attack occurs in two steps.

1. The First Step: Accessing the Telecommuter's Computer

The hacker gains access to the telecommuter's computer in one of several possible ways. For example, a telecommuter might "share" the home computer with the hacker by sharing files on the computer with other Internet users without any security. When this occurs, the hacker can simply connect to the shared computer and access its resources. In many cases, the original user will not even know that someone else has accessed the computer.

ISPs frequently warn their subscribers about the risks of backdoor hacker attacks. For example, MediaOne[70] issued the following warning to its subscribers:

> **MediaOne Express RD Security Notice**
>
> As a MediaOne Express customer, you are probably aware that the Internet is a shared resource, with many people utilizing it at any given time. One popular feature of our MediaOne Express Service allows you to share your files with other users. However, we want to remind you that use of the file-sharing feature increases the risk that other Internet users could gain access to any of the files on your computer's hard drive. As a result, **you** must remain aware of these risks and secure your computer from access by other users. **We strongly encourage you to take these steps to prevent other users from gaining access to your computer files.** . . .

Alternatively, a hacker might plant a Trojan Horse in the telecommuter's computer.[71] A Trojan Horse can be programmed to wait until the telecommuter enters a valid user name and password and then to send that information to the hacker, who can then use it to access the company's internal network.[72]

---

70. *See* MediaOne, Inc., *MediaOne Express RD Security Notice* (Dec. 23, 1997) *available at* http://www.law.suffolk.edu/academic/hightech/students/maiertelesec.html (last visited July 9, 2001).

71. *See Beware the Trojan Horse*, *at* http://www.wired.com/news/technology/1,1282,13477,00.html (July 7, 1998).

72. *See* Bridis, et al., *supra* note 3, at A3; *see also* Vijayan, et al., *supra* note 3; Loew, *supra* note 3, at 22; Higgins, *supra* note 69.

Although the possibility of a Trojan Horse attack is worrisome, even more damage can result if a hacker plants a remote control applet in a telecommuter's computer.[73] This device allows the hacker to function as if actually sitting at the target computer.[74] Like the Trojan Horse, the remote control applet runs in the background of a telecommuter's computer without the telecommuter ever noticing its presence. The hacker does not have to go through the effort of obtaining someone else's name and password. Instead, the hacker simply remotely controls the computer and monitors when the telecommuter enters all the appropriate passwords for the various security systems. The hacker then "pulls the strings" of the telecommuter's computer. And to the employer's firewall security systems, the information appears to be sent from an authorized telecommuter.[75]

A remote control applet can be installed on a remote computer if the telecommuter interacts with an Internet website that has been imbedded with the applet.[76] When the website is accessed to download information, the telecommuter's IP address can easily be recorded by the website or by the hacker. When the information is downloaded from the website, the imbedded remote control applet is also downloaded to the remote computer. When the downloaded information is executed, the remote control applet is also executed in the background.[77] Without current anti-virus protection, the remote control applet will run in the background without alerting the telecommuter. At this point, the hacker only needs to use the telecommuter's IP address to interact with the remote control applet.

One notorious remote control applet is "Back Orifice," which is a program developed by a group known as "the Cult of the Dead Cow."[78] This applet allows the hacker to control and monitor remotely a computer running the

---

73. *See* Whatis.com, "Applet," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999) (noting that "applet" is an expression for a small computer program or application).

74. *See* Delio, *supra* note 31, *at* http://www.wired.com/news/infostructure/0,1377,43981,00.html (May 24, 2001).

75. *See* Commodon.com, *The Current List of Remote Control Trojan* (offering a current list of remote control Trojan Horse applets) *at* http://www.commodon.com/threat/threat-all.htm (last visited July 10, 2001).

76. *See Beware the Trojan Horse*, *at* http://www.wired.com/news/ technology/1,1282,13477,00.html (July 7, 1998).

77. *See* News Release, *ZDNET Site Sends Users to Backdoor Program, Softseek.Com Promotes Trojan Horse to Unwitting Users, NWI*, (Oct. 7, 1999) *at* http://www.nwi.net/~pchelp/security/alerts/softseek.htm.

78. *See* James Glave, *Back Orifice a Pain in the . . . ?*, WIRED (July 29, 1998), *available at* http://www.wired.com/news/news/technology/story/14092.html.

Microsoft Windows operating system. Back Orifice has become so pervasive that there are reports that it has compromised 1,400 Internet accounts in Australia.[79] Windows NT is also vulnerable to these kinds of remote control applets, as evidenced from the "Remote Explorer" or "RICHS" virus.[80]

2. The Second Step: Accessing the Employer's Internal Network

The second step in a backdoor attack is for a hacker, now in control of the telecommuter's computer, to use the telecommuter's trusted tunnel connection to access the company's internal network. The company's security views the hacker's action as the action of the telecommuter. Therefore, a backdoor attack can circumvent the strongest multi-tiered firewall security systems. Because the network traffic comes from the trusted telecommuter, the security system cannot tell that a hacker is issuing the commands.

Such a backdoor attack was recently used against Microsoft. In that instance, a hacker gained backdoor access to source code information stored on a telecommuter's computer and to information on Microsoft's internal network.[81] This information could have also included confidential information owned by third parties.

C. Unique Benefits of Internet Telecommuting

The primary economic benefit of Internet telecommuting is the cost that it saves on leased office space. Office space in a U.S. metropolitan area may cost $25 per square foot per month, or even more.[82] At that price, a 50 square-foot office costs an employer $1,250 per month, which amounts to $15,000 per year per employee. If an employee spends little time at the office, this cost does not represent a strong return on investment. Indeed, thousands of dollars might be saved by initiating a telecommuter program,[83] with the initial setup costs recouped within the first few months of telecommuting.

---

79. *See* Christopher Jones, *Back Orifice Surfaces Down Under*, WIRED (Nov. 17, 1998), *available at* http://www.wired.com/news/news/technology/story/16310.html.

80. *See* CERT Coordination Center, *CERT® Incident Note IN-98-07: Windows NT "Remote Explorer" Virus*, *at* http://www.cert.org/incident_notes/IN-98-07.html (last visited July 9, 2001).

81. *See* Bridis, *supra* note 3 at A3.

82. *See* Reis Reports, http:www.reisreports/com (updated July 10, 2001) (exact rates vary by city).

83. *See* Kathy McCabe, *Working the Virtual Office*, Boston.com, *at* http://www.boston.com/business/emerging/past_features/virtualoffice.htm (last visited July 9, 2001).

Other tangible benefits result from Internet telecommuting. First, employers enjoy increased employee productivity, decreased absenteeism, improved employee retention, and reduced employee recruitment costs.[84] Second, employees enjoy a reduction in commute time, greater flexibility in daily scheduling, more control over environmental conditions such as room temperature, fewer interruptions, reduced stress levels, and an overall increase in morale and job satisfaction.[85] Third, society enjoys less traffic congestion, less air pollution, less gas consumption, and lower costs for road maintenance and repair.[86] If proper security measures are implemented, these benefits can outweigh the risk from hackers.

D. The Probability of a Backdoor Attack

Using national statistical averages, the general probability of a backdoor attack can be calculated. But for a specific telecommuter at a given time, an analyst would need to use fact-specific values and probabilities. For instance, the probability of attack on an Internet telecommuter working for an entity such as Microsoft or the U.S. Department of Defense would be much higher than average. Further, the probability of backdoor attacks may change as new security measures and new attack methods are developed.

Generally, in 20 percent of Internet attacks, the hacker obtains full access to the computer.[87] Of the annual attacks on a typical Internet domain in 1999, about 57.9 percent were successful.[88]

The analysis that follows identifies the average probability of a backdoor attack on a company's internal network through an Internet telecommuter. This analysis provides merely a statistical model that may be useful in conducting such an analysis for a specific business, based on recent variables.

---

84. *See* Dombrow, *supra* note 7, at 689.

85. *See id.*

86. *See id.*

87. Fialka, *supra* note 37, at B2.

88. *See* Howard, *supra* note 38, at Chapter 7.

The first step is to identify the numbers of users.

A. At the end of 1998, there were approximately 70,000,000 Internet users in the U.S.[89]

B. Based upon three independent estimates made in 1999, an average of 13,000,000 telecommuters worked in the U.S.[90]

C. To calculate the total number of Internet telecommuters in the U.S., take 30 percent of B (since 30 percent of telecommuters connect to the Internet).[91] This figure is computed as follows: 0.3 x 13,000,000 = 3,900,000.

D. To calculate the percentage of Internet telecommuters as compared to all Internet users in the U.S., divide C by A. This figure is computed as follows: 3.9M / 70M = 5.57 percent.

The second step is to identify the probabilities of backdoor attacks.

E. The probability of a successful attack on a company's internal network in a year was identified above as 0.579.[92]

F. The probability of any Internet user being successfully attacked by any method in a year is 1 in 45, or 2.2 percent.[93]

G. The probability of any Internet user (F) being successfully attacked by a remote control method in a year is approximated by taking 10 percent of F. This number is computed as follows: 0.1 x 0.0222 = 0.00222.

---

89. *See* CyberAtlas, *70 Million Americans Access Net*, Internet.com (May 14, 1999), *at* http://www.cyberatlas.com/big_picture/geographics/article/0,1323,5911_151261,00.html.

90. *See* THE COLUMBIA ENCYCLOPEDIA: SIXTH EDITION, *available at* http://www.bartleby.com/65/te/telecommut.html (last visited July 9, 2001); Telework America, *Employers Save $10,000 per Teleworker in Reduced Absenteeism and Retention Costs: Teleworkers Increase to 10 Percent of U.S. Adults* (Oct. 27, 1999), *at* http://www.telecommute.org/twa/1999_research_results.shtml; Find/SVP Press Release, *U.S. Telecommuting Trend Surpasses 11 Million* (visited Apr. 10, 1999), *at* http://etrg.findsvp.com/prls/pr97/telecom.html.

91. *See* Murphy, *supra* note 60, at 50.

92. *See supra* notes 38-39, 88 and accompanying text.

93. *See* Howard, *supra* note 38, at Abstract.

H. The probability of an Internet telecommuter (D) being successfully attacked by a remote control method (G) in a year is obtained by taking the product of D and G. This figure is computed as follows: 0.0557 x 0.00222 = 0.0001236.

I. The probability of a backdoor attack on the employer's internal network (H) through an Internet telecommuter (E) per year is obtained by taking the product of E and H. This probability is computed as follows: 0.579 x 0.0001236 = 0.0000715.[94]

Two variables, however, may increase the probability per telecommuter. First, the base 0.579 probability was obtained from a random sample of CERT-focused reports; thus, it may not reflect focused attacks on popular targets such as a U.S. military site or Microsoft. Second, the CERT data may underrepresent the true number of attacks since it is estimated that less than five percent of all attacks are reported to CERT. Thus, the probability may be understated by a factor of twenty.

Even if the probability of a backdoor attack is as small as 0.0000715, that number is significant. When applied to the relevant population of 3.9 million Internet telecommuters, the probability predicts that there will be about 279 successful backdoor attacks on telecommuters and their employers' networks in the next 12 months.

E. Precautions Against Backdoor Attacks

Tunnel clients come in two forms — basic and advanced. Basic tunnels protect transmitted information with encryption. Advanced tunnels, which are more costly, protect information with both encryption and features similar to firewalls. An alternative approach to tunneling is to install a full firewall for each telecommuter.

1. Basic Tunnels (Encryption Information Protection)

Allowing telecommuters to connect to a company's network through the Internet saves money, but increases risks. To mitigate those risks, employers can use Virtual Private Network[95] (VPN) tunneling[96] security products. Basic VPN

94. *See Securing E-Commerce*, SOLUTIONS INTEGRATOR, Apr. 1999, at 67.

95. *See* Whatis.com, "Virtual Private Network (VPN)," *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212220,00.html (last modified Oct. 18, 1999).

96. *See id.* at "Tunneling."

tunnels use encryption to protect information in the event of interception.[97] If a hacker obtains encrypted data, that information will have limited value without the decryption keys. But basic tunnels do not prevent access to the telecommuter's computer. Therefore, basic tunnels do not protect telecommuters or their employers from backdoor attacks.

A tunnel service must be installed to implement a basic tunnel connection between the telecommuter and the employer's internal network. The tunnel service consists of a client component on the telecommuter's computer and a server component inside the company's network.[98] Because the Internet is used to connect telecommuters, the risk of interception is high. To protect transferred information, basic tunnels provide an encrypted path between the telecommuter and the company's internal network.

With this system in place, raw information is encrypted and placed inside a packet for transmission. The communication over the Internet is initially set up using highly secure 1024-bit encryption, which can be described as strong but slower. Once established, the communication continues at a faster-paced 40-bit encryption, with the firewall configured to allow the tunnel packets to pass only to the tunnel server. VPN tunnel clients can be implemented with software-only products such as AltaVista's Tunnel or Microsoft's Tunnel,[99] or by using hardware products that are external to the telecommuter's computer.[100]

Table 1, below, summarizes the cost of providing basic tunnel service to a telecommuter. Costs include the client components plus the distributed cost of the tunnel server. Note that the cost of the Internet service from the ISP is not included in Table 1, since the telecommuter is expected to have Internet access.

The information in Table 1 is computed as follows: the cost of basic tunnel client software ranges from free software included in the operating system[101] to $100 per telecommuter computer. Therefore, when using free software, the cost for basic tunnel service is the cost of the server divided by the number of telecommuters. The cost of a tunnel server is approximately $5,000 for all associated hardware and software.[102]

---

97. *See id.*

98. *See id.*

99. *See* Microsoft Corp., *Virtual Private Networking: An Overview*, *at* http://msdn.microsoft.com/workshop/server/feature/vpnovw.asp (May 29, 1998).

100. *See* Vic Cutrone, *Cisco 1720 Ensures Secure Links*, NETWORK COMPUTING (Feb. 8, 1999), *at* http://www.networkcomputing.com/1003/1003sp1.html.

101. *See* Microsoft Corp., *Virtual Private Networking: An Overview*, *at* http://msdn.microsoft.com/workshop/server/feature/vpnovw.asp (May 29, 1998).

102. Compaq Computer Employer, *AltaVista Tunnel*, *at* http://altavista.software.digital.com/tunnel/index.asp (Mar. 24, 1999).

The cost per telecommuter depends on the number of telecommuters a company employs. Thus, for 10 telecommuters, the total cost is $5,000, and the cost per telecommuter would be $5,000 divided by 10 or $500 per telecommuter. For 100 telecommuters, the total cost is still $5,000, and the cost per telecommuter would be $5,000 divided by 100 or $50 per telecommuter. For 1,000 telecommuters, the total cost is still $5,000, and the cost per telecommuter would be $5,000 divided by 1,000 or $5 per telecommuter.

Since one VPN server can handle about 1,000 telecommuters (although VPN server capacity varies widely), 1,100 telecommuters would require two tunnel servers for a total cost of $10,000, and the cost per telecommuter would be $10,000 divided by 1,100 or $9.09 per telecommuter. For 5,000 telecommuters, a company would need five tunnel servers for a total cost of $25,000, and the cost per telecommuter would be $25,000 divided by 5,000 or $5 per telecommuter. Therefore, for numbers of telecommuters above 1,000, the cost per telecommuter remains between $5 and $10.

2. Advanced Tunnels (Encryption Information Protection Plus Firewall Access Prevention)

An advanced VPN tunnel provides the encryption features found in basic tunnels as well as preventive security features similar to firewalls, which protect a telecommuter's computer from a hacker's unauthorized access.[103] Advanced tunnel products are available from a number of vendors, including Altiga[104] and 3Com,[105] for a few hundred dollars per telecommuter computer.

Some advanced tunnels also offer a security feature that precludes a hacker from running a remote control applet by limiting communication to exchanges between the company's network and the telecommuter's computer.[106] In this way, a telecommuter could not simultaneously access the employer's network and the Internet. Thus, on the other side of the advanced tunnel client, a hacker could not access the telecommuter's computer while it was in communication with the employer's network. Although disabling this feature makes the telecommuter's computer less secure, the feature can be disabled if a telecommuter needs to "split tunnel" by simultaneously communicating with the internal network and the Internet.[107]

---

103. *See* Higgins, *supra* note 69.

104. *See* Mike Fratto, *Altiga Concentrates on VPN Security*, NETWORK COMPUTING (Mar. 22, 1999), *at* http://www.networkcomputing.com/1006/ 1006sp1.html.

105. *See* Vic Cutrone, *3Com Tunnels a Secure Solution*, NETWORK COMPUTING (Mar. 8, 1999), *at* http://www.networkcomputing.com/1005/1005sp1.html.

106. *See, e.g.*, Fratto, *supra* note 104.

107. *See* Mike Fratto, *Nortel Updates Contivity for Enterprises*, NETWORK COMPUTING *at* http://www.networkcomputing.com/922/922sp2.html (last

The cost of providing advanced tunnel service to a telecommuter is higher than basic tunnel security and is summarized in Table 1 below. Here, the cost of one advanced tunnel server varies widely based on make and model,[108] but $5,000 is a rough approximation of all associated hardware and software.

For up to 99 telecommuters, the cost per telecommuter is $200; for 100-999 telecommuters, the cost per telecommuter is $100; for 1,000-4,999 telecommuters, the cost per telecommuter is $50; and, for 5,000 or more telecommuters, the cost per telecommuter is $10.[109]

The cost for advanced tunneling is then computed by combining the cost of the client components with the distributed cost of the tunnel server. Note, again, that the cost of the Internet service is not added to the cost of tunneling, since the telecommuter is expected to already have Internet access from an ISP. Thus, for 10 advanced telecommuters, the cost is $200 per telecommuter for components and $500 per telecommuter for server costs, which equals $700 per telecommuter, or a grand total of $7,000. For 100 advanced telecommuters, the component cost of $100, plus the server cost of $50, equals $150 per telecommuter, or a grand total of $15,000. For 1,000 advanced telecommuters, the cost per telecommuter is $50 in component costs, plus the server cost of $5, equals $55 per telecommuter, or a grand total of $55,000.

Since one server can handle about 1,000 telecommuters (although VPN server capacity varies widely), 1,100 telecommuters would necessarily require two tunnel servers. This scenario would present the employer with a total cost of $10,000, and a distributed cost of $9.09 per telecommuter for the server. For 1,100 advanced telecommuters, the additional cost per telecommuter would be $50. The server cost would be $9.09, resulting in a cost of $59.09 per telecommuter, or a grand total of $65,000. Five thousand telecommuters would require five tunnel servers for a total cost of $25,000, and a distributed cost of $5 per telecommuter. Thus, 5,000 advanced telecommuters would result in a per-client cost of $10 for components, and a $5 telecommuter cost, resulting in a total cost of $15 per telecommuter, or a grand total of $75,000.

---

visited July 9, 2001).

108. *See* Mike Fratto, *A Dizzying Array of VPN Choices*, NETWORK COMPUTING, *at* http://www.networkcomputing.com/1010/1010buyers3.html (May 17, 1999).

109. *See* Fratto, *supra* note 104.

Table 1
Cost of Implementing Tunnels for Internet Telecommuters

Number of Telecommuters	Basic Tunnel		Advanced Tunnel	
	Cost per Person	Total Cost	Cost per Person	Total Cost
1	$5,000	$5,000	$5,200	$5,200
10	$500	$5,000	$700	$7,000
100	$50	$5,000	$150	$15,000
1,000	$5	$5,000	$55	$55,000
1,100*	$9.09	$10,000	$59.09	$65,000
5,000	$5	$25,000	$15	$75,000
10,000	$5	$50,000	$15	$150,000

* Cost per telecommuter varies depending on the number of telecommuters. Typical price break points occur at even quantities. The quantity 1,100 is included here to demonstrate the importance of calculating the numbers using specific values.

3. Individual Firewalls

Another option is to install a full firewall system, in addition to a VPN tunnel, at every Internet telecommuter's computer. Free or inexpensive firewall products such as ZoneAlarm[110] and BlackICE[111] provide basic firewall-like protection. Although these products may serve as a good starting point to increase security, they may not be the best choice for companies because using such products substantially increases user support costs. Additionally, due to limited manufacturer support, telecommuters may face costly challenges in configuring complicated features.

Alternatively, commercial-strength standalone firewall units such as Cisco's PIX[112] can be installed in front of each Internet telecommuter's computer. This approach would dramatically increase the security level, but would also increase the cost per telecommuter by many thousands of dollars, in addition to increasing user support costs.

---

110. *See* Zone Partners, *ZoneAlarm Pro*, *at* http://www.zonelabs.com/ (last visited July 9, 2001).

111. *See* Network ICE Corp., BlackICE Defender, *at* http://www.networkice.com/html/small_home_office.html (last visited July 9, 2001).

112. *See* Cisco Systems, Inc., PIX Firewall, *at* http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm (last visited July 10, 2001).

V. POTENTIAL LIABILITY FROM INSECURE INTERNET TELECOMMUTERS

If a third party is injured by a backdoor attack, an employer may be found liable under a variety of legal theories. This section discusses two basic theories under which an employer might be found liable — breach of contract and negligence. It also suggests ways that an employer may use to protect itself against such liability. Finally, the section considers whether, in protecting itself against liability, an employer should: (1) use basic measures such as firewalls to protect its internal network from backdoor attacks;[113] or (2) install more expensive methods of protection, such as advanced tunnels, on every telecommuter's computer.[114]

This article does not address the potential criminal and civil liability of the hacker who actually perpetrates the harm. In general, however, a hacker may be criminally liable under federal statutes such as the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Economic Espionage Act, and the National Stolen Property Act and under similar state criminal statutes. Depending on the circumstances of the attack, a hacker may face civil liability under state law based on various theories including fraud, misrepresentation, and breach of contract.[115]

A. Contractual Liability

A third party that is injured due to a company's using insecure Internet telecommuters could bring an action for breach of contract. In general, a contract action is based on an express written or oral agreement between two parties supported by adequate consideration.

For example, suppose a delivery company named "DeliverCo" hires a software development company named "SoftCo" to create a proprietary program for DeliverCo's scheduling needs. The two companies execute an agreement specifying the program to be created and the other details of their relationship. DeliverCo then supplies SoftCo with confidential and trade secret information for the program specifications. An Internet telecommuter employed by SoftCo

---

113. *See* David L. Gripman, *The Doors are Locked but the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167 (1997); *see generally* Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167 (1990).

114. *See* Andrew M. Reidy, *Home Work Problems: Employers Must Address Liabilities of Telecommuting*, ABA JOURNAL, Jan. 2000, at 70.

115. *See* Robin A. Brooks, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?*, 17 REV. LITIG. 343 (1998).

begins work on the program using his home computer. Using a backdoor attack, a hacker successfully gains access to SoftCo's network, steals DeliverCo's confidential and trade secret information, and shares the information with a DeliverCo competitor. Depending on the terms of the original contract with SoftCo, DeliverCo may be able to sue for breach of contract.

The following sections describe remedies for breach of contract and protective terms and conditions that could be negotiated into a contract.

1. Remedies for Breach of Contract

For breach of contract, plaintiffs may obtain monetary damages and, in some cases, specific performance; various contractual theories are available including reformation and rescission.[116] On contract claims, plaintiffs may recover actual, but not punitive, damages. Thus, recovery is typically limited to compensation for direct economic harm resulting from a backdoor attack.[117]

In most contractual relationships, damages are limited by negotiation and by legal precedent to those resulting directly from breach.[118] For example, contractual damages might include the engineering and programming costs associated with replacing a piece of software damaged in the attack and the decrease in value of the formerly secret information. The client's lost profits, however, would be considered consequential damages, which are more difficult to prove and thus are less likely to be recoverable.[119]

Still, consequential damages — if not disallowed in the contract — can be recovered if a reasonable person would have foreseen the consequential damages at the time of contract formation.[120] An injured client in this situation can argue that backdoor attacks and the resulting harm are specifically foreseeable in light of the recent attacks on Microsoft[121] and the obvious threat of invasion by computer hackers.[122]

---

116. RESTATEMENT (SECOND) OF CONTRACTS §§ 347-377 (1981).

117. *See* Vitex Mfg. Corp. v. Caribtex Corp., 377 F.2d 795, 799 (3d Cir. 1967).

118. ALAN S. GUTTERMAN, CORPORATE COUNSEL'S GUIDE TO TECHNOLOGY TRANSACTIONS § 126.201 (1999).

119. *Id.*

120. RESTATEMENT (SECOND) OF CONTRACTS § 351 cmt. A, illus. 5 (1981).

121. Bridis, *supra* note 3, at A3; *see also* Vijayan, et al., *supra* note 3.

122. *See* Havenick v. Network Express, Inc., 981 F. Supp. 480, 504 (E.D. Mich. 1997) (quoting a Pacific Bell engineer who stated that the "biggest issues with telecommuting are speed and security").

2. Protective Provisions in Contracts

a. Confidentiality and Nondisclosure Provisions

A confidentiality provision is critical to an agreement in which one of the parties employs Internet telecommuters. Such a provision defines the permissible use of and protective measures for confidential information. For example, such a provision might read as follows:

> Each Party agrees: (i) not to use, disseminate, or in any way make available the other Party's Confidential Information, except to the extent necessary for the performance of this Agreement; and (ii) to treat all Confidential Information of the other Party with the same degree of care as it accords its own Confidential Information. Each Party represents that it exercises at least a reasonable standard of care to protect its own Confidential Information.[123]

This particular provision creates a mutual obligation upon the parties to exercise, at the very least, commercially reasonable care in dealing with the other party's information. Thus, an actionable breach of contract might occur if one party allowed the other party's information to be obtained by a backdoor attack through an unreasonably insecure Internet telecommuting connection. In such a case, the issue of breach would be resolved through a factual inquiry into whether advanced, basic, or no VPN tunnel protection would be commercially reasonable under the specific circumstances.

Industry custom often serves as a starting point in identifying commercial reasonableness.[124] If industry custom is to use advanced tunnels for all telecommuters, a company that has followed this custom would be less vulnerable to liability under a confidentiality provision imposing a duty of commercial reasonableness. In contrast to the past practice of not providing any protection for their telecommuters' computers, employers are increasingly spending the money to provide advanced VPN security for these computers.[125]

b. Express Warranties

A client that entrusts valuable information to a company would benefit from including in the written contract an express warranty clause. Such a clause might be drafted as follows:

---

123. *See* GUTTERMAN, *supra* note 118, § 102.001.

124. *See* RESTATEMENT (SECOND) OF CONTRACTS § 205 (1981).

125. *See* Bridis, *supra* note 3, at A3

> Company covenants, represents, and warrants that it will exercise due professional care and competence in the performance of its obligations herein, including but not limited to, in the protection of Client's information.[126]

Such a warranty imposes on the company a high standard to protect against backdoor attacks.

c. Express Limits on Liability

Parties may also negotiate and agree on express limits on their liabilities for breach of contract. For example, a software developer might include the following provision:

> In no event will Developer be liable to Client for lost profits, special damages, or consequential damages. Developer's total liability to Client for damage, costs, and expenses will not exceed the fees actually paid by Client under this Agreement.[127]

This provision creates a cap on potential liability as well as a limit on the types of damages that may be sought.[128]

A client, however, must weigh the risks and benefits of using a service provider that insists on limiting its liability in this way. If the client intends to share valuable confidential information and knows that the service provider uses insecure Internet telecommuting connections, then the risk may be intolerable.

d. Liquidated Damages

If, at the time of contract formation, the possible damages resulting from a breach are difficult to ascertain, the parties may decide to specify the amount of liquidated damages to be awarded for a breach. The following provision is an example of a liquidated-damages clause:

> Both Parties hereby agree that: (i) the resulting injuries from a breach of this Agreement are not readily identifiable; and (ii) the amount of liability for breach of this Agreement will be one hundred thousand dollars ($100,000).[129]

---

126. *See* GUTTERMAN, *supra* note 118, § 2.120.

127. *See id.* § 126.201.

128. *See* RESTATEMENT (SECOND) OF CONTRACTS § 347 (1981).

129. GUTTERMAN, *supra* note 118, § 115.001.

When a client suffers harm from a backdoor attack to a company with an insecure Internet telecommuting connection, such a provision may provide relief. But courts typically uphold such provisions only if the amount specified was a reasonable forecast of the actual resulting damages.[130]

In the example above, then, if the actual injury is $10,000, the provision probably would not be enforced because the forecasted amount was an order of magnitude different from the actual damages, and not a reasonable forecast of them. Consequently, the client would have to seek and prove actual, instead of liquidated, damages.[131] If, however, the specified amount is reasonably close to the actual damages, the specified amount will probably be awarded.[132]

In Internet telecommuting, the injury resulting from a backdoor attack can vary greatly. It is difficult, therefore, to draft a liquidated-damages clause that will later be viewed by a court as a reasonable forecast of actual damages.

e. Force Majeure

The parties may also agree to include a provision that excuses performance under extreme, unavoidable circumstances. For example:

> Each Party will be excused from default or delay in the performance of its contractual obligations if the default or delay is caused by fire, flood, earthquake, elements of nature, acts of God, wars, riots, civil disorders, rebellions, revolutions, or any other similar cause beyond the reasonable control of the Party.[133]

This provision excuses only unforeseeable events that are beyond a party's reasonable control.[134] Since a backdoor attack, however, is foreseeable in today's business world and is not beyond a company's reasonable control, a force majeure provision should not excuse default or breach from insecure telecommuters.

---

130. RESTATEMENT (SECOND) OF CONTRACTS § 351(3) (1981).

131. *See, e.g.*, Dave Gustafson & Co. v. State, 156 N.W.2d 185, 189 (S.D. 1968).

132. *See* Wasserman's Inc. v. Township of Middleton, 645 A.2d 100, 109 (N.J. 1994).

133. GUTTERMAN, *supra* note 118, at § 106.020.

134. RESTATEMENT (SECOND) OF CONTRACTS § 351 (1981); *see* Spang Indus., Inc. v. Aetna Cas. & Sur. Co., 512 F.2d 365, 369 (2d Cir. 1975) (quoting Leonard v. New York, Albany & Buffalo Electro-Magnetic Tel. Co., 41 N.Y. 544, 567 (1870)).

B. Tort Liability for Negligence

A client whose data or information is lost due to a backdoor attack may potentially bring a tort action for negligence. To succeed on such a claim, of course, the client would have to prove every element of such a claim under traditional negligence theory.

1. Remedies for Negligence

When a plaintiff establishes damages beyond those that are purely economic, then the injured party can recover all damages, including direct, consequential, special, past, present, and future damages.[135] Recovery may also include compensation for damaged personal property,[136] as well as punitive damages if the defendant's conduct is found willful or wanton.[137]

2. Elements of a Negligence Claim

a. Duty

The first element to be proved is that the defendant-company owed the plaintiff a duty of care.[138] This may be a significant hurdle if the plaintiff had no special relationship with the company, but was merely a consumer who voluntarily shared certain personal information that was later discovered by a hacker. Under these circumstances, a court would have to consider whether a company that maintains customer information and uses Internet telecommuters has a duty to protect that information from backdoor hackers.[139]

Under the well-known test of *Palsgraf v. Long Island Railroad Co.*,[140] a defendant owes a duty of reasonable care to persons within the foreseeable zone of danger created by the defendant's acts or omissions.[141] Under this analysis,

---

135. *See* DAN DOBBS, THE LAW OF REMEDIES § 5 (2d ed. 1993).

136. *See id.*

137. *See id.* § 3.11(1).

138. *See* PROSSER & KEETON ON TORTS §§ 30, 129 (5th ed. 1984).

139. *See* RESTATEMENT (SECOND) OF TORTS § 281 (1965).

140. *See* Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 99 (1928).

141. *Id.* Palsgraf stood 30 feet away from an employee of the railroad. While assisting another passenger onto a train, the employee caused the passenger to drop a bag containing fireworks. The fireworks ignited, causing a scale to fall on Palsgraf. Judge Cardozo found that the employee owed a duty of care to the passenger since the passenger was in the foreseeable zone of danger. Since Palsgraf was not in the foreseeable zone of danger, however, the employee did

an injured plaintiff would argue that a company using Internet telecommuters owes a duty of care to any party when it is foreseeable that the party's information is susceptible to a backdoor attack. Risks from backdoor attacks to companies using Internet telecommuters are a primary concern today and have been a foreseeable problem since at least 1997.[142]

Based on an analogy to premises liability, companies should be found to owe a duty to those whose data they store. In particular, a company employing telecommuters owes a duty to protect another party's information when insecure Internet telecommuters constitute a hazardous situation that is or should have been clear to the company.[143] This proposed duty is analogous to a property or business owner's duty of care to ensure that its common or business areas are in a safe condition.[144]

Traditional premises liability actions can arise, for example, when a third party commits a crime that injures a person who is rightfully in a common area that the owner has a duty to keep safe.[145] In such an area, it is assumed that the owner has taken reasonable steps to make the premises safe.[146] Liability is more likely if the owner knew of previous crimes in the common area and thus recognized the likelihood of future crimes, but took no steps to prevent them.[147]

A similar type of liability may arise in slip-and-fall cases.[148] Although the injured party is merely an invitee — such as a customer shopping in a store — the law imposes on the owner a duty to inspect the premises periodically to discover any hazardous condition and to protect against foreseeable injuries.[149]

---

not owe her a duty of care. Conversely though, a minority of jurisdictions follow Judge Andrews's dissent in *Palsgraf*. Under that view, the employee did owe Palsgraf a duty of care since her harm was causally connected to the employee's conduct.

142. *See, e.g.*, Havenick, 981 F. Supp. at 504 (quoting a Pacific Bell engineer who stated that the "biggest issues with telecommuting are speed and security").

143. *Cf.* RESTATEMENT (SECOND) OF TORTS § 343A (1965) (addressing landowner liability to invitees when dangers on property are open and obvious).

144. RESTATEMENT (SECOND) OF TORTS § 344 (1965).

145. *See* Kline v. 1500 Mass. Ave. Apt. Corp., 439 F.2d 477, 484 (1970); *see also* Ryals v. U.S. Steel Corp., 562 So. 2d 192, 194 (Ala. 1990).

146. *See* Doe v. Dominion Bank of Wash., 963 F.2d 1552, 1560 (D.C. Cir. 1992); *see also* Tillman v. Great Lakes Steel Corp., 17 F. Supp. 2d 672, 679 (E.D. Mich. 1998).

147. *See* Lay v. Dworman, 732 P.2d 455, 457 (Okla. 1986).

148. *See* PROSSER & KEETON ON TORTS § 61 (5th ed. 1984).

149. *See* RESTATEMENT (SECOND) OF TORTS §§ 333-338 (1965).

A duty like that arising from premises ownership should be imposed on companies that use Internet telecommuters.[150] Backdoor attacks occur in what might be thought of as "common areas" owned by the company. Although the harm is to intangible property rather than to a person, this distinction should not justify less protection.

A property owner owes a duty of reasonable care to eliminate hazardous conditions about which it knows or should have known. Business conducted with Internet telecommuters is similar to business involving common areas and traditional storefronts. Because Internet risks are widely known, a company knows or should know of the risk of backdoor attacks on Internet telecommuting connections. Therefore, a company should assume that it owes a duty to implement proper security measures for Internet telecommuters, thus protecting those within its "common areas" from the risk of backdoor attacks.[151]

The property analogy does not work as naturally for businesses that do not require as much physical space as do more traditional companies. For example, many new consulting firms dispatch their consultants to the client site and have an Internet presence only to handle internal business.[152] Here, the client should nevertheless be legally treated as business invitees. For example, Internet service providers (ISPs) sell Internet access services in an almost completely electronic environment. Subscribers sign up for the service online without ever having to set foot inside an ISP's office. Only a few square feet of physical space are needed to house the ISP's equipment. While subscribers do not physically go to the ISP's office, their interactions with the ISP are the same as those with traditional businesses, thus making the subscribers similar to business invitees.

A duty also exists when the company creates a peril by using insecure Internet telecommuting connections. Although there is generally no duty to act, a duty is created when the company itself creates an unreasonable risk to third-party information.[153]

---

150. *See* Gellerman v. Shawan Rd. Hotel Ltd. Partnership, 5 F. Supp. 2d 351, 353 (D. Md. 1998).

151. *See* Helene R. Stewart, *Out of Sight, Out of Mind? The Legal Issues in Telecommuting for Your Business Client*, 6 BUS. L. TODAY 48, 51 (1996).

152. *See* Hasbro Inc. v. Clue Computing Inc., 994 F. Supp. 34, 38 (D. Mass. 1997) (noting that on its website, Clue describes itself as "a completely virtual company" and adds that "the employees telecommute or work at client sites").

153. *Cf.* Brown v. Wal-Mart Stores, Inc., 976 F. Supp. 729, 734 (W.D. Tenn. 1997); *see also* RESTATEMENT (SECOND) OF TORTS § 308 (1964) (addressing the negligence standard when an actor allows a third party to use "a thing" that is controlled by the actor); RESTATEMENT (SECOND) OF TORTS § 289 (1964) (describing the standard of reasonable conduct when an actor's conduct might cause "an invasion of another's interest").

b. Standard of Care

A plaintiff alleging negligence must also identify the standard of care that a defendant should have met in protecting the plaintiff's information.[154] A company should exercise reasonable care in most cases to protect information.[155] But if "reasonable care" is the standard, what must a company do to offer its clients reasonable protection from backdoor attacks on telecommuting connections?

(1) Industry custom is not determinative.

In *The T.J. Hooper*,[156] Judge Learned Hand rejected the notion that industry custom established the standard of reasonable care. There, two tugboats continued pulling two barges in a severe storm, ultimately losing the barges and their cargo at sea. The barge and cargo owners sued the owner of the tugboats. The claimants alleged that the tug owner had breached the standard of reasonable care by failing to equip the tugboats with radios that would have warned of the storm in time for the tug masters to seek shelter. At the time of the accident, most tugboats were not equipped with radios, even though radios were readily available. The court held that customary practice in an industry is not conclusive in establishing the standard of care.[157] According to the court, the minimum standard of care required that tugboats be equipped with radios, regardless of industry custom.[158]

Internet telecommuters without adequate security precautions are like the tugboats without radios in *The T.J. Hooper*. Although the industry norm may be to use only basic tunnels, this level of protection is not sufficient for all situations. Rather, the standard of care is the conduct a reasonable company would have followed to protect a client's information. For example, reasonable conduct might require: (1) installing firewalls wherever the company network connects to the Internet; (2) using encryption;[159] (3) regularly monitoring the network for any security breaches; and (4) documenting, publishing, and

---

154. *See* PROSSER & KEETON ON TORTS §§ 29-30 (5th ed. 1984).

155. *See* RESTATEMENT (SECOND) OF TORTS § 283 (1965).

156. *See* The T.J. Hooper, 60 F.2d 737 (2d Cir. 1932).

157. *See id.* at 740; *see also* Gripman, *supra* note 113, at 179-80 (noting, however, that industry custom may be admissible to help determine the feasibility of a particular preventive measure).

158. *See* RESTATEMENT (SECOND) OF TORTS § 295A (1965).

159. *See* Rustad & Eisenschmidt, *supra* note 28, at 230.

enforcing a security policy.[160] Thus, even if a defendant could show that the industry custom was to have minimal security, that custom would not be determinative of the standard of reasonable care.

(2) Risk-utility analysis can set the standard of care.

If industry custom is not determinative of the standard of care, how should the standard be defined? One answer comes from the risk-utility analysis of the Second Circuit in *Carroll Towing*.[161] There, a barge sank at night, when no crewmember was stationed onboard. Carroll Towing argued that an onboard crewmember might have prevented some of the damage. In the analysis of negligence, the court used a four-step economic risk-utility formula to quantify reasonable conduct.[162]

The first step is to identify the amount of potential damage (the liability) and the percent chance that the damage will occur (the probability). The second step is to determine the risk of harm by multiplying the liability and the probability. The third step is to identify the burden, which is the cost of reasonable precautions adequate to prevent the damage from occurring. The fourth step is to identify the standard of care by comparing the risk of harm to the burden of precautions.

If the risk of harm is less than the burden to avoid that risk, then the standard of care does not require an investment in the precautions. Conversely, if the risk of harm is greater than the burden, the standard of care requires an investment in the precautions. The court stated this analysis succinctly, in algebraic terms: "if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B is less than PL."[163]

This risk-utility analysis reflects the public-policy concept that precautions should not cost more than the harm they are intended to prevent.[164] This risk-utility analysis will be used later in this article to identify the standard of care a company should use to protect Internet telecommuting connections from backdoor attacks.

---

160. *See* Gripman, *supra* note 113, at 184.

161. *U.S. v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947).

162. *See id.; see also* RESTATEMENT (SECOND) OF TORTS §§ 292, 293 (1965).

163. *Carroll Towing Co.*, 159 F.2d at 173.

164. *See* Richard Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29 (1972), *cited in* DAN B. DOBBS, TORTS AND COMPENSATION 160 (2d ed. 1993); Rustad & Eisenschmidt, *supra* note 28, at 248.

(3) No professional standard of care applies here.

To hold a company to a higher professional standard of care,[165] a client must establish several elements including minimum educational requirements, a certification process, and a disciplinary procedure. Further, the client must prove that the company held itself out as a professional organization.[166]

It is difficult to define a professional standard of care in the information-technology community because there are no minimum entrance requirements.[167] Just about anyone can claim to be a computer professional. Although several technical bodies offer certification through examination,[168] companies that hire computer personnel are under no obligation to require certification.

Even if a client could show that the company should be held to a higher professional standard of care, the objective standard requires that the company possess the knowledge and exercise the skill of an ordinary member of the profession.[169] Put simply, the standard is set by what an ordinary company would do in a same or similar circumstance.[170] Since the industry standard for telecommuters is one of supplying only basic tunnel protection, an ordinary company would provide basic tunnels. Thus, the professional standard of care would not impose on a company the duty to provide any greater protection against backdoor attacks.

c. Breach of the Standard of Care

The third element a plaintiff must show is that the company breached the applicable standard of care.[171] To show a breach of the general standard of

---

165. *See* RESTATEMENT (SECOND) OF TORTS § 299A (1965).

166. *See* Hosp. Computer Sys., Inc. v. The Staten Island Hosp., 788 F. Supp. 1351, 1361 (D. N.J. 1992), (citing Lincoln Rochester Trust Co. v. Freeman, 311 N.E.2d 480 (1974)).

167. *See* Rustad & Eisenschmidt, *supra* note 28, at 249.

168. Cisco Sys., Inc., *Cisco Certified Internetwork Expert (CCIE), at* http://www.cisco.com/warp/public/625/ccie/ (last visited July 10, 2001; Microsoft Corp., *Microsoft Certified Professional (MCP, at* http://www.microsoft.com/trainingandservices/redirect/mcp.htm (last visited July 10, 2001); and Novell, Inc., *Certified Novell Engineer (CNE), at* http://www.novell.com/education/certinfo/cne (last visited July 10, 2001).

169. *See* RESTATEMENT (SECOND) OF TORTS § 299A (1965).

170. *See* Heath v. Swift Wings, Inc., 252 S.E.2d 526, 529 (N.C. App. 1979).

171. *See* PROSSER & KEETON ON TORTS §§ 29-30 (5th ed. 1984).

reasonableness, the plaintiff might assert various factual theories.[172] For example, the plaintiff might argue, among other things, that the corporation had negligently:

(1) failed to install adequate security measures, such as firewalls and encryption;

(2) failed to recognize problems with its security measures;

(3) failed to run anti-virus programs;[173]

(4) failed to properly train and supervise its employees; or

(5) failed to adequately prevent unauthorized access.[174]

For a quantitative breach analysis, the risk-utility analysis can be applied to the Internet telecommuting environment. Analysis is conducted on a per-telecommuter basis because this example presupposes a successful backdoor attack ultimately coming through one telecommuter. If backdoor attacks occurred through more than one telecommuter, the probabilities and risks would need to be adjusted for those facts.

The following hypothetical risk-utility analyses use the 0.0000715 national average as the probability of a successful backdoor attack. As before, any actual analysis would require fact-specific values.

The amount of the company's liability, in the event of a successful hacker attack, depends on the value of the client's information. Suppose that a client's trade secrets are valued at $50,000. The probability that a hacker could successfully access the company's internal network with a backdoor attack through a telecommuter's computer was previously identified as 0.0000715 per telecommuter. The risk of harm to the client's information for each telecommuter is the product of the liability ($50,000) and the probability (0.0000715), which equals $3.58 per telecommuter. The cost to the company of installing a basic tunnel depends on the number of telecommuters. As previously explained, for 1,000 telecommuters the cost is $5 per telecommuter.[175] Because

---

172. *See* RESTATEMENT (SECOND) OF TORTS §§ 281, 298 (1965).

173. *See* Robin A. Brooks, *supra* note 115, at 343.

174. *See* Gripman, *supra* note 113, at 184.

175. The burden is computed per telecommuter, rather than cumulatively for all telecommuters, because each telecommuter is a point of potential vulnerability. In other words, every telecommuter's computer could be compromised, and each computer could be an avenue of liability for the employer. Also, the cost of Internet access has not been included in the burden

the risk of harm to the client ($3.58) is less than the burden on the company to preclude that harm ($5), the company *would not* have to install even basic tunnels to avoid breaching its standard of care.[176]

A small increase in the value of the client's information, however, produces a different result. If the company's potential liability is raised to $75,000, while the probability of a successful backdoor attack remains at 0.0000715, the risk of harm rises to $5.36. The company's burden remains at $5 per telecommuter to install basic tunnels on 1,000 telecommuters. The risk of harm to the client ($5.36) is greater than the burden on the company of preventing that harm ($5). Here, the company would breach its standard of care if it failed to install basic tunnels.[177]

If the company's potential liability is raised to $500,000, while the probability of a successful backdoor attack remains at 0.0000715, the risk of harm rises to $35.75. The company's burden to supply basic tunnels to 1,000 telecommuters is $5, while the burden to supply advanced tunnels to 1000 telecommuters is $55. With these variables, the risk of harm to the client ($35.75) is greater than the burden of supplying basic tunnels ($5), but less than the burden of supplying advanced tunnels ($55). Thus, to satisfy its standard, the company would still be required only to install basic tunnels.[178]

The outcome changes as the value of the information increases. For example, if the company's potential liability is raised to $1,000,000, while the probability of a successful backdoor attack remains at 0.0000715, the risk of harm rises to $71.50. The company's burden to supply basic tunnels to 1,000 telecommuters is $5, while the burden to supply advanced tunnels to 1,000 telecommuters is $55. Using these variables, the company would be expected to install advanced tunnels because the risk of harm to the client exceeds the cost of using the more expensive precautions.[179] If the company failed to install advanced tunnels, it would breach the applicable standard of care under this analysis.

---

to protect against risk to the client's information because the telecommuter is expected to have an Internet connection, whether or not tunneling services are provided.

176. *See* U.S. v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

177. *See id.*

178. *See id.*

179. *See id.*

d. Causation

The fourth element that a plaintiff must show is that the company's breach caused the plaintiff's injury.[180] Causation, which includes actual cause and proximate cause, is the element that connects breach to injuries.[181] The causal connection must be direct enough to show that the alleged negligent conduct caused the injury.[182]

In a tort action involving an Internet telecommuting connection, a client would have to show that the company's failure to install adequate security measures caused the client's injury. A client could establish such a causal link by proving that the hacker compromised the telecommuter's computer because of inadequate security measures and then used the computer to gain access to the client's information stored on the corporation's internal network.

(1) Actual Cause

The client must show that the corporation's conduct actually caused the injury. This actual cause, or cause in fact, means that but for the conduct of the corporation, the client would not have suffered harm. If the client would have suffered harm regardless of the company's negligence, then cause in fact cannot be established.[183] On the other hand, if the company could have prevented the harm by using adequate security precautions, cause in fact would be satisfied.

The client would also have to prove that the hacker actually came through a telecommuter's computer. The log of network activity commonly kept by a company's network administration staff could be a crucial piece of evidence for the client. This activity log is an electronic file that keeps track of network traffic. A log file can also be configured to identify communications between specific computers. In other words, the log would indicate whether the telecommuter's computer accessed the client's information.

For the company, a log file may provide both helpful and harmful evidence. On one hand, a company may need to keep a log file to show that it met the applicable standard of care for clients.[184] On the other hand, a plaintiff could use the same log file to prove cause in fact by showing that the hacker came in through the telecommuter's computer.

---

180. *See* PROSSER & KEETON ON TORTS §§ 29-30 (5th ed. 1984).

181. *See* RESTATEMENT (SECOND) OF TORTS § 281 (1965).

182. *See id.* § 328A.

183. *See* Perkins v. Texas & New Orleans R.R., 147 So. 2d 646, 648 (La. 1962).

184. *See*. David J. Loundy, *E-LAW 4: Computer Information Systems Law and System Operator Liability*, 21 SEATTLE U. L. REV. 1075 (1998), *available at* http://www.Loundy.com/E-LAW/E-Law4-full.html (last visited July 9, 2001).

(2) Proximate Cause — Foreseeability

A plaintiff must also show that the injury was a foreseeable consequence of the company's conduct. If the injury was too remote to be foreseeable, or was not a natural consequence of the corporation's conduct, the corporation's conduct will not be found to have proximately caused the client's injuries.[185] Certain consequences of hacker attacks are foreseeable, while others are not.

The foreseeability of hacker attack raises several questions. How foreseeable was it that the hacker would access this client's information through the telecommuter's computer? If it was foreseeable, were the client's injuries a natural consequence of the breach?

The defendant company may argue that the hacker's criminal conduct was an intervening event that broke the causal connection between the corporation's breach and the client's injuries. This argument generally prevails when the torts or crimes of third parties are not foreseeable. But when the specific torts or crimes of third parties are foreseeable, the third party's conduct will not constitute an intervening event.[186]

With telecommuting over the Internet, a hacker's torts or crimes are specifically foreseeable, so they almost certainly will not be considered an intervening event.

e. Injury

The fifth and final element that must be shown is that the client suffered actual injury as a result of the corporation's conduct.[187] The client must demonstrate that hacker access to the client's information resulted in a loss. Unlike a plaintiff in a contract action, a plaintiff in a negligence action could claim the engineering cost required to repair the damage, lost revenue, market share, trade secret, good will, reputation, or other business-related or economic losses.[188]

A critical component in such an action for negligence requires showing more than economic injury, even if economic injuries amounted to millions of dollars in harm.[189] In particular, a plaintiff has to show personal injury or damage to property. A plaintiff might thus be without a tort remedy if all the harm is economic. In some situations, however, there may be property damage.

---

185. *See* Palsgraf v. Long Island R.R., 162 N.E. 99 (N.Y. 1928).

186. *See* Russo v. Baxter Healthcare Corp., 140 F.3d 6 (1st Cir. 1998).

187. *See* PROSSER & KEETON ON TORTS §§ 29-30 (5th ed. 1984).

188. *See* Gripman, *supra* note 113, at 182.

189. *See* Patrick J. Miyaki, *Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?*, 8 SANTA CLARA COMPUTER & HIGH. TECH. L.J. 121, 137 (1992).

For example, in a backdoor attack through Internet telecommuting connections, there may be damage to data, information, or software — all of which are property — might be considered damage to property and be compensable.

Individual plaintiffs may also suffer compensable injuries based on the hacker's invasion of their privacy or resulting disclosure of confidential information. This might occur if a hacker obtained private information, such as a police record, and revealed it to the general public, resulting in a loss of reputation. The law on whether disclosure of true but private information creates a claim varies from state to state and also implicates free speech issues.

3. Possible Defenses to Negligence

A defendant could attempt to raise the defense of comparative negligence. Such a defense requires the defendant to show that the plaintiff's own negligence objectively contributed to the injury.[190] But such a defense seems unlikely in this context unless the plaintiff had access to the defendant's system and somehow created the risk that resulted in the backdoor attack.

Assumption of the risk is a defense that no longer exists under the law of some states. If the defense is viable, however, it provides a complete defense if the plaintiff subjectively knew and appreciated the risk, and still voluntarily chose to encounter it.[191] This defense might apply, for example, if the plaintiff knew and appreciated that the defendant's Internet telecommuters were insecure, and nevertheless voluntarily chose to encounter the risk of a backdoor attack.

VI. CONCLUSION

Internet telecommuters may provide modern organizations with important benefits. But companies must not ignore the risks that this practice creates to third-party information. Hackers can compromise the computers of Internet telecommuters and then use those connections to circumvent security measures and access internal networks. Once inside, a hacker may steal or destroy confidential and proprietary information of a company's clients and customers.

Internet telecommuters without adequate security are like the tugboats without radios in *The T.J. Hooper* case. Although industry custom may be to use only basic VPN tunnels to protect Internet telecommuters, more costly and more advanced VPN tunnels may ultimately be found necessary to meet the standard of care. If adequate precautions are not taken, a company may face significant liability in contract or tort for resulting injuries to third parties.

---

190. *See* McIntyre v. Balentine, 833 S.W.2d 52, 57 (Tenn. 1992).

191. *See* Walk v. Starkey Mach., Inc. 180 F.3d 937, 939 (8th Cir. 1999).

To address the risk of backdoor attacks, companies using Internet telecommuters should analyze their security measures. Security precautions should then be implemented to provide protection proportionate to the value of information to which the telecommuters have access. If Internet telecommuters do not have adequate protection, then their employer should invest in products that provide appropriate VPN, encryption, and firewall security.

Using only a small part of the costs saved through Internet telecommuting, a company can typically implement security measures that will protect valuable third-party information from backdoor attacks. With legal standards still uncertain and hacker attacks commonplace, such an investment in security may ultimately save a company millions of dollars in liability, while preserving its reputation and goodwill.