UIC John Marshall Journal of Information Technology & Privacy Law

Volume 16
Issue 1 *Journal of Computer & Information Law - Fall 1997*

Article 7

Fall 1997

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)

David L. Gripman

Recommended Citation

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)

https://repository.law.uic.edu/jitpl/vol16/iss1/7

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

I. INTRODUCTION

> Twas the [night] before Christmas, and the employees of XYZ Corp. were logging off a successful year with holiday parties at company headquarters in New York City. Meanwhile, inside their locked, darkened offices, not a creature was stirring, not even a computer mouse—or so they thought. Unbeknownst to the merrymakers, a team of professional hackers in Texas [from WheelGroup Corporation] was preparing to invade XYZ's [computer] systems from 1,600 miles away.[1]

A few months earlier, an executive from WheelGroup had boasted to *Fortune Magazine* that they had yet to find a network they could not penetrate electronically.[2] "It's really very easy to do . . . . If it's a big network, it may take us an evening. Otherwise it may take two hours,"[3] the executive boasted. *Fortune* took this boast as a challenge and found

[1] Richard Behar, *Who's Reading Your E-mail?*, FORTUNE, Feb. 3, 1997, at 57. This scenario is based on a true story. *Id.* XYZ Corporation is a fictitious name as the real Fortune 500 corporation requested anonymity. *Id.* at 58. The hackers in this story are from WheelGroup Corp., a San Antonio computer security firm that conducts "external assignments" as a diagnostic service for clients. *Id.* at 57.

[2] Behar, *supra* note 1, at 57-58.

[3] Behar, *supra* note 1, at 58. For further illustration, *see Noted & Notorious Hacker Feats*, BYTE, Sept. 1995, at 151. On February 15, 1995, the FBI finally arrested Kevin D. Mitnick, who had been on the run since 1992. *Id.* In 1989, Mitnick was convicted and sentenced to three years probation for breaking into Digital Equipment Corporation's computer network system and stealing its software. *Id.* Since his 1989 conviction, Mitnick has allegedly broken into a California motor vehicles database, stolen 20,000 credit card account numbers from an on-line service, gained control of New York and California telephone switching hubs via modem, eavesdropped on telephone calls, mutated home telephones into quarter-demanding pay phones, and stored data that he had stolen from other networks. *Id.* Mitnick states, "I know the computer systems of the world are not as safe as they think . . . . Information is not safe. Only military computers are secure." *Mitnick Confesses: "No One is Secure!,"* DATAMATION, Jan. 15, 1996, at 8.

a respected "Fortune 500"[4] company willing to take on the challenge with WheelGroup.[5] This challenge was dubbed "Operation Nutcracker"[6]

[4] *The Fortune 500 Largest U.S. Corporations*, FORTUNE, Apr. 29, 1996, at F1. A company on this list is one of the 500 largest companies in the United States based on annual revenues. *Id.*

[5] Behar, *supra* note 1, at 58.

[6] Behar, *supra* note 1, at 57-61. This fascinating story is as follows: First, the hackers needed to find out how to link up with *XYZ*. *Id.* at 58. Fortunately, all they had to do was access via the Internet the Network Information Center ("NIC"), a public registry of all computer domain names. *Id.* If a company doesn't register its name there, legitimate visitors would have no way of reaching the company electronically. *Id.* Second, the hackers accessed another public registry, Domain Name Service (DNS), which provides more specific information on subnets within each domain, and e-mail (electronic mail) gateways for a company's messages. *Id.*

At 1:10 a.m., of the first day, now having individual targets, WheelGroup began "bouncing" some e-mail. *Id.* at 59. The U.S. Postal Service, when unable to deliver a letter, postmarks the letter so as to mark the journey of the letter—e-mail is handled in the same way. *Id.* Thus, when WheelGroup sent an e-mail to an *XYZ* employee in New York, the message "bounced back" because of the purposeful misspelling of the sender's name. *Id.* The hackers discovered there was only one hop between the employee's computer and *XYZ*'s gateway. *Id.* If they cracked the gateway, they would gain access to *XYZ*'s network. *Id.*

At 2:02 a.m., the hackers began "pinging," which is using a software program to send an electronic beam to every *XYZ* address to see which machines are alive. *Id.*

At 2:17 a.m., the hackers discovered a firewall, which is the software that *XYZ* uses to ward off hackers. *Id.* For three hours they attempted to penetrate the network to no avail. *Id.*

At 5:00 a.m., WheelGroup decided to forego the Internet and instead attack *XYZ*'s individual computers by a method called "war dialing," which meant automatically dialing thousands of phone numbers within a specific range (close to *XYZ*'s main phone number). *Id.* The hackers downloaded a free Internet hacker program called "ToneLoc" which performed the "war dialing" on one phone line and one computer for the next 16 hours. *Id.*

At 9:13 p.m., the hackers found that upon returning to the operating room, "ToneLoc" had found 55 modems at *XYZ*. *Id.* In two hours, the hackers accessed a fax server at one of *XYZ*'s subsidiaries. *Id.* They cracked the passcode resulting in their ability to access a dial-out line, which allowed them to place long-distance calls anywhere in the country. *Id.* at 60. They were now able to use *XYZ*'s computers to hack into other companies' computers leaving *XYZ* to take the blame. *Id.* The hackers then accessed an *XYZ* computer near Washington, D.C. and assumed control "to issue purchase orders, review lists of vendors and products, and even set currency exchange rates for international sales." *Id.*

At 12:01 a.m., of the second day, WheelGroup accessed another computer located in *XYZ*'s tax department at *XYZ*'s headquarters and gained full "root" power which meant they could destroy all of the computer's data or leave a virus to infect the network. *Id.* at 60-61.

At 2:02 a.m., The hackers obtained root access to four computers in *XYZ*'s technology department. *Id.* at 61. If they were real intruders, they would install "sniffer" software, a network traffic analyzer that captures account names and passwords as they travel the network during business hours. *Id.* Then the hackers would have the information they needed to travel from department to department. *Id.* Operation Nutcracker ended with a final trick on *XYZ*: "E-mail spoofing." *Id.* The hackers sent a bogus e-mail to the *XYZ* executive who approved of *Fortune's* experiment, proposing a $5,000 bonus to the employee and originated in Texas, 1,600 miles away from *XYZ*'s headquarters in New York.[7] Operation Nutcracker extended over a two day period, and within that time the hackers infiltrated seven of *XYZ*'s computers.[8] They penetrated a subsidiary near Washington, D.C., and the corporate tax division in Manhattan.[9] They achieved "root access"[10] on five systems, hence enjoying the same capabilities as members of *XYZ* corporation. Moreover, the hackers accessed computers used exclusively by *XYZ*'s technology department.[11] Operation Nutcracker demonstrates that while current security systems are very sophisticated, a hacker only needs access to one remote computer (major corporations usually have thousands all over the country and the world) to wreak havoc on a company's finances and operations or to have a springboard[12] to harm another company's computers or to steal its assets.[13] The business losses can be staggering, as MCI discovered when hackers downloaded more than 50,000 credit card numbers which were used to make more than

who planned the project. *Id.* The hackers disguised the e-mail to look like it came from one of the executive's managers. *Id.* The executive responded to the surprised manager with an, "Okay, fine." *Id.* WheelGroup could have intercepted the message without the manager's knowledge, but this was unnecessary as their point was already proven. *Id.* A final note, Nutcracker went undetected the entire time. *Id.* at 57.

[7] Behar, *supra* note 1, at 57.

[8] Behar, *supra* note 1, at 57.

[9] Behar, *supra* note 1, at 57.

[10] Behar, *supra* note 1, at 57. "Root access" means having the same power over a networked computer system as a system administrator (a person who operates and maintains the computer network). *Id.*

[11] Behar, *supra* note 1, at 57.

[12] Behar, *supra* note 1, at 58. A springboard is "anything serving as the starting point or providing the impetus for something else." WEBSTER'S NEW WORLD DICTIONARY 1298 (3rd ed. 1989). "A hacker, exploiting your somewhat lax security practices, breaks into your network and launches attacks on other sites, using the guise of being a member of your network as his or her access key." Aileen Crowley, *In the Eyes of the Law: New Legal Risks can Make Companies Accountable for Hackers' Rude Intrusions*, PC WK., June 17, 1996, at E1. For example, Boeing reported an attack on its supercomputer center in Seattle. David Bicknell, *How to Avoid Getting Snared by the Net*, COMPUTER WKLY., Nov. 16, 1995, at 20. Boeing was used as a "springboard" site to launch an attack on the local federal district court system. *Id.* Judges' rulings were altered and the local system administrator had no clue the attacks took place. *Id.*

[13] Kate Button, *Hacking Off The Hackers: Problems with Hackers in the U.S. and the FBI's Plan to Catch Them*, COMPUTER WKLY., Jan. 16, 1997, at 40. Russian hackers electronically pierced Citibank's secured computer network and stole approximately $12 million. *Id.* Ultimately, the FBI apprehended the hackers and all but $400,000 was recovered. *Id.* "What the Citibank story brings out is that even the most sophisticated and secure organizations [sic] (and Citibank is certainly one of them) are facing some serious risks when it comes to electronic commerce" says security policy expert, Charles Cresson Wood of Baseline Software in Sausalito, California. *Id.*

$50 million in charges and purchases.[14]

Any corporation connected to the Internet is vulnerable to hacker intrusions because the Internet is accessed by millions of people.[15] To make matters worse, the information on how to infiltrate a corporation is freely available on the Internet.[16] A hacker can cause a plethora of problems ranging from infecting a computer network with a virus[17] to intentionally shutting down a corporation's computer systems so that the corporation cannot distribute its products.[18] In addition to severe business losses, the service, repair, and restoration costs from hacker intru-

[14] Button, *supra* note 13, at 40. Tom Peltier, the corporate information protection coordinator for Detroit Edison Power Company, suggests that "because the risk of on-line crime is so great, there will be a mass exodus of corporate users of the Internet when they realize their vulnerability." *Id.* "According to federal law enforcement estimates, online thieves steal more than $10 billion worth of data in the United States annually." Clinton Wilder & Bob Violino, *Online Theft: Trade in Black-Market Data is a Growing Problem for Both Business and the Law*, INFORMATIONWEEK, Aug. 28, 1995, at 30. "Illegal data traded and sold online includes calling-card numbers from long-distance telephone service providers, cellular service activation codes, stolen credit-card numbers, . . . and . . . the bounty also includes corporate trade secrets such as high-tech companies' research and development plans." *Id.* at 32.

[15] Jo-Ann M. Adams, Comment, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 403, 406 (1996) (footnote omitted). "In all, reasonable estimates are that as many as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999." ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996), *aff'd* 117 S. Ct. 2329 (1997).

[16] Behar, *supra* note 1, at 66. Virtually every weapon a hacker needs to penetrate corporate computers is accessible on the Internet and there are even hacker magazines available that provide step-by-step tips. *Id.*

[17] Vicky H. Robbins, *Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software*, COMPUTER LAW., July 1993, at 20. Defining a computer virus as:

> [S]oftware that 'infects' a user's computer system much in the same way that a biological virus infects a living organism. It is a program that is passed from computer to computer by secretly attaching and copying itself into other programs that are then copied either by diskette or via computer network. A virus can be written to perform malicious tasks after infecting a new computer or to do no more than copy itself from machine to machine. At best, a virus is irritating and inconvenient; at worst, it can corrupt and destroy data and lock up an entire system.

Id.

[18] *See, e.g.*, Revlon Inc. v. Logisticon Inc., No. 705933 (Cal. Super. Ct., Santa Clara Cty., complaint filed Oct. 22, 1990). The Revlon complaint did not involve a hacker but a software company that dialed into Revlon's computer system and intentionally disabled Revlon's system because Revlon had not paid the software company in full for software Revlon had purchased from the software company. *Id.* Revlon could not distribute its products as two of its distribution centers were shut down because its computer system was disabled for three days losing an estimated $20 million in revenues. *Id.* The case was settled out-of-court. *Id.* The Revlon case offers some indication that despite the generally settled principle that tort law does not apply to purely economic loss, tortious interference with contractual relations may be a theory upon which recovery is based. Joseph P. Zammit, *Tort Liability for Mishandling Data*, 322 PLI/PAT 429, 440-41 (1991).

sions can be staggering. For example, in the well-known computer virus case of *United States v. Morris,*[19] the damage caused by a virus ranged from $96 million to $186 million based upon the labor costs to eradicate the virus and monitor the computer systems' recovery.[20]

Computer network security is practically nonexistent in many companies which subjects such companies to substantial risk.[21] As the corporation Revlon, Inc.[22] discovered, a disabled computer system can preclude a company from shipping products to its customers, thus causing millions of dollars in losses.[23] A hacker who successfully disrupts or interferes with the operations of a business causing millions of dollars in losses can be criminally prosecuted under the Computer Fraud and Abuse Act.[24] However, the Act does not provide a financial remedy to the victim corporation or third parties harmed as a result of the victim corporation's injury.[25] Moreover, even if the Act did provide a financial remedy, the typical hacker does not have the financial resources to compensate the victim corporation or injured third parties.[26] Thus, there is

[19] 928 F.2d 504, 505-06 (2d Cir. 1991), *cert. denied,* 502 U.S. 817 (1991) (stating that Morris created a virus that spread throughout the Internet disabling thousands of computers around the world). IBM has taken the threat of viruses very seriously by spending millions of dollars at IBM's High Integrity Computing Laboratory ("HICL") on its computer immune system project. *Protection Money,* COMPUTER BUS. REV., Dec. 1, 1996, *available in* 1996 WL 8660446. HICL has over 200 employees and "has even recruited leading scientists from the fields of biology and immunology." *Id.* Experts from HICL warn "that with 8,000 known viruses already identified, and an estimated six new varieties currently being discovered every day, the virus problem is far from being solved." *Id.* Analysts say companies "must treat their anti-virus polic[ies] and practices as strategic issues." *Id.*

[20] Susan C. Lyman, *Civil Remedies for the Victims of Computer Viruses,* 21 SW. U. L. REV. 1169, 1172 (1992).

[21] Crowley, *supra* note 12, at E8. A 1996 Computer Security Institute/FBI Computer Crime and Security Survey asked the respondents: "Do you have a written policy on how to deal with network intrusions?" 58% responded no and only 35% responded yes. *Id.* In 1988, infamous computer hacker Kevin D. Mitnick broke into Digital Equipment Corporation's purportedly secure computer network and "wreaked havoc to the tune of $4 m[illion] in damages." Kate Button, *Hunter and the Hunted,* COMPUTER WKLY., Mar. 14, 1996, at 38. "By 1992, Mitnick was officially named the FBI's most wanted computer criminal." *Id.*

[22] Revlon, No. 705933 at 1.

[23] *Id.* For example, Revlon alleged losses of $20 million when the defendant dialed into Revlon's computer system and disabled it. *Id.*

[24] 18 U.S.C. § 1030 (West Supp. 1996) (imposing criminal penalties for: 1) hackers who intentionally access computers without authorization and whose conduct involves interstate or foreign communication or; 2) hackers who knowingly and with intent to defraud access without authorization computers that are used in interstate or foreign communication).

[25] *Id.*

[26] Lyman, *supra* note 20, at 1195. "Often, a typical computer vandal may have little money with which to pay a judgment." *Id.* "[H]ackers rarely have deep pockets." Behar, *supra* note 1, at 60.

a need to prevent such hardships concomitant with the need for an available remedy should such hardships occur.

This Comment proposes a tort remedy in negligence that imposes a duty on a corporation to have adequate computer network security to prevent hacker intrusions that can severely damage the corporation itself, or other Internet-connected third party corporations damaged resulting from the original hacker intrusion.[27] This issue is a unique product of the Information Age with no established rules[28] and potentially enormous consequences. Part II of this Comment discusses the reality of the current threat of hacker intrusions, the inadequacy of current remedies, how tort law has evolved to adequately handle computer-related cases, and why the tort of negligence is the appropriate remedy. Part III discusses a proposed standard of care corporations should maintain to avoid tort liability in negligence, analyze how this tort remedy fits into the current legal framework, and demonstrate a successful application of negligence principles that achieves effective corporate computer network security and ample redress to potential victims of hacker intrusions. Part IV of this Comment concludes by proposing that liability in tort for computer hacking is both an effective deterrent for hackers and inadequately computer-secured corporations, and an adequate remedy for injured parties based upon a minimum standard of care.

II. BACKGROUND

A. The Threat to Corporate Computer Networks Is Real

The dramatic advancements in Internet and computer security are

[27] *See generally* Crowley, *supra* note 12, at E1. A hacker had penetrated Net Daemons, ironically, a network support outsourcing company that advised clients on Internet security. *Id.* The hacker then used Net Daemon's computer network as a springboard to connect into some of Net Daemon's customers' computer networks as Net Daemon's computer network was already connected electronically to its customers' computer networks for business relationship reasons. *Id.* at E8. The hacker impersonated a Net Daemon employee and fooled some of Net Daemon's customers' computer networks into believing that a Net Daemon employee was entering the customers' computer networks. *Id.* Net Daemon's customers were upset by the security breaches, but fortunately for Net Daemons, no one took legal action against Net Daemons. *Id.* Traci Bair, a program manager at International Data Corporation in Framingham, Massachusetts, warned, "Things like this happen all the time—holding people responsible is going to be the difference." *Id.* at E1.

[28] Behar, *supra* note 1, at 60. "[T]here hasn't been such a case to date, computer experts say it's only a matter of time." *Id.* "There hasn't been an important case where this has been tested yet, but there will be," says Mark Rasch, Director of Information Security, Law, and Policy for the security consulting firm Science Applications International Corp., of McLean, Va. Crowley, *supra* note 17, at E1.

evidenced by devices such as firewalls[29] and encryption[30] technology. Nevertheless, the reality of hackers breaking into government[31] and corporate[32] computer systems is still a critical problem. A few months ago, Dennis Hughes, the FBI's senior expert on computer crime, stated, "[t]he hackers are driving us nuts. Everyone is getting hacked into. It's out of control."[33]

[29] Michael Rustad & Lori E. Eisenschmidt, Article, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 227 (1995). Firewalls are computer devices that create a shell of protection between a network and possible intruder by restricting the flow of information entering and exiting a firm's computer or LAN (local area network) via communication devices. *Id.*

[30] Rustad & Eisenschmidt, *supra* note 29, at 230. Encryption is the scrambling of a digital message which "render[s] it meaningless to anyone who does not have the key to decrypt the message." *Id.* The industry standard is RSA which is a 64-digit key which can be broken with about $8.2 million worth of equipment. *Id.* at 301 n.100. "One industry expert markets encryption systems using 170-digit RSA keys and flatly asserts they are 'unbreakable.'" *Id.* at 233.

[31] Rustad & Eisenschmidt, *supra* note 29, at 217. The Pentagon disclosed that a 1994 internal audit of their network security performed by an in-house team utilizing hacker techniques successfully penetrated 88% of the 8,900 government computers they hacked. *Id.* Only 4% of the break-ins were detected. *Id.* Federal officials, using for the first time a court-ordered wiretap on the Internet, charged an Argentine student with hacking into computers of the Defense Department, the Navy, and the National Aeronautics and Space Administration. *First Internet Wiretap Leads to a Suspect*, N.Y. TIMES, Mar. 31, 1996, at I20. The student, from his computer in Buenos Aires, hacked his way into computers at the Naval Command, the Control and Ocean Surveillance Center in San Diego, the Naval Research Laboratory in Washington, NASA's Jet Propulsion Laboratory in Pasadena, CA, NASA's Ames Research Center at Moffett Field, CA, and the Los Alamos National Laboratory in New Mexico containing "files relating to research on state-of-the-art satellites, radiation and energy-related engineering." *Id.* It will cost more than $100,000 just to investigate the NASA intrusion and to secure the systems from future break-ins. *Id.*

[32] Marc S. Friedman & Kenneth R. Buys, *'Infojacking': Crimes on the Information Superhighway*, COMPUTER LAW., Oct. 1996, at 6. An Information Week survey of 200 businesses in 1995 surprisingly concluded that 95% admitted to being victims of computer fraud. *Id.* The Senate's Permanent Investigations Subcommittee reported that major banks and corporations lost $800 million from hackers in 1995. *Id.* Rockwell International, Inc., a major corporation, admits to being under attack on a "regular basis" from hackers using the Internet. *Id.*

[33] Behar, *supra* note 1, at 59. In February, 1996, FBI director Louis Freeh informed a Senate panel that "23 countries are engaging in economic spying against American businesses succeeding in some cases 'with a few keystrokes.'" *Id.* at 64. Freeh cited the major culprits as China, Canada, France, India, and Japan. *Id.* "The biggest security problem organizations face today is information brokers. Since the end of the Cold War there have been a lot of people trained in espionage who don't have a lot to do." says Dan White, national director of information security at Ernst & Young in Chicago. Wilder & Violino, *supra* note at 14, at 40. Richard Ress, a supervisory agent with the FBI's national computer crime squad in Washington, D.C., says, "[c]orporate secrets used to be stolen one box at a time. Now the equivalent of a hundred boxes can be copied and E-mailed. All you need is one hacker, and the entire hacker community may know about it by sundown." *Id.* at 32.

Computer network security is virtually nonexistent in many companies and part of the reason is because of the explosive growth of personal computers in corporate America.[34] This growth has somewhat decentralized and attenuated Management Information Systems'[35] ("MIS") control of all the computing power within a corporation.[36] The combination of massive personal computer proliferation and growth disproportionate to MIS's ability to manage such growth, along with more knowledgeable computer end users assuming more of the maintenance of their own systems, leaves security gaps in a corporation's computer network.[37] Furthermore, companies that suffer hacker intrusions keep quiet.[38] Most companies want to avoid the unwanted publicity.[39] However, keeping quiet about the problem of hacker intrusions does little to

[34] Michael Henderson, *PC-LAN Combinations Should Be Helpful to MIS Departments of the Fortune 1000*, COMM. NEWS, Feb. 1, 1986, at 32. "The explosive growth of the personal-computer (PC) market caught many of the Fortune 1000 data processing departments by surprise. Personal computers sprouted throughout the organizations and had firmly established themselves before information managers could gain any semblance of control." *Id.*

[35] *See generally* Rustad & Eisenschmidt, *supra* note 29, at 221. Management of Information Systems is the group within a corporation that manages the mainframe computer and all other associated computer systems. *Id.*

[36] *See generally The Business Rationale Driving Java Processors in Corporations*, DATA STORAGE REP., Mar. 1, 1996, *available in* 1996 WL 8622449. Before the advent of the personal computer, the computing performed for corporate America was done by mainframe computer systems governed by the Management of Information Systems ("MIS") department. *Id.* MIS was responsible for the data backups and security. Rustad & Eisenschmidt, *supra* note 29, at 221. As personal computer growth within corporations exploded, LAN (local area network) administrators were hired to manage and support these personal computers and networks. *See* Mary Hanna, *Net Growth Outpaces Expertise*, SOFTWARE MAG., July 1, 1995, at 41. However, corporations did not have enough qualified people to keep pace with the growth of personal computers and LANs. *Id.* "There just aren't enough people to do LAN management very well," said James Hardy, enterprise management architect at SSDS Inc., a systems integrator based in Englewood, Colorado. *Id.* "Even worse, many companies aren't even aware that their people don't know how to do it well," says Hardy. *Id.* Therefore, the LAN administration and security at many corporations is inadequate. *Id.*

[37] Jim Sobczak, *Who's Running the Show?*, BUS. COMM. REV., Sept. 1, 1996, at 70. As personal computers and LANs proliferated, the computing power shifted from the mainframe and MIS to the end users. *Id.* at 71. Therefore, the end users were more independent and could install and maintain their own software applications. *Id.*

[38] *See* Richard Power, *Follow the Money*, LAN MAG., Oct. 1, 1996, at 54. Martha Stansell Gamm of the U.S. Justice Department and prosecutor of infamous hacker Kevin Mitnick, indicates that corporations are under a vast scale of hacker attacks. Bicknell, *supra* note 12, at 20. Stansell Gamm claims the true numbers are kept hidden because most companies whose systems are infiltrated are not disclosing the incidents. *Id.* Stansell Gamm also asserts that for every one case that is reported, nearly 500 are kept secret. *Id.* Stansell Gamm cites a Computer Security Institute report showing that incidents of proprietary business theft rose 260% from 1985 to 1993. *Id.* The report concludes that of 8,932 attacks, 7,860 were successful but only 19 incidents were reported. *Id.*

promote awareness and solve the overall problem.[40]

B. Applying Tort Principles As a Deterrent and a Remedy

Having established that the threat of hacker intrusions is real, the next issues that must be addressed are: (1) how to provide an incentive for corporations to take hacker intrusions more seriously; (2) how to deter hackers from infiltrating corporate computer networks; and (3) how to provide a remedy to those injured by hacker intrusions. Unlike criminal law,[41] contract law,[42] or the law of the Uniform Commercial Code,[43] tort law provides an effective solution to these issues. The major pur-

[39] Power, *supra* note 38, at 54. Only 17% of the respondents that suffered a hacker intrusion reported the incident to law enforcement. *Id.* Over 70% of the respondents that suffered a hacker intrusion cited negative publicity as the reason for non-disclosure. *Id.*

[40] Bicknell, *supra* note 12, at 20. While keeping quiet avoids unwanted publicity, it prevents companies from learning about each other's misfortunes and taking the appropriate future precautions. *Id.*

[41] *See generally* Lyman, *supra* note 20, at 1197. Criminal law punishes the perpetrator and doesn't compensate the victim. *Id.* "The criminal law is concerned with the protection of interests common to the public at large . . . . [O]ften it accomplishes its ends by exacting a penalty from the wrongdoer." W. PROSSER & W. KEETON, THE LAW OF TORTS § 1, at 5 (5th ed. 1984). "[A] foremost purpose of criminal law is to serve the interest of the state in maintaining an ordered society and deterring future crime. Victims' interests are relegated to civil actions." Christopher T. Igielski, Note, *Washington Defendants' New Right of Pre-Trial Flight*, 19 SEATTLE U. L. REV. 633, 633-34 (1996)(footnote omitted).

[42] *See generally* John Jay Fossett, *The Development of Negligence in Computer Law*, 14 N. KY. L. REV. 289, 291 (1987). Contract law presupposes a prior agreement and this is not feasible for unknown but foreseeable plaintiffs (a company or person injured because of another company's lax computer security). *Id.* For example, hacker *A* infiltrates and uses company *B's* powerful computer network to penetrate and disable company *C's* computer network causing company *C* to fail to deliver mission critical components to a customer. *See id.* "[T]o deny recovery in this instance for lack of privity of contract is fundamentally unfair." 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, 185 (1990). "Contract liability is imposed by the law for the protection of a single, limited interest, that of having the promises of others performed." PROSSER & KEETON, *supra* note 41, § 1, at 5. Thus, if hacker *A* uses company *B's* computer network to penetrate and disable company *C's* computer network, company *C* cannot recover from company *B* using a contract theory of recovery because there were no promises or prior agreements made. *See generally id.*

[43] BLACK'S LAW DICTIONARY 1064 (6th ed. 1991). Uniform Commercial Code (U.C.C.) is a code of law "governing commercial transactions (including the sales and leasing of goods, transfer of funds, commercial paper, bank deposits and collection, letters of credit, bulk transfers, warehouse receipts, bills of lading, investment securities, and secured transactions)." *Id.* Thus, U.C.C. law is similar to contract law and suffers from the same inability to redress injuries to parties not part of the original bargain or transaction. *See generally* Fossett, *supra* note 42, at 291.

poses of tort law,[44] besides preventing people from "taking the law into their own hands," are: (1) to deter wrongful conduct; (2) to encourage socially responsible behavior; and (3) to restore injured parties to their original condition by compensating them for their injuries.[45] Applying tort law to corporations deters companies from having lax computer network security; applying tort law to hackers deters them from infiltrating companies because of the threat of monetary penalties.[46] Tort law encourages socially responsible behavior from companies by imposing a duty on them to exercise reasonable care in providing corporate computer network security.[47] Tort law also encourages socially responsible behavior from hackers because of their duty not to penetrate corporate computer networks where a foreseeable injury to another can occur.[48] If companies or hackers breach their duty then the injured parties are compensated for their injuries and are restored "to their original condition, insofar as the law can do this . . . ."[49]

C. How Negligence Has Evolved to Adequately Handle Computer Cases

Traditionally, contract law, not tort law, has been the basis of recovery for most computer-related cases.[50] This is because the damages from a computer-related claim were almost exclusively economic, and courts have traditionally denied negligence claims for purely economic losses.[51] The prohibition of negligence claims for purely economic losses was sometimes called either the "per se prohibitory rule," the "physical harm rule," or the "economic loss rule."[52] The rule barred recovery for economic losses absent physical injury or property damage.[53] The economic loss rule's rationale was to prevent "mass litigation, fraudulent claims,

[44] John W. Wade, Et Al., Prosser, Wade and Schwartz's Torts 1 (9th ed. 1994). "A tort is a civil wrong . . . for which the law provides a remedy. This area of law imposes duties on persons to act in a manner that will not injure other persons." *Id.*

[45] *Id.*

[46] Prosser & Keeton, *supra* note 41, § 1, at 6. "The purpose of the law of torts is to adjust [for] . . . losses, and to afford compensation for injuries sustained by one person as the result of the conduct of another." *Id.* (quoting Cecil A. Wright, *Introduction to the Law of Torts*, 8 Cambridge L.J. 238 (1944)).

[47] *See generally* Wade et al., *supra* note 44, at 1.

[48] *See generally* Wade et al., *supra* note 44, at 1.

[49] Wade et al., *supra* note 44, at 1.

[50] Fossett, *supra* note 42, at 291.

[51] Massingale & Borthick, *supra* note 42, at 181.

[52] *See* Massingale & Borthick, *supra* note 42, at 181-182. "[T]he economic loss rule precludes tort recovery of economic loss in the absence of physical injury to persons or other property." Timothy Davis, *College Athletics: Testing the Boundaries of Contract and Tort*, U.C. Davis L. Rev. 971, 992-93 (1996) (footnote omitted).

[53] *See* Massingale & Borthick, *supra* note 42, at 181. *See also* Davis, *supra* note 52, at 992-93.

and liability disproportionate to the defendant's fault."[54] However, there are fundamental problems with this rule when applied to computer-related cases. For example, hacker *A* illegally[55] penetrates corporation *B's* inadequately secured computer network. Then hacker *A*, impersonating a legitimate corporation *B* computer network user, uses the significant computing power of corporation *B's* computer network as a springboard to penetrate and shut down corporation *C's* computer network. Corporation *C's* business suffers severe financial loss. In this scenario, Corporation *B* escapes liability because the economic loss rule bars recovery for economic damages absent physical injury.[56]

Today, many courts recognize the fundamental unfairness of the economic loss rule and, therefore, are allowing recovery in negligence for purely economic losses.[57] In *People Express Airlines v. Consolidated Rail Corporation,*[58] the New Jersey Supreme Court concluded, "a defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty."[59] Some commentators argue that contract theories, rather than negligence theories, should apply in all computer cases resulting in economic loss.[60] However, using the above example of hacker *A* penetrating corporation *B* and using corporation *B*'s computer network to penetrate and harm corporation *C*, contract law fails to provide a remedy to corporation *C* for hacker

[54] Massingale & Borthick, *supra* note 42, at 182.

[55] *See* Adams, *supra* note 15, at 409 (describing computer hacking as a computer crime). "The hacker may go beyond breaking into a computer system and actually alter or destroy data." *Id.* at 410.

[56] Davis, *supra* note 52, at 992-93.

[57] *See* People Express Airlines v. Consolidated Rail Corp., 495 A.2d 107 (N.J. 1985) (rejecting the economic loss rule and allowing the plaintiff corporation to prosecute its claim for purely economic loss when a railway accident caused a tank of flammable liquid to spill and ignite near the plaintiff's business. The fire was contained and no physical damage occurred though the plaintiff's business operations were interrupted sustaining large financial losses). *See also* J'Aire Corp. v. Gregory, 598 P.2d 60, 64 (Cal. 1979) (stating "[w]here the risk of harm is foreseeable, as it was in the present case, an injury to the plaintiff's economic interests should not go uncompensated merely because it was unaccompanied by any injury to his person or property"); Mattingly v. Sheldon Jackson College, 743 P.2d 356, 360 (Ala. 1987) (holding "[a] defendant owes a duty of care to take reasonable measures to avoid the risk of causing economic damages, aside from physical injury [or property damage] . . . ."). *But see* Dundee Cement Co. v. Chemical Labs., Inc., 712 F.2d 1166 (7th Cir. 1983) (holding a cement plant could not recover from a truck owner and driver responsible for blocking the only road to the cement plant, allegedly causing purely economic damages because of the cement plant customers' inability to reach the plant).

[58] 495 A.2d at 107.

[59] *Id.* at 118.

[60] Massingale & Borthick, *supra* note 42, at 185.

A's misdeeds[61] because corporation *C* is not in privity[62] (a general requirement of contract law for liability) with corporation *B*. Therefore, the theory of negligence is more appropriate as it provides a remedy to injured third parties (e.g., corporation *C*) and avoids the overly harsh result of contract law.[63] Injured third parties are now more likely than ever to need a negligence remedy in an Information Age where anonymous access to the Internet fosters an environment in which unidentifiable perpetrators can injure third parties.[64]

D. The Proposed Remedy in Negligence—An Overview

Currently, there is no direct case law providing a remedy to a third party corporation injured on the Internet by a hacker's illegal use of another corporation's computer network to inflict harm.[65] Yet, one day there might be a case where a hacker easily penetrates a corporation's computer network as many corporations have not taken adequate security measures. According to security expert Clifford Stoll, "[t]he security weaknesses of both systems and networks, particularly the needless vulnerability due to sloppy systems management and administration, result in a surprising success rate for unsophisticated attacks."[66] The question then becomes how to motivate corporations to take computer network security more seriously? The answer lies with the theory of negligence[67] meaning "those who use computers have a duty to use them with care."[68]

[61] *See* Adams, *supra* note 15, at 410-11 (discussing how a hacker can break into a computer system and alter or destroy data).

[62] Black's Law Dictionary 833 (6th ed. 1991). Privity of contract is that connection or relationship which exists between two or more contracting parties. *Id.*

[63] *See* Fossett, *supra* note 42, at 292 (discussing the advantages of negligence theories over contract theories).

[64] *See, e.g.,* Wilder & Violino, *supra* note 14, at 32 (discussing the use of anonymous remailer programs that strip the e-mail identifiers from an e-mail message making the e-mail anonymous and untraceable).

[65] Crowley, *supra* note 12, at E1. "There hasn't been an important case where this has been tested yet, but there will be," says Mark Rasch, Director of Information Security, Law, and Policy for the security consulting firm Science Applications International Corp., of McLean, Va. *Id.* "[T]here hasn't been such a case to date, computer experts say it's only a matter of time." Behar, *supra* note 1, at 60.

[66] Massingale & Borthick, *supra* note 42, at 172.

[67] Wade et al., *supra* note 44, at 131. Negligence is "conduct which falls below the standard of care established by law for the protection of others against the unreasonable risk of harm." *Id.*

[68] Fossett, *supra* note 42, at 293-94. "Holding a company responsible for the actions of its computer does not exhibit a distaste for modern business practices . . . . The fact that [business operations] are carried out by an unimaginative mechanical device can have no effect on the company's responsibility for . . . errors and oversights." State Farm Mutual Auto. Ins. Co. v. Bockhorst, 453 F.2d 533, 536-37 (10th Cir. 1972).

Negligence provides a fair and equitable allocation of incentives, deterrence, and remedies to all parties involved as it fulfills three major objectives: (1) provides an incentive for corporations to take their computer network security more seriously; (2) deters hackers from illegally dialing into computer networks because even unintentional harm may make them liable; and (3) provides injured corporations or persons a remedy for their injuries.[69] A plaintiff may recover in negligence if he or she can prove the following elements: (1) a duty to use reasonable care; (2) a breach of that duty; (3) a reasonably close causal connection between the conduct and resulting injury; and (4) actual loss or damage to the protected interest of another.[70]

1. *Duty of Reasonable Care*

The plaintiff must prove that the corporation has a legal duty to the plaintiff to exercise reasonable care in maintaining adequate computer network security, thereby, protecting the plaintiff from an unreasonable risk of harm that could result from hacker intrusions.[71] Reasonable care is usually defined as the degree of care a reasonable person would exercise under the circumstances.[72] The risk reasonably perceived defines

[69] *See* WADE ET AL., *supra* note 44, at 1.

[70] *See* WADE ET AL., *supra* note 44, at 131.

[71] *See* WADE ET AL., *supra* note 44, at 131. "A duty, or obligation, recognized by the law, requiring the person to conform to a certain standard of conduct, for the protection of others against unreasonable risks." PROSSER & KEETON, *supra* note 41, § 30, at 164. "[T]he [corporation] is required to conduct [itself] in a particular manner at the risk that if [it] does not do so [it] becomes subject to liability to another to whom the duty is owed for any injury sustained by such other, of which that actor's conduct is a legal cause." RESTATEMENT (SECOND) OF TORTS § 4 (1965). "The duty of any person is the obligation of due care to refrain from any act which will cause foreseeable harm to others even though the nature of that harm and the identity of the harmed person or harmed interest is unknown at the time of the act . . . ." Donohue v. Senecal, 541 N.W.2d 742, 747 (Wis. 1995) (quoting A.E. Inv. Corp. v. Link Builders, Inc., 214 N.W.2d 764, 766 (Wis. 1974)).

[72] Massingale & Borthick, *supra* note 42, at 176-77. "The standard of conduct imposed by the law is an external one, based upon what society demands generally of its members, rather than upon the actor's personal morality or individual sense of right or wrong." PROSSER & KEETON, *supra* note 41, § 30, at 169. At common law, the standard of conduct was that of a "reasonable man under like circumstances." The "reasonable man" is denoted as:

> [A] person exercising those qualities of attention, knowledge, intelligence, and judgment which society requires of its members for the protection of their own interests and the interests of others. It enables those who are to determine whether the actor's conduct is such as to subject him to liability for harm caused thereby, to express their judgment in terms of the conduct of a human being. The fact that this judgment is personified in a 'man' calls attention to the necessity of taking into account the fallibility of human beings.

RESTATEMENT (SECOND) OF TORTS § 283 cmt. b (1965).

the duty owed and limits that duty to foreseeable plaintiffs.[73] Therefore, the plaintiff must show that the risk was foreseeable and that he or she could have been harmed by a hacker's intrusion.[74] Whether the corporation has a duty to a particular plaintiff is a question of law.[75]

2. *Breach of Duty*

The plaintiff must also prove that the corporation breached its duty to exercise reasonable care.[76] There are several ways for a corporation to breach its duty. Such ways include "failure to recognize defects in [its computer network security], the failure to correct defects, or the failure to warn of the defects."[77] The plaintiff may also prove a breach of duty by showing a failure to train and supervise employees on adequate security procedures[78] or failure to utilize reasonable means[79] to secure the computer network from unauthorized use.[80]

[73] *See* Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 100 (N.Y. 1928). "The risk reasonably to be perceived defines the duty to be obeyed, and risk imports relation; it is risk to another or to others within the range of apprehension." *Id.* "It is said that the defendant's responsibility must be limited to harm which results from the realization of the particular risk or hazard which the defendant has created." PROSSER & KEETON, *supra* note 41, § 43, at 283.

[74] Sun 'n Sand, Inc. v. United Cal. Bank, 582 P.2d 920, 936 (Cal. 1978) (quoting Dillon v. Legg, 441 P.2d 912, 920 (Cal. 1968)). "[T]he chief element in determining whether defendant owes a duty . . . to plaintiff is the foreseeability of the risk." *Id.* "A defendant's duty is established when it can be said that it was foreseeable that his act or omission to act may cause harm to someone. A party is negligent when he commits an act when some harm to someone is foreseeable." Donahue, 541 N.W.2d at 747 (quoting Rolph v. EBI Cos., 464 N.W.2d 667 (Wis. 1991)). "A duty may exist to one who is unknown and remote in time and place." Kirk v. Michael Reese Hosp. & Med. Ctr., 483 N.E.2d 906, 951 (Ill. App. Ct. 1985).

[75] Midkiff v. Hines, 866 S.W.2d 328, 332 (Tex. App. 1993) (stating "[g]enerally, the existence of a duty is a question of law"). *See also* Ernst v. Parkshore Club Apts. Ltd. Partnership, 863 F. Supp. 651, 654 (N.D. Ill. 1994). "Whether defendants owed a duty of care is a question of law to be decided by the court." *Id.*

[76] WADE ET AL., *supra* note 42, at 131. "A failure to conform to the standard [of conduct imposed by law] is negligence, . . . even if it is due to clumsiness, stupidity, forgetfulness, an excitable temperament, or even sheer ignorance . . . . In other words, society may require of a person [or corporation] not to be awkward or a fool." PROSSER & KEETON, *supra* note 41, § 31, at 169.

[77] Massingale & Borthick, *supra* note 42, at 178.

[78] *See generally Ernst*, 863 F. Supp. at 655. "[E]mployers are directly liable for negligent hiring and retention, and, thus, have a duty to refrain from hiring or retaining an employee who is a threat to third persons . . . ." *Id.*

[79] *See* Marie A. Wright, *Protecting Information from Internet Threats*, COMPUTER FRAUD & SECURITY BULL., Mar. 1, 1995, *available in* 1995 WL 8321941. Reasonable means to secure a computer network include using a firewall, using encryption technology, requiring employees to implement standard security procedures such as virus checks, periodic password changes and/or using more complex passwords. *Id.*

[80] Massingale & Borthick, *supra* note 42, at 178.

3. *Proximate Cause*

The third element the plaintiff must prove is that the corporation's failure to provide adequate security was the proximate cause[81] of the plaintiff's injury.[82] Proving proximate cause means: (1) showing the defendant's act or omission was the actual cause or cause-in-fact of the injury;[83] and (2) that the plaintiff's injury was the foreseeable consequence of the risk created by the defendant's act or omission.[84] Therefore, if the plaintiff can demonstrate that the corporation's failure to provide adequate computer network security was the actual cause of the injury and that the plaintiff's injury was the foreseeable consequence of the corporation's failure to provide adequate computer network security, then the plaintiff has a prima facie case of proximate cause.

There can be more than one proximate cause but the plaintiff only has to prove one proximate cause to recover.[85] For example, hacker *A*'s illegal entry into corporation *B*'s computer network can be one cause, corporation *B*'s inadequate computer security can be another cause, and if hacker *A* uses the corporation *B*'s computer network as a springboard into corporation *C*'s computer network, corporation *C*'s inadequate computer network security can also be another cause. However, if corporation *C* (the plaintiff) sues corporation *B* (the defendant) for failure to provide adequate computer network security, defendant corporation *B*

[81] BARRON'S LAW DICTIONARY 64 (3rd ed. 1991). Proximate cause is "that which in a natural and continuous sequence unbroken by any new independent cause produces an event, and without which the injury would not have occurred." *Id.* "'Proximate cause' . . . is merely the limitation which the courts have placed upon the actor's responsibility for the consequences of the actor's conduct . . . . [It] must be limited to those causes which are so closely connected with the result and of such significance that the law is justified in imposing liability." PROSSER & KEETON, *supra* note 41, § 41, at 264.

[82] WADE ET AL., *supra* note 44, at 131. "A reasonably close causal connection between the conduct and the resulting injury." *Id.*

[83] BLACK'S LAW DICTIONARY 152 (6th ed. 1991). "That particular cause which produces an event and without which the event would not have occurred." *Id.* "The defendant's conduct is a cause of the event if the event would not have occurred but for that conduct; conversely, the defendant's conduct is not a cause of the event, if the event would have occurred without it." PROSSER & KEETON, *supra* note 41, § 41, at 266.

[84] Massingale & Borthick, *supra* note 42, at 178. "Foreseeability relates to the natural and probable consequences of an act. One need only reasonably foresee that an injury may result from a dangerous condition . . . . The particular kind of injury need not have been foreseen." Hueston v. Narragansett Tennis Club, Inc., 502 A.2d 827, 830 (R.I. 1986). "A duty of care runs only to 'foreseeable plaintiffs,' any person or class of persons who could reasonably be expected to be injured by the system manager's negligence." Massingale & Borthick, *supra* note 42, at 178.

[85] *See Hueston*, 502 A.2d at 830 (holding that a concurring cause can be a proximate cause of a plaintiff's injury). *See also* Nobles v. White County, Illinois, 973 F.2d 544, 549 (7th Cir. 1992) (stating that there can be more than one proximate cause of a plaintiff's injury).

will argue that hacker *A*'s criminal act was unforeseeable[86] and therefore, constituted an intervening cause.[87] Plaintiff corporation *C* can defeat this argument by showing that hacker *A*'s illegal access was foreseeable and that defendant corporation *B*'s failure to provide adequate computer network security was the proximate cause of plaintiff corporation *C*'s injury.[88]

4. *Damages or Injury*

The final element the plaintiff must prove in a negligence case is that he or she suffered an injury.[89] The damages suffered by a plaintiff from a hacker's illegal acts or a corporation's inadequate security will almost exclusively comprise of economic damages.[90] As discussed earlier,[91] courts in the past have not allowed negligence claims for purely economic losses. However, some modern courts are allowing such claims and may continue to do so as more technology-related claims arise.[92]

III. ANALYSIS

A. The Current Problem of No Minimum Corporate Computer Network Security Standards

Most corporations have always taken steps to protect their documents from unauthorized access by securing the documents in locked file

[86] *See* Barnes v. Gulf Power Co., 517 So.2d 717, 718 (Fla. Dist. Ct. App. 1987) (holding that a criminal attack upon the plaintiffs by unknown assailants was an unforeseeable independent intervening cause of the plaintiff's injuries, thus releasing the defendant employer of the plaintiffs from liability).

[87] Black's Law Dictionary 568 (6th ed. 1991). Intervening cause is "[a]n act of an independent agency which destroys the causal connection between the negligent act of the defendant and the [plaintiff's] wrongful injury," thus relieving the defendant of liability. *Id.*

[88] *See* Britton v. Wooten, 817 S.W.2d 443, 449 (Ky. 1991) (rejecting the general rule that the criminal acts of third parties relieve the original negligent party from liability). *See also* Arneil v. Schnitzer, 144 P.2d 707, 718 (Or. 1944) (applying the principle that if a criminal act is reasonably foreseeable, the causal connection between the defendant's original negligent act is not broken by the intervening criminal act); Hodge v. Nor-Cen, Inc., 527 N.E.2d 1157 (Ind. Ct. App. 1988) (holding that the criminal act of an arsonist was not an intervening event that broke the causal connection between the landlord's negligence and the plaintiff's injuries).

[89] Massingale & Borthick, *supra* note 42, at 181. Injury is the "[a]ctual loss or damage resulting to the interests of another." Wade et al., *supra* note 44, at 131.

[90] Massingale & Borthick, *supra* note 42, at 181 (discussing that most injuries suffered in computer cases are economic).

[91] *See* discussion *supra* Part II.C.

[92] *See, e.g.,* People Express Airlines v. Consol. Rail Corp., 495 A.2d 107 (N.J. 1985). *See also, e.g.,* Thompson v. San Antonio Retail Merchants Ass'n, 682 F.2d 509, 515 (5th Cir. 1982) (affirming trial court's findings that the defendant failed to exercise reasonable care in programming its computer system causing the plaintiff's credit report to be inaccurate).

cabinets behind locked doors.[93] Just as corporate clients expect a business to secure their physical files from unauthorized access, they should also expect a business to secure its computerized files from unauthorized access.[94] Unfortunately, there are no generally accepted computer network security standards that corporations must follow.[95] Thus, a plaintiff who incurs damages because of a corporation's inadequate computer network security will not have a remedy, unless the plaintiff shows the corporation owed the plaintiff a duty to exercise reasonable care in protecting the corporation's computer network.[96] Therefore, to provide an incentive for corporations to maintain adequate computer network security and to provide injured plaintiffs a remedy, a minimum standard of computer network security must be delineated and maintained.

B. Defining the Duty of Minimum Computer Network Security Levels for Corporations

In general, a corporation's duty can be defined as a duty to select and implement security measures, to monitor the security measures' effectiveness, and to maintain and adapt the security measures according to changing security needs.[97] When implementing security measures, a corporation must balance the cost of adequate security versus the usability of a system as a company does not want to implement security measures so cumbersome that they reduce employee productivity.[98] Yet, when in doubt, a corporation should err on the side of caution and maintain the following minimum computer network security standards.[99]

[93] Michael H. Agranoff, *Curb on Technology: Liability for Failure to Protect Computerized Data Against Unauthorized Access*, 5 Santa Clara Computer & High Tech. L.J. 263, 267 (1989).

[94] *Id.*

[95] *Id.* at 274. "[T]here are no generally-accepted industry-wide standards of due care for the protection of computerized data, and even more surprising is the fact that computer security principles have been well known to practitioners for over a decade." *Id.*

[96] Agranoff, *supra* note 93, at 274. "Thus, presently, enterprises which hold computerized data are virtually free from liability for harm caused by unauthorized access, even though the methods to protect that data are common knowledge in the industry." *Id.*

[97] Massingale & Borthick, *supra* note 42, at 187.

[98] J. Martin, Security, Accuracy, And Privacy In Computer Systems 5 (1973). "Security and accuracy controls increase the cost of a computer system and in some cases degrade its performance somewhat." *Id.*

[99] Massingale & Borthick, *supra* note 42, at 187. This comment recognizes the financial impracticality for small companies to implement a comprehensive computer security regime. Thus, the size and financial resources of a company must be considered when determining the scope of a company's duty pursuant to the minimum computer network security standards proposed in this comment.

1. *Establish and Publicize a Corporate Computer Network Security Policy*

Security measures and policies can be difficult to implement and are often inconsistent.[100] However, a corporation's security policy is essential to establishing both the systems and data being protected, and the necessary security procedures protecting such systems and data.[101] The policy should describe the corporation's overall security objectives, reflect the corporation's serious concern of the risk of hacker intrusions, include provisions for performing a risk analysis, assign employee responsibility and accountability, and plan for disaster recovery (i.e., have a backup plan if systems or data are compromised).[102] A corporation must commit itself to this security policy to show the corporation exercised reasonable care in providing an adequate computer network security policy.

2. *Prevent Unauthorized Access to Computer Systems*

According to Michael H. Agranoff, a computer security expert, "[a]ccess control software is the heart of any computer security system. Its viability clearly depends upon proving the identity of the person attempting to access the system. This is usually done via a password."[103] Thus, passwords are probably the most important and yet most vulnerable[104] element of computer security because users have typically been careless with their passwords.[105] Users have typically chosen obvious combinations like their initials or spouse's name, or they write them down and put the passwords in their desks.[106] "It is estimated that 'over half of the passwords in use are said to be the first names of spouses and children, birthday and anniversary dates, or the names of super-he-

[100] Wright, *supra* note 79.

[101] Wright, *supra* note 79. "[A]n Internet security plan must be considered in the context of overall [corporation] and computer security." Dave James, *Barbarians at the Gate: Internet Security in the Law Firm/Corporate Environment*, 425 PLI/PAT 277, 308 (1995). Internet and phone-connected corporations "don't exist in isolation, and Internet security must be considered in the context of a [corporation's] overall security plan." *Id.* at 293.

[102] Wright, *supra* note 79.

[103] Agranoff, *supra* note 93, at 285.

[104] Rustad & Eisenschmidt, *supra* note 29, at 228. "The current overwhelming ignorance and indifference toward password security in companies constitutes one of the greatest threats to computer systems' security." *Id.* at 239.

[105] Massingale & Borthick, *supra* note 42, at 190. "[T]he tendency of persons to choose easily-remembered (and thus easily-guessed) passwords, or even to write these passwords down in an obvious place, is part of security folklore." Agranoff, *supra* note 93, at 290.

[106] Massingale & Borthick, *supra* note 42, at 190. "When allowed to choose their own passwords, many people tend to pick passwords that are easy for them to remember or use . . . . These kinds of passwords are not too difficult to guess." Emilio Jaksetic, *Passwords One Step Toward Ensuring Computer Security*, CORP. LEGAL TIMES, Apr., 1996, at 19.

roes.'"[107] A corporation should encourage users to use passwords that are not easy to guess like pronounceable nonsense words, or words with numbers or special characters inserted, and yet are easy to remember.[108] A corporation should also encourage users to memorize their passwords and not write them down, and also should encourage employees to change their passwords every few months.[109]

Hacker programs are available that crack passwords by trying every word in the dictionary (including variants of words and names) until it guesses the correct password.[110] Thus, with the high speed of computers and the comprehensiveness of these dictionary programs, common passwords can be cracked within minutes or hours.[111] However, even rudimentary security programs can detect these attempts and set off an alarm that can log the hacker off the system.[112] Therefore, if a corporation takes adequate measures to encourage its employees to use more complicated passwords, then the corporation can show it exercised reasonable care in implementing password security.

3. *Implement Administrative Security Controls*

Administrative security controls ensure that the policies and procedures for maintaining computer security are properly utilized.[113] Administrative controls include establishing a separate security apparatus in a corporation,[114] educating employees about computer security,[115]

[107] Rustad & Eisenschmidt, *supra* note 29, at 229.

[108] Jaksetic, *supra* note 106, at 19. "[U]se pass phrases that consist of combinations of two or three 4-letter or 5-letter words randomly selected from a dictionary, with arbitrary numbers or symbols (e.g., crest!pear or dust5rent)." *Id.*

[109] Jaksetic, *supra* note 106, at 19. "However a password is generated, its security value decreases with time. As a rule of thumb, you should change your password every six months or sooner." *Id.*

[110] Rustad & Eisenschmidt, *supra* note 29, at 229. "[H]ackers can use software programs that systematically try to crack passwords. Such programs will have a high degree of success against poorly chosen passwords." Jaksetic, *supra* note 106, at 19. "There are many programs and databases available that help hackers guess passwords, and if you use a password based on any known word, it will likely be included in one or more of these databases." James, *supra* note 101, at 305-06 (footnote omitted).

[111] Rustad & Eisenschmidt, *supra* note 29, at 229.

[112] Rustad & Eisenschmidt, *supra* note 29, at 229.

[113] Agranoff, *supra* note 93, at 288.

[114] Agranoff, *supra* note 93, at 288. "Establishing and implementing security policies for all employees and creating an IT [Information Technology] security officer position to monitor compliance will go far in a court battle to establish due diligence." Crowley, *supra* note 12 at E8.

[115] *See* Agranoff, *supra* note 93, at 288. For example, conducting training classes to teach employees to keep their passwords confidential and to keep their computers and offices physically secure. *See generally* Massingale & Borthick, *supra* note 42, at 188-89.

posting the corporation's security policies,[116] performing background checks on employees who have access to sensitive information,[117] protecting against computer viruses,[118] ensuring the corporation has insurance[119] against data disaster or virus attacks, and ensuring the physical locations of computers and other sensitive components are secured.[120] The administrative controls are the procedural mechanisms for the company's computer security policy.[121] Thus, if the corporation can properly implement its administrative security controls, then the corporation can show it exercised reasonable care in its procedures and policies for providing adequate computer network security.

4. *Install Firewalls*

Firewalls are extremely important in preventing hackers on the Internet from penetrating a corporation's internal computer network.[122] Firewalls are hardware and software devices (sometimes referred to as routers or gateways) that link a computer network to the Internet and prevent unauthorized access.[123] Firewalls can isolate effectively a corporate computer network from the outside world by monitoring and restricting all incoming and outgoing communications and by regulating

[116] *Setting up a Corporate Policy for Internet Use: A Checklist*, COMPUTER LAW STRATEGIST, Oct. 1995, at 5. For example, providing notice (written or on the computer screen) that unauthorized use is not permitted. *Id.*

[117] *See generally* Agranoff, *supra* note 93, at 288. For example, not hiring a felon convicted of robbery to protect a corporation's trade secrets. *Id.*

[118] *See* Agranoff, *supra* note 93, at 288. For example, installing anti-virus software and ensuring that all disks entering and leaving a company are virus free. *Thirty Steps to Information Security*, COMPUTER FRAUD & SECURITY BULL., Aug. 1, 1996, *available in* 1996 WL 8723589. Also, "[d]ownload [data] only from trusted sites, or don't download [data] at all." James, *supra* note 101, at 297.

[119] Robbins, *supra* note 17, at 20. "Recently, insurance companies have begun to offer all-risk computer insurance policies which specifically include coverage for losses caused by computer viruses." *Id.*

[120] Agranoff, *supra* note 93, at 284-85. "Physical security controls have two main objectives: to restrict access to facilities, and to protect hardware and software from damage if disaster occurs." *Id.* Advice to a computer system manager is:

> You also need to keep your backup tapes or disks physically secure (from both human and non-human threats) and keep copies in a location separate from the machine you've backed up (in cases of fire, flood, etc., if the backup is near the original data source both may be destroyed).

James, *supra* note 101, at 299.

[121] Agranoff, *supra* note 93, at 288.

[122] Rustad & Eisenschmidt, *supra* note 29, at 227. "Firewalls create a shell of protection between a network and possible intruders." *Id.* "[A] firewall is now almost mandatory." James, *supra* note 101, at 292.

[123] Rustad & Eisenschmidt, *supra* note 29, at 227. Firewalls can also link an individual computer to the Internet but typically act as a gatekeeper to all of the communication traffic coming into and out of the corporate network. *Id.*

remote dial-in access.[124] Firewalls are not impenetrable but are a very effective deterrent[125] and are important to show the corporation exercised reasonable care in protecting its computer network.

5. *Use Encryption Technology*

Despite the corporate use of security policies, passwords, and firewalls, the communication channels to and from a corporation are still unsafe as hackers can intercept incoming and outgoing communications.[126] Therefore, a method to protect the transmitted data must be utilized and encryption[127] technology is the answer. "Encryption refers to any algorithm[128] applied to a digital message which scrambles the plain text message, rendering it meaningless to anyone who does not have the key to decrypt the message."[129] Encryption protects the integrity and confidentiality of a corporation's data and ensures its authenticity, whether it is stored or transmitted across communication channels.[130]

There are many types of encryption technologies but generally, these technologies are categorized as private key systems and public key systems.[131] Private key systems use the same key to encrypt and decrypt messages, therefore, it is important that only the sender and receiver know the key.[132] The most popular and widely used private key system is the Data Encryption Standard ("DES"), which is the federal encryption

[124] Rustad & Eisenschmidt, *supra* note 29, at 227-28. "Firewall technology has evolved considerably in recent years and now provides significant protection against the unwanted inflow or outflow of digital data." *Id.* at 288.

[125] Behar, *supra* note 1, at 59 (discussing that the hackers were unable to crack *XYZ* corporation's firewall).

[126] Agranoff, *supra* note 93, at 287. "For some transmission of data, it just doesn't make sense to use the Internet or any other insecure channel. While it's certainly possible to hack into phone lines or leased lines, it's more difficult and occurs less frequently than on the Internet." James, *supra* note 101, at 307.

[127] *Changing Policies Towards Encryption and Internet Security*, COMPUTER FRAUD & SECURITY BULL., June 1, 1996, *available in* WL 8723573. Encryption comes from ancient Greek and means "secret writing." *Id.* "Encryption . . . is the only known defense to wiretapping." Agranoff, *supra* note 93, at 287. "If you need to send confidential information through the Internet or other insecure channels, or if you can't guarantee the physical security of your in-house computers, then the best way to protect your data from unauthorized access is to encrypt it." James, *supra* note 101, at 299.

[128] WEBSTER'S NEW WORLD DICTIONARY 33, 34 (3rd ed. 1989). "[A]ny systematic method of solving a certain kind of problem" or "a predetermined set of instructions for solving a specific problem in a limited number of steps." *Id.*

[129] Rustad & Eisenschmidt, *supra* note 29, at 230.

[130] Rustad & Eisenschmidt, *supra* note 29, at 231-32. "Encryption may be used to protect passwords and data, and to verify communications." *Id.* at 301 n.78.

[131] Wright, *supra* note 79.

[132] Wright, *supra* note 79. "With private-key cryptography, the same secret key is used both to encrypt and decrypt a file." James, *supra* note 101, at 300.

standard enunciated in 1977.[133] However, there is a growing concern however that the DES standard is too weak for today's requirements.[134]

Public key systems use two different keys, one private and one public, to encrypt and decrypt messages.[135] "[T]he sender and receiver need not share a secret key."[136] Instead, the receiver generates a public key and a private key.[137] The sender encrypts a message using the public key; however, the message cannot be read without the corresponding private key.[138] The most powerful and widely used public key system is the RSA algorithm.[139] While RSA is extremely powerful and safe, RSA is significantly slower than DES.[140] In order to get the best of both worlds, a corporation can use a combination of DES and RSA algorithms to provide confidentiality, integrity, and authenticity in the corporation's computer network environment.[141] Encryption technology is not

[133] Wright, *supra* note 79. "The federal government has used Data Encryption Standard ("DES"), a 56-bit, single key encryption technology, since the mid-1970s for its sensitive, but not classified, information." Rustad & Eisenschmidt, *supra* note 29, at 230 (footnote omitted).

[134] Rustad & Eisenschmidt, *supra* note 29, at 231. "[T]he National Institute of Standards & Technology ("NIST"), while reauthorizing the government's use of DES in 1993, simultaneously indicated the approaching end of its usefulness." *Id.*

[135] Wright, *supra* note 79.

[136] James, *supra* note 101, at 302.

[137] James, *supra* note 101, at 302. The receiver can send the public key over the Internet, thus the name "public key." *Id.*

[138] James, *supra* note 101, at 302. "Messages encrypted with the receiver's public key can be decrypted only with the corresponding private key." *Id.* It is not mathematically feasible to determine the private key code from the public key and vice versa. Wright, *supra* note 79.

[139] Rustad & Eisenschmidt, *supra* note 29, at 231. "RSA is marketed by RSA Data Security of Redwood City, California, and it has become the de facto encryption industry standard." *Id.* "RSA" represents the names of its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. *Id.* at 301 n.87.

[140] Rustad & Eisenschmidt, *supra* note 29, at 231-32. "One drawback of using public-key systems is that encryption and decryption are typically much slower than are private-key systems (depending on the implementation, DES can be from 100 to 10,000 times as fast as RSA)." James, *supra* note 101, at 304.

[141] Rustad & Eisenschmidt, *supra* note 29, at 231-232. These authors discuss that:

> While public key processing has the disadvantage of being about 100-times slower in software and 1,000 times slower in hardware than DES, various methods are already circulating to mitigate this shortcoming. One solution is to use RSA primarily to transmit brief messages. For longer messages, RSA encryption can be used to send the recipient a one-time single key encryption scheme, which then can be used to send the subsequent long message. Since the single key encryption scheme is used only one time, the security of the transmission is not compromised. A third method, known as 'RSA digital envelope,' combines DES and RSA as follows: '[F]irst the message is encrypted with a random DES key, and then, before being sent over an insecure communications channel, the DES key is encrypted with RSA. Together, the DES-encrypted message and the RSA-encrypted message are sent.'

Id. at 232 (footnotes omitted).

impenetrable[142] but whatever type of encryption a corporation uses, encryption technology is important to secure the data communication lines to and from a corporation's computer network. A corporation's use of encryption technology is essential to show the corporation exercised due care in securing its communication lines to and from its computer network.

6. *Protect Computer Resources from Insider Abuse*

A corporation must secure its computer network not only from outsider intrusions, but also from insider intrusions by its own employees.[143] Corporate losses from insider intrusions can be staggering. A November 23, 1996 Information Systems Security survey of 236 security managers and executives concluded that 46 percent of the 236 companies admitted insider abuse of their computer systems.[144] The losses were dramatic: 22 percent indicated losses between $50,000 and $200,000, and an additional 20 percent indicated losses between $200,000 and $500,000.[145]

A corporation can take steps to prevent insider computer abuse by performing background checks on its employees who control access to sensitive data.[146] Also, when an employee is terminated for any reason, he should be escorted to his desk while he removes his personal belongings and all security codes must be submitted to the firm.[147] Anything the employee had to do with security (e.g., passcodes, entry to physically secured locations in the company) should be considered compromised

[142] Rustad & Eisenschmidt, *supra* note 29, at 233 (discussing that parallel processing may make it possible to crack a 64-digit key).

[143] Rustad & Eisenschmidt, *supra* note 29, at 238. "While encryption seems to be providing a solution to the problem of insecure Internet transactions, many firms are still failing to take adequate internal security measures to protect against computer security breaches by their employees." *Id.*

[144] William J. Cook, *Industrial Espionage and the Internet*, CHICAGO LAW., Feb. 1997, at 57-58. "[These findings] are similar to a Michigan State survey in October 1995 of 150 corporate security directors, which revealed that 98.6 percent of their companies had experienced a computer-related crime and that 75 percent to 80 percent of the incidents were caused by insiders." *Id.* at 58.

[145] *Id.*

[146] *See generally* Agranoff, *supra* note 93, at 288. The corporation should incorporate into its computer security policy that it will perform a background check on anyone it hires who may have access to sensitive data. *Id.* It also makes sense to perform background checks on its existing employees and to annually review its files to make sure no employees who are in control of sensitive data have not had a background check. *Id.* The annual review would close the loophole of an employee who was formerly in a nonsensitive area of the company from being promoted to a sensitive area of the company without a background check. *Id.*

[147] Rustad & Eisenschmidt, *supra* note 29, at 238.

and all related passcodes or locks should be changed.[148] While this may seem harsh, it is an effective way to prevent insider computer abuse and to show the corporation exercised reasonable care in securing its computer network.[149]

7. *Monitor the Effectiveness of Computer Network Security and Update Security When Necessary*

The corporation has a duty to monitor the effectiveness of its computer security policies, procedures, and infrastructure.[150] Monitoring computer network access is essential and any attempt to access computer files or programs should be logged[151] for future reference, and all suspicious accessing should be reviewed and if necessary, terminated.[152] For example, if during a computing session, five attempts were made to access a file and all five attempts were denied, the access control software could automatically "suspend" the particular user until a system administrator investigates and "unsuspends" that particular user.[153] In addition, the corporation should consider using computer network security auditing products that provide a great deal of network security analysis and reporting.[154] For example, the Internet Scanner 3.2[155] can scan a corporation's computer network and comprehensively probe for network vulnerability, check for firewall security holes, and provide suggestions to fix the security holes.[156] The vast array of Internet and computer security devices make it feasible for a corporation to monitor the effectiveness of its computer security and to update its security when necessary. This is important to demonstrate a corporation has

[148] Rustad & Eisenschmidt, *supra* note 29, at 238.

[149] *See generally* Rustad & Eisenschmidt, *supra* note 29, at 238. This situation is not different from days past when after an employee was terminated, he or she was required to turn in his keys to his file cabinet, office, or other secured location. *Id.*

[150] Massingale & Borthick, *supra* note 42, at 191.

[151] Agranoff, *supra* note 93, at 294. Logging is defined as:

> [T]he electronic recording of significant ACS [Access Control Software] files activity. Such activity will normally include all access requests which the security system denied such as invalid password attempts, or any valid requests which the system administrators somehow deemed worthy of inclusion. The purposes of logging are to catch actual malefactors, deter potential malefactors, and provide information for system recovery.

Id.

[152] Massingale & Borthick, *supra* note 42, at 191.

[153] Agranoff, *supra* note 93, at 294.

[154] *See* Michael Surkan, *Daemons Defy Hackers: Internet Scanner Best Ferrets Out Network Security Breaches*, PC WK., Feb. 5, 1996, at N1.

[155] *Id.* The Internet Security System Inc.'s Internet Scanner 3.2 was rated the best network security scanner. *Id.*

[156] *Id.*

exercised reasonable care in maintaining the security of its computer network.

C. An Illustration of a Cause of Action in Negligence for a Corporation's Failure to Provide Adequate Computer Network Security

1. *The Fact Pattern*[157]

A team of hackers has successfully dialed into *ABC* Corporation, a medium sized company with $200 million in revenues and ten locations throughout the United States. The hackers next use *ABC*'s computers and modems to freely "war dial"[158] until they hack into *DEF* Corporation's computer systems. *ABC* did not have a firewall and had easy passwords to crack, otherwise the hackers could not have broken into *ABC*'s computer systems. However, *DEF* did have a firewall but the hackers cracked a critical password to a remote computer in *DEF*'s warehouse (which was connected to the main warehouse computer that ran *DEF*'s national product distribution system) by using a hacker dictionary program.[159] Finally, the hackers electronically penetrated *DEF*'s main warehouse computer and completely disabled it. The combination of *DEF*'s three days of lost business and the costs of getting its computer system running again amounted to an alleged total loss of $20 million.

2. *The Negligent Corporation's Liability*

ABC Corporation is liable in negligence to *DEF* Corporation.[160] According to the minimum corporate computer network security standards proposed earlier in this comment,[161] *ABC* had a duty to provide ade-

[157] A combination of two true stories into one hypothetical illustrates how a negligence case can be brought against a corporation that fails to provide adequate security to its computer network. The two combined stories are from the professional hackers from WheelGroup Corp. in the introduction of this comment and from the filed complaint of Revlon, Inc. *See* Revlon Inc. v. Logisticon Inc., No. 705933 (Cal. Super. Ct., Santa Clara Cty., complaint filed Oct. 22, 1990). Revlon filed a complaint against a software company that dialed into Revlon's computer system and disabled it for three days, losing Revlon an alleged $20 million in revenues. *Id.*

[158] Behar, *supra* note 1, at 59-60. War dialing is using modems to dial automatically thousands of phone numbers within a specific range to find other modems to connect with. *Id.* Then such connections are used to hack into the attached computer systems. *Id.*

[159] Rustad & Eisenschmidt, *supra* note 29, at 229. "Hacker dictionary programs operate by trying every word in the dictionary (including variant of words and names) until a password match is found." *Id.*

[160] RESTATEMENT (SECOND) OF TORTS § 282 (1965). "[N]egligence is conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm." *Id.*

[161] *See* discussion, *supra* Part III.B.1-7. The minimum corporate computer network security standards are: (1) establish and publicize an organizational security policy; (2)

quate network security so that *DEF*, a foreseeable plaintiff,[162] was not subjected to the unreasonable risk of the hackers' intrusion.[163] *ABC* breached its duty to provide adequate computer network security by not having a firewall installed and by not having the proper procedures in place to prevent use of easy passwords by *ABC* employees.[164] The heart of this cause of action in negligence is the seminal rule on foreseeability by Justice Cardozo, "the risk reasonably to be perceived defines the duty to be obeyed."[165] Foreseeability[166] defines the duty[167] owed by *ABC* to foreseeable plaintiffs,[168] (i.e., *DEF* Corp.) and computer hacking is

prevent unauthorized access to computer systems; (3) implement administrative security controls; (4) install firewalls; (5) use encryption technology; (6) protect computer resources from inside jobs; (7) monitor the effectiveness of computer network security and update security when necessary. *See* discussion, *supra* Part III.B.1-7 [hereinafter Network Security Standards].

[162] Massingale & Borthick, *supra* note 42, at 177. "[A] duty imposes an obligation only towards those who would be foreseeably endangered and only with respect to those risks or hazards that are reasonably foreseeable." *Id.*

[163] Massingale & Borthick, *supra* note 42, at 177. "A duty of care runs only to 'foreseeable plaintiffs,' any person or class of persons who could reasonably be expected to be injured by the system manager's negligence." *Id.*

[164] It is important to note this comment does not propose that a successful hacker intrusion by itself constitutes a breach of duty. The duty imposed on the corporation is the failure to *provide* adequate security measures, not the failure to have *hacker-proof* security measures in place. For example, if *ABC* Corporation had had a firewall installed and could show that it had adequate procedures in place to prevent unauthorized access by demonstrating that it had employee training classes, etc., then *ABC* is probably not liable in negligence.

[165] Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 100 (N.Y. 1928).

[166] *See generally id.* "In tort law, the 'foreseeability' element of proximate cause is established by proof that [the] actor, as [a] person of ordinary intelligence and prudence, should reasonably have anticipated danger to others created by his negligent act." BLACK'S LAW DICTIONARY 649 (6th ed. 1991).

[167] Hartsfield v. McRee Ford, Inc., 893 S.W.2d 148, 150 (Tex. Ct. App. 1995). The court describing the factors used in determining whether there is a duty:

> Imposition of a duty involves several factors, including 'risk, foreseeability, and likelihood of injury weighed against the social utility of the actor's conduct, the magnitude of the burden of guarding against the injury and consequences of placing that burden on the [defendant].' Courts have traditionally considered foreseeability to be the most significant of these factors.

Id. "The duty of any person is the obligation of due care to refrain from any act which will cause foreseeable harm to others even though the nature of that harm and the identity of the harmed person or harmed interest is unknown at the time of the act." A.E. Inv. Corp. v. Link Builders, Inc., 214 N.W.2d 764, 766 (Wis. 1974).

[168] This comment recognizes that the *Palsgraf* case represents the proposition that a foreseeable plaintiff is one who is specifically identifiable at the time of the negligent act's occurrence. PROSSER & KEETON, *supra* note 41, § 43, at 285. Thus, this comment proposes to broaden the holding in *Palsgraf* to include plaintiffs whose identity is not known to the defendant at the time of the negligent act's occurrence. Such broadening is appropriate and indeed necessary, because the Internet links people and companies (and creates new risks) in ways not contemplated by Justice Cardozo in 1928.

clearly a foreseeable risk a corporation takes when it connects to the Internet or operates a computer network that is susceptible to hacker intrusions because the network is attached to phone lines.[169]

DEF Corporation has suffered $20 million in damages. *ABC* Corporation's inadequate computer network security was the actual cause or cause-in-fact[170] because if *ABC* did not have inadequate security, *DEF* would not have suffered $20 million in damages. *DEF*'s damages were also the foreseeable consequence of *ABC*'s unreasonable risk of not having adequate computer network security, and therefore, proximate cause is shown.[171] Thus, *ABC* is liable to *DEF* in negligence because *ABC* had a duty to provide adequate network security, *ABC* breached that duty by not having a firewall and by not having procedures in place to prevent easy passwords from being utilized, and *DEF*'s $20 million in damages were the foreseeable consequence of *ABC*'s inadequate computer network security.

3. *The Negligent Corporation's Failed Defense and Counterarguments*

ABC can assert the defense of contributory negligence[172] or assert the theory of comparative negligence[173] for *DEF* Corporation's alleged negligence in failing to provide its own adequate computer network security.[174] However, according to the standard of care proposed in this

[169] Pamela Samuelson, *Can Hackers Be Sued for Damages Caused by Computer Viruses?*, COMM. OF THE A.C.M., June 1989, at 666. "[T]he owner of the computing system . . . [h]as a duty of care to create reasonable safeguards against unauthorized access . . . because the penchant for hackers to seek unauthorized entry is well-known in the computing community." *Id.*

[170] BLACK'S LAW DICTIONARY 152 (6th ed. 1991). "[T]he injury . . . would not have happened but for the conduct of the wrongdoer." *Id.*

[171] *See* Stewart v. Federated Dep't Stores, Inc., 1991 WL 88068 1, 2 (Conn. Super. Ct. 1991). "The foreseeability of the act . . . determines whether there is proximate cause." *Id.* "[L]egal cause exists when 'the injury is of a type which a reasonable man would see as a likely result of his conduct.'" DeMyrick v. Guest Quarters Suite Hotels, 944 F. Supp. 661, 666 (N.D. Ill. 1996).

[172] BLACK'S LAW DICTIONARY 716-17 (6th ed. 1991). Contributory negligence is a defense where the plaintiff breaches his duty to protect himself from injury and is a contributing cause of his injury. *Id.* Contributory negligence is a complete bar to plaintiff's recovery in only five states: Alabama, Maryland, Virginia, North Carolina, and the District of Columbia. WADE ET AL., *supra* note 44, at 568.

[173] BLACK'S LAW DICTIONARY 193 (6th ed. 1991). Comparative negligence is where the amount of negligence is measured in terms of percentage and any damage allowed to plaintiff is diminished in proportion to the amount of negligence attributable to the plaintiff's conduct. *Id.*

[174] This comment does not discuss the doctrines of joint and several liability, contribution, and assumption of risk because the advent of comparative negligence has significantly diminished the applicability of these doctrines in most states. *See* John Scott Hickman, Note, *Efficiency, Fairness, and Common Sense: The Case for One Action as to Percentage of*

comment,[175] *DEF* probably would not be liable in negligence (i.e., *DEF* would not be assigned a proportional percentage of the fault thus reducing *ABC*'s percentage of fault) unless *DEF* violated the other areas of its duty to provide adequate computer network security.[176] *ABC* may also argue that the criminal act of the hackers was an unforeseeable intervening cause[177] relieving *ABC* from liability. However, *ABC*'s argument fails when *DEF* demonstrates that the hackers' criminal act was foreseeable and that it is anomalous that "[t]he happening of the very event the likelihood of which makes the actor's conduct negligent and so subjects the actor to liability cannot relieve him from liability."[178]

Alternatively, *ABC* may argue that its fault should by reduced by the intentional fault of the hackers. However, this argument should fail because shifting some of *ABC*'s liability to the hackers would reduce the incentive for corporations like *ABC* to provide adequate computer network security.[179] *ABC* can pursue reducing its monetary cost of liability

Fault in Comparative Negligence Jurisdictions that Have Abolished or Modified Joint and Several Liability, 48 VAND. L. REV. 739, 741-42 (1995). The trend has been:

> The past decade has seen a marked increase in the number of states that have either abolished or modified the joint liability rule and replaced it with some form of comparative fault .... In 1950 only five jurisdictions in the United States applied comparative negligence to most negligence cases. By 1995, forty-six states had adopted comparative negligence by either legislative or judicial action.

Id (footnotes omitted). "Assumption of risk is not favored by the courts .... [T]he advent of comparative negligence is prompting courts to implement a merger of the defenses of contributory negligence and [ ] assumption of risk." WADE ET AL., *supra* note 44, at 594.

[175] Network Security Standards, *supra* note 161.

[176] For example, if *DEF* did not have a firewall installed and did not use encryption technology, then *DEF* may be assigned a percentage of the fault. This percentage would reduce proportionally the percentage of fault attributed to *ABC* and, thus, reduce *ABC*'s percentage of liability. *Id.*

[177] BLACK'S LAW DICTIONARY 568 (6th ed. 1991). Intervening cause is "[a]n act of an independent agency which destroys the causal connection between the negligent act of the defendant and the wrongful injury." *Id.*

[178] RESTATEMENT (SECOND) OF TORTS § 449 cmt. b (1965). *See also* Slawson v. Fast Food Enters., 671 So.2d 255, 259 (Fla. Dist. Ct. App. 1996) (finding the defendant business liable for failing to protect a patron from a reasonably foreseeable intentional attack by a third party. The court stated that "if the reasonable possibility of the intervention, criminal or otherwise, of a third party is the avoidable risk of harm which itself causes one to be deemed negligent, the occurrence of that very conduct cannot be a superseding cause."); Cruz v. Middlekauff Lincoln-Mercury, Inc., 909 P.2d 1252, 1257 (Utah 1996) (stating "the thief's criminal acts, though intervening, do not preclude a finding of proximate cause if the acts were foreseeable").

[179] *See* Wal-Mart Stores, Inc. v. McDonald, 676 So.2d 12, 22 (Fla. Dist. Ct. App. 1996) (holding that "allowing [a negligent] tortfeasor to place the blame entirely or largely on the intentional wrongdoer would serve as a disincentive for the negligent tortfeasor to meet its duty [of] reasonable care to prevent intentional harm from occurring"). *See also* Kansas State Bank & Trust Co. v. Specialized Trans. Serv., Inc., 819 P.2d 587, 606 (Kan. 1991) (reasoning that negligent tortfeasor should not be allowed to reduce its fault by the intentional fault of another that the negligent tortfeasor had a duty to prevent).

by directly suing the hackers for trespass to chattel (and *DEF* also can assert such action against the hackers).[180] Nevertheless, *ABC*'s liability to *DEF* remains and stems from its failure to provide adequate computer network security to prevent a foreseeable hacker intrusion that caused damage to *DEF*.

IV. CONCLUSION

The use of computers and the Internet is increasing every day. The current lack of minimum corporate computer network security standards and the economic loss rule leave injured parties without redress from hacker intrusions into corporate computer networks. However, this comment has described how tort law has developed in recent years as an appropriate legal tool to solve computer and Internet related issues. Tort law helps solve the social problem of computer hacking by deterring hackers and providing an incentive for corporations to provide adequate computer network security. Otherwise, the hacker is liable in trespass and the corporation is liable in negligence, both as remedies available to the injured party.

This Comment has proposed a minimum standard of care for corporate computer network security. Without a nationally recognized standard of care, an injured party may fail to prove the negligent corporation had a duty to that injured party. Therefore, a national standard of care must be adopted either by case law or federal legislation providing corporations an incentive to bolster their computer network security and providing injured parties a remedy. This standard of care will go a long way in promoting computer security awareness and in preventing the potentially grave risks and consequences associated with using computers and the Internet.

David L. Gripman

[180] Thrifty-Tel, Inc. v. Bezenek, 54 Cal.Rptr.2d 468, 473 (Cal. Ct. App. 1996) (ruling that a long-distance telephone company victimized by hackers could recover under a theory of trespass to chattel).