PHYSICAL LOSSES IN CYBERSPACE

*Hazel Glenn Beh**

TABLE OF CONTENTS

INTRODUCTION

We used to live in a physical[1] world where first party insurance comfortably covered fortuitous physical events that damaged our tangible property. Today, a business's most valuable property may exist largely in cyberspace without physical form.[2] The perils that face these new business

---

* Hazel Glenn Beh, Associate Professor of Law, William S. Richardson School of Law, University of Hawaii. The author thanks Matt McCall for research assistance, Professor Raymond Panko for sharing his work on human error and Christopher G. Trainer, Middle Market Practice Leader, e-business, at Marsh, Inc., for providing information about Net Secure, Marsh's insurance product for e-business.

1. Physical is defined as "of or relating to material things." THE AMERICAN HERITAGE DICTIONARY 1325 (4th ed. 2000).

2. Cyberspace is "the continuum of computer networks and bulletin board systems in which on-line communication takes place." *Id.* at 452. William Gibson gave the world the term, "cyberspace" which he referred to as "a consensual hallucination," Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1617 n.42 (1999) (citing WILLIAM GIBSON, NEUROMANCER 51 (Ace Books 1984)), referring to the collective belief that there is some space behind the computer screen. *See* Kenneth P. Weinberg, *Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)*, 5 J. INTELL. PROP. L. 667, 670-71 (1998). On a more philosophical level, it has been defined "as 'the conceptual space where words, human relationships, data, wealth, and power are

forms are not the traditional perils of fires, floods, and other physical forces of man and nature, but perils that exert no apparent physical force and leave no sign of physical damage behind.

An e-business is different than a bricks and mortar business in how it values itself, in what it regards as assets, and in how it conducts its business. An e-business counts its intangibles as some of its most valuable assets. In addition, an e-business transacts business at an Internet site rather than through face-to-face contact at a storefront location; therefore, it needs to guard against all kinds of interruptions that may directly or indirectly disrupt its connection to the cyberworld. The perils of the cyberworld are necessarily different than those that imperil traditional business. E-businesses face more perils in the cyberworld than in the physical world, including risks unheard of a decade ago, such as computer programming errors, hacker attacks, and computer viruses.

This Article explores first party insurance coverage for losses associated with business in cyberspace. Section Two describes the nature and magnitude of property and business interruption risks associated with computer and Internet dependent businesses. It highlights the inescapable conclusion that this nascent business form, at least at present, is extremely vulnerable to perils unknown just a few years ago. Section Three briefly examines relevant provisions in traditional property, business interruption, and crime policies and also discusses several judicial decisions that consider whether computer-based losses are covered under traditional insurance contracts. While some coverage may exist under these traditional policies, insureds and insurers seeking more certainty will find the infirmities of these policies readily apparent.

Section Four predicts that existing gaps in coverage and the current state of uncertainty will be transitory. Insurers will respond quickly to adverse judicial decisions by drafting more ironclad exclusions and by offering more suitable insurance products. Quite possibly, the availability of these new policies will have the positive secondary effect of reducing risks as insurers pool their knowledge to identify vulnerabilities and require insureds to strengthen their Internet security measures. Finally, this section examines one of several new insurance products currently on the market that affords first party coverage for cyberlosses. These new policies are fundamentally different than traditional products: the named perils insured

---

manifested by people using computer technology.'" *Id.* at 671 (quoting Michael Johns, *The First Amendment and Cyberspace: Trying to Teach Old Doctrines New Tricks*, 64 U. CIN. L. REV. 1383 (1996) (quoting HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY 5 (1993))).

against are those specific to computer-based businesses; covered property expressly includes intangible assets stored on a computer; and the nature of the losses covered are those uniquely associated with e-business.

I. BUSINESS RISKS IN A COMPUTER-DEPENDANT WORLD

The assets of businesses are increasingly intangible.[3] A significant portion of a company's assets now include intangibles, such as electronically stored information including "accounting information, intellectual property (e.g. trade secrets, know-how, patent information, design data, source code), key customer and supplier data, and competitive information."[4]

The Internet has also allowed businesses to rapidly and dramatically change their mode of operation.[5] The mode of business operations for an e-business is largely computer-to-computer; these businesses depend less on face-to-face transactions than a bricks and mortar operation.[6] Moreover, the ability to transact business without personal interaction and a physical location has changed a business's capacity to expand as well as its rate of expansion. The Internet's affordable, direct access to a nearly unlimited number of potential customers[7] means businesses can rapidly grow and reach markets that bricks and mortar businesses could not.[8]

---

3. "In the past, an enterprise's critical infrastructure consisted of its physical plant, equipment and inventory. In the emerging technology-based environment, however, an enterprise's core operations depend on electronic information and computer networks." Emily Q. Freeman, *E-merging Risks: Operational Issues and Solutions in a Cyberage*, RISK MGMT., July 2000, at 13-14. At least 50% of the value of information or technology-based companies may be found in "the data itself and the ability of that computer system to deliver information to people within the organization." Leslie Werstein Hann, *E-Commerce Safety Nets*, BEST'S REV., PROP./ CASUALTY INS. EDITION, Dec. 1998, at 71, 75. *See also* Spencer M. Taylor & Sean W. Shirley, *Insurance and Cyber-Losses: Coverage for Downloading Disaster*, 62 ALA. LAW. 193, 195 (2001); David R. Cohen & Roberta D. Anderson, *Insurance Coverage for "Cyber-Losses,"* 35 TORT & INS. L.J. 891, 893 (2000).

4. Freeman, *supra* note 3, at 14.

5. *See* Greg Nelson, *Exposed on the Net: A Comparison of Internet Business Exposures with Standard Business Policies*, 53 CHARTERED PROP. & CASUALTY UNDERWRITERS J. 106 (July 2000), *available at* 2000 WL 19802210. Nelson explains the attraction for businesses, including "instant connectivity" with consumers, the ability to conduct sales, advertising, and customer service through a single media and at a lower cost. *See id.*

6. *See id.*

7. There are an estimated 152 million Internet consumer users worldwide and their numbers are increasing each year. *Id.* (citing Victoria Pasher, *Insurers Falling Behind in*

E-businesses confront risks that are of a different character than those of business operations that involve storefronts, inventories, and physical plants.[9] Even a new vocabulary has developed around the new risks that Internet businesses face.[10] The perils[11] that threaten an Internet-based business include such risks as information theft,[12] insertion of malicious codes,[13] denial of service attacks,[14] access violations, failure of computer

---

Internet Race, NAT'L UNDERWRITER PROP. & CASUALTY-RISK & BENEFITS MGMT. EDITION, Mar. 10, 1997, at 1).

8. E-commerce growth has been phenomenal. Estimates of the amount of business over the net are available at http://www.emarketer.com. Business-to-business e-commerce represents the largest slice of business. *See* Nelson, *supra* note 5 (noting that 92% of the $1.4 trillion Internet business projected for 2003 will be between businesses, rather than consumer purchases). *See also* ActivMedia Research LLC, *The Real Numbers BEHIND 'Net Profits '98*, Apr. 1998, at http://www.activmediaresearch.com/real_number_1998.html.

9. *See* Shirish Nadkarni, *Love Bug Losses Outside Remit of Cyber-policies*, INS. DAY, May 9, 2000, at 12.

10. For a detailed description of cyber-crimes, see Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 COMPUTER & HIGH TECH. L.J. 177 (2000).

11. These insurance "perils" are "challenges" to a new breed of criminal with extensive computer expertise. *Id.* at 181. Hackers are computer users intent upon gaining unauthorized access to a computer system. *Id.* Crackers are hackers "with criminal intent." *Id.* at 182. Hackers may be politically motivated, disgruntled employees, common criminals, or "recreational hackers," *see id.* at 182-86, seeking "the thrill of the challenge or . . . bragging rights in the hacking community." *Id.* at 185.

12. "Information theft, the appropriation of data transmitted over computer networks or stored in networked computers. This could include credit card numbers, customer lists or marketing information that could be used by competitors." Len Strazewski, *E-commerce: Avoiding Land Mines While Chasing the Gold Mines*, ROUGH NOTES, Apr. 1, 1999, at 48, *available at* 1999 WL 14748686 (describing seven common risks identified by IBM and Fidelity & Deposits, a financial service firm, in assessing industry risk). The 2001 Computer Crime and Security Survey from the Computer Security Institute (a trade organization of computer security specialists), with cooperation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad of principally large corporations and government agencies reports that "the most serious financial losses occurred through theft of proprietary information (34 respondents reported $151,230,000) and financial fraud (21 respondents reported $92,935,000)." Press Release, Patrice Rapalus, Director, Computer Security Institute, Financial Loses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar (Mar. 12, 2001), *at* http://www.gocsi.com/prelea/000321.htm [hereinafter CSI Press Release].

13. *See* Sinrod & Reilly, *supra* note 10, at 215-26 (describing methods and objectives of inserting malicious codes including "viruses, worms, and Trojan programs"); Daniel J. Langin et al., *Virus Insurance: Issues and Answers*, NAT'L UNDERWRITER PROP. & CASUALTY-RISK & BENEFITS MGMT. EDITION, Sept. 11, 2000, at 33, *available at* 2000 WL 10594047 (describing nature and effects of malicious codes); Strazewski, *supra* note 12. Viruses are aptly named, for they occur at least as frequently as the common cold occurs in

security,[15] programming errors,[16] and misuse or misappropriation of intangible assets.[17] Employees pose the biggest threat to a business's computer resources.[18] Dishonest employees and former employees steal proprietary and other confidential information, and disgruntled employees attack their employer's computer systems more frequently than outsiders.[19]

In the new frontier of cyberspace, the risks to e-businesses are extraordinarily pervasive.[20] Surveys indicate that 90% of businesses have

---

humans. In the CSI survey, 94% of respondents detected computer viruses last year. CSI Press Release, *supra* note 12.

14. *See generally* Sinrod & Reilly, *supra* note 10, at 189-203 (describing methods and objectives of denial of service attacks). "Denial of Service, or failure of transactional services that have been promised to customers. This risk involves slow down or failure of Internet servers during extremely high volume of interaction." Strazewski, *supra* note 12. CSI reports that 38% of survey respondents detected denial of service attacks. CSI Press Release, *supra* note 12.

15. *See* Strazewski, *supra* note 12. In the CSI survey of large corporations and government agencies, 85% detected computer security breaches. CSI Press Release, *supra* note 12.

16. *See* Panko, *infra* note 30 (discussing programming errors).

17. "Social engineering, or various human activities to misuse trust to obtain access, passwords, services or other unapproved value from a computer system." Strazewski, *supra* note 12.

18. *See* Sinrod & Reilly, *supra* note 10, at 184.

19. *Id.* at 184-85. In fact, some estimate that company insiders commit 80% of attacks and 71% of unauthorized access. *Id.* at 185 (citing Mathew Nelson, *Internet Security Systems' Chris Klaus Says Companies Should Close Back Doors to Be Secure*, INFOWORLD, Jan. 10, 2000, at 40a).

20. The computer is a great equalizer. Indeed, one individual can wreak havoc on large corporations and governments:

> One person with a computer, a modem and the requisite knowledge and skills has the capacity to wreak considerable havoc. The "I love you" virus, for example, caused an estimated $6.7 billion in damages in the first 5 days. . . . Such figures have to be treated very cautiously as the underlying methodology for the calculation is not always clear. Nevertheless, there can be little argument about the extent of the disruption. Even more striking, the effects were caused by a single individual with poor support and little preparation. While the love bug should have been an obvious wake-up call because of its enormous cost, the impact was lessened because these costs were so diffused among business, government, and educational institutions as well as individual computer users. As a result, the sense of threat was also diffused thus lessening the degree of concern that would have been generated had the impact and costs been more focused. The lesson though was very clear: the development of national and global information systems has outpaced appropriate safeguards and security measures. This provides new targets and new opportunities for criminal organizations, terrorist

experienced computer security breaches,[21] and losses to U.S. businesses in 1998 were estimated to have "exceeded $200 billion."[22] CERT, Carnegie Mellon's federally funded center studying Internet vulnerabilities and attacks, reported dramatic increases in Internet security breaches over the past decade.[23] The Love Bug e-mail virus, introduced in 2000, is estimated to have caused worldwide losses of $15.3 billion in computer downtime and software damage.[24] "[T]here are an estimated 30,000 computer viruses in existence today" with "approximately 300 new viruses created each month."[25] Moreover, most businesses are unprepared to manage the risks as their shift to this business form outpaces implementation of risk management measures.[26]

The risks associated with conducting business on the Internet cannot be regarded as mere inconveniences to e-businesses. Even the short-term unavailability of a website may have long-term consequences in the electronic business world. E-customers are regarded as extremely fickle and expect both speed and reliability from those with whom they do business. For example, web surfers reportedly will wait only an average of eight seconds for a site to load before abandoning the website for another

---

> groups and hostile nations. To expect that they will fail to exploit these opportunities would not only be a mistake but also would run counter to early indications of such activity.

Phil Williams et al., *Intelligence Analysis for Internet Security*, Carnegie Mellon Software Engineering Institute, *at* http://www.cert.org/archive/html/Analysis10a.html (last visited Nov. 10, 2001).

21. John Conley, *Outwitting Cybercriminals*, 47 RISK MGMT. 18, 21 (2000). A 1999 survey of 342 companies revealed that 91% suffered hacking incidents in the past year. *Id.*

22. Ron Lent, *Anti-hacker Coverage in Demand*, J. COM., Aug. 26, 1999, at 10, *available at* 1999 WL 6382580.

23. CSI reported that "Eighty-five percent of respondents (primarily large corporations and government agencies) detected computer security breaches in the last twelve months" and that "[s]ixty-four percent acknowledge financial losses due to computer breaches." *CSI Press Release*, *supra* note 12. The 35% of respondents willing or able to quantify the losses placed them at $377,828,700. *Id.* *See* CERT COORDINATION CTR, CARNEGIE MELLON UNIV., *CERT/CC Statistics 1988-2001* (Apr. 2000), *available at* http://www.cert.org/stats/cert_stats.html (last modified Oct. 15, 2001).

24. Craig Harris, *Cyber Peril*, CAN. INS., Aug. 1, 2000, at 1719, *available at* 2000 WL 16873900, at *2.

25. Sinrod & Reilly, *supra* note 10, at 216 (citing CERT data).

26. Barbara Bowers, *Getting a Grasp on E-Commerce Risks*, BEST'S REV., Mar. 1, 2001, at 57, *available at* 2001 WL 12285238 (describing survey findings that risk managers acknowledge they are inadequately prepared to manage technology risks).

location.[27] Thus, web-based businesses perceive even brief interruptions and slowdowns as potentially devastating.[28]

Errors in programming and in operating computers are a significant source of loss as well.[29] Despite our perception that computers are accurate, in fact, errors and computing go hand-in-hand.[30] Programming

---

27. *See* Christine Y. Chen & Greg Lindsay, *How to Lose a Customer In a Matter of Seconds*, FORTUNE, June 12, 2000, at 326, *available at* http://library.northernlight.com/LH20000601010000222.html; Laura Wonnacott, *The Speed of Business: If Your Pages are Slow, Your Customers Will Go*, INFOWORLD, Sept. 8, 2000, *available at* http://www.infoworld.com/articles/op/xml/00/09/11/000911opsavvy.xml; Keynote Systems, *The Economic Impacts of Unacceptable Web Site Download Speeds* (1999), *at* http://www.keynote.com/solutions/assets/applets/wp_downloadspeed.pdf (last visited Nov. 10, 2001).

28. Mark Leon, *Balancing e-Business Opportunity and Risk*, INFOWORLD, May 12, 2000, *available at* http://www.infoworld.com/articles/su/xml/00/05/15/000515sucover_cto.xml (last visited Nov. 10, 2001). *See* Doug Levy & Janet Kornblum, *Web-Site Outages Can Send Customers Scurrying*, USA TODAY, June 15, 1999, at 1B (reporting on an increasing customer intolerance to site unavailability and willingness to switch to a competitor); Sally Whitney, *Risky Business in Cyberspace*, BEST'S REV., June 1, 2000, at 143 ("If an Internet company is offline for 72 hours, it may be down for good.").

29. *See, e.g.*, Paul Gillin, *Crashing Successes*, COMPUTERWORLD, Mar. 8, 1999, at 34, *available at* 1999 WL 5936206 (reporting on server crashes at Charles Schwab, a business doing 60% of its volume online); Levy & Kornblum, *supra* note 28, at 1B (reporting a failure rate at top e-commerce sites of 4.45% and reporting that a nearly 30 hour outage at eBay cost up to $5 million); Sara Nathan, *Amazon.com Site Crashes for Second Time*, USA TODAY, Dec. 1, 2000, 1B (reporting on "internal bugs" that resulted in two site crashes of 15 and 30 minutes).

30. Software engineers recognize that no amount of testing will produce error free programs, only that employing multiple testing mechanisms reduces the number of errors. *See* T. CAPERS JONES, ESTIMATING SOFTWARE COSTS, 554-61 (McGraw-Hill Education Group 1998). Consider this comment on the inevitability of software errors:

> Human error research indicates that human error is tenacious because people are not terribly good at detecting and correcting errors. The Human Error website at http://panko.cba.hawaii.edu/HumanErr/Proofrd.htm shows that error detection and correction rates approaching 90% only occur in the simplest processes, such as proofreading for spelling errors in which the misspelling is not itself a valid word. If the result of the spelling error is itself a valid word, error detection rates fall to about 70%. Even this is high compared to error detection and correction for logical errors in mathematics, which in Allwood's classic study succeeded in only about half of all errors. Error detection and correction for omission errors is much lower still.
>
> More directly, the Human Error website has data from a number of software team code inspection studies, in which a *group* of programmers goes over a program one line at a time to look for errors.

errors and resulting defects in computer software design are inevitable,[31] and expose computer-dependent businesses to substantial losses.[32]

II. STRETCHING TRADITIONAL FIRST PARTY INSURANCE TO FIT NEW FORMS OF PROPERTY AND BUSINESS OPERATIONS

Although "most businesses seem to have assumed that their activities on the Internet are covered by their existing policies,"[33] that assumption is uncertain at best.[34] Policyholders might assume that traditional first party

---

> These intensive code inspections only find around 80% of all errors despite the use of team code inspection by programming professionals.
>
> . . . .
>
> Software developers, who are highly experienced with errors, respond to the difficulty of detecting errors by engaging in massive amounts of formal testing. About a third of the total software development effort goes into formal testing, and even after several stages of testing, errors remain in about 0.1% to 0.3% of all lines of code.

Raymond R. Panko, *Spreadsheet Errors: What We Know. What We Think We Can Do*, Proceedings of the Spreadsheet Risk Symposium (July 17-18, 2000), *at* http://panko.cba.hawaii.edu/ssr/Mypapers/EUSPRIG_2000.htm (last visited Nov. 10, 2001).

31. *See* Jube Shiver, Jr., *FAA Software Flaw Spotlights Malady of Digital Age Aviation: The Glitch In Palmdale that Delayed Air Traffic is Blamed on Coding and on Insufficient Testing and Controller Training*, L.A. TIMES, Oct. 27, 2000, at C1, *available at* 2000 WL 25911869. On October 19, 2000, installation of the Federal Aviation Administration's new software shut down air traffic across southwestern United States for several hours. *Id.* "The problem at Palmdale—one of the nation's busiest traffic control centers—stemmed from a previously unknown bad instruction among 250,000 lines of computer code in the multimillion – dollar FAA software upgrade system." *Id.*

32. *See, e.g.*, Joe Kilsheimer, *Glitch Costs AOL Users on Packard Bell-NECs: A Programming Error in Computers Sold in January is Responsible for Huge Online Charges*, ORANGE COUNTY REG., Mar. 13, 1997, at C3, *available at* 1997 WL 7421277; Jon Van, *Software Bugs Turning Deadly in Complex Era*, CHI. TRIB., Dec. 14, 1986, at 1 (discussing dangers of "lethal bugs" in software involving aviation, medicine and NASA and prevalence of programming errors).

33. Nelson, *supra* note 5. "Insurance products were developed for another day and age, and when you try to apply traditional insurance policies to the same perils on the Internet, there may be no coverage or large gray areas where coverage is unclear." Whitney, *supra* note 28, at 143. *See also* EUGENE R. ANDERSON ET AL., INSURANCE COVERAGE LITIGATION § 18.01, at 18-5-18-6 (2d ed. Supp. 2000).

34. Nelson, *supra* note 5. Nelson acknowledges that even some insurers assume that the Internet is merely another mode of distribution and so covered under existing policies. *Id.* He cautions that neither the premiums charged under existing policies nor the contract language adequately account for the risk additional exposures pose, including the consequences of expanding from a local region to a worldwide audience and the nature of the risks themselves. *Id.*

policies can and should stretch to provide coverage in the absence of clear exclusions,[35] but insurers insist that cyberlosses are not the intended underwritten risks of traditional insurance products.[36] There are few reported decisions because these controversies have arisen only recently,[37] and a lack of judicial guidance at the very least leaves insureds under traditional policies uncertain as to coverage for some of their most valuable assets, and insurers uncertain as to the scope of their exposure.[38]

---

35. Robert L. Carter, Jr. & Donald O. Johnson, *Coverage for Computer Viruses*, NAT'L L.J., June 5, 2000, at B9 (attorneys representing policyholders asserting there may be coverage for viruses); Roberto Ceniceros, *Managing e-commerce risks: New coverage introduced to protect against first-party and third-party risks*, BUSINESS INS., Jan. 24, 2000, at 1, *available at* 2000 WL 8170344 (quoting policyholder attorney who argues that all-risk policies do cover cyber attacks); Cohen & Anderson, *supra* note 3, at 892, 927; and Dimitry Elias Léger, *Why Internet Insurance Isn't the Best Policy*, FORTUNE, July 10, 2000, at 260, *available at* 2000 WL 3462446 (quoting policyholder attorneys arguing that current all risk policies do cover cyber attacks) make a strong case for insureds. The authors analyze traditional first party policies and assert that these policies do cover a substantial amount of e-commerce first party losses.

36. *See* Conley, *supra* note 21, at 22; Freeman, *supra* note 3, at 22, 25-26; Hann, *supra* note 3, at 74-75; Harris, *supra* note 24, at 1719; Langin, *supra* note 13; Nelson, *supra* note 5.

37. CGL decisions are not particularly analogous. *See* INS. SERVS. OFFICE, INC., COMMERCIAL GENERAL LIABILITY COVERAGE FORM CG 00 01 07 98, at 13 (1997) (on file with author), *available at* Alliance of American Insurers, The Insurance Professionals' Policy Kit (2000 ed.). A CGL policy commonly defines property damage differently; it includes either physical injury to or loss of use of tangible property. *Id.* Decisions related to loss of intangibles such as data or loss of use due to defective programs have been variable under the CGL. *See, e.g.*, Seagate Tech., Inc. v. St. Paul Fire & Marine Ins. Co., 11 F. Supp. 2d 1150 (N.D. Cal. 1998) (holding that under a CGL policy, insured's defective disk drives did not cause physical damage to tangible property where disks did not harm the other parts of the computer but only failed to operate properly); Magnetic Data, Inc. v. St. Paul Fire & Marine Ins. Co., 442 N.W.2d 153 (Minn. 1989) (suggesting but not determining that under a CGL policy, accidental erasure of data from client's disk does not constitute loss of use of tangible property); St. Paul Fire & Marine Ins. Co. v. Nat'l Computer Sys., Inc., 490 N.W.2d 626 (Minn. Ct. App. 1992) (holding that under a CGL policy, employee's misappropriation of client's proprietary information does not constitute damage to tangible property); Retail Sys., Inc. v. CNA Ins. Co., 469 N.W.2d 735 (Minn. Ct. App. 1991) (holding that under a CGL policy, disappearance of client's computer tape constituted physical injury or destruction of tangible property).

38. *See* Nelson, *supra* note 5. Not only are perils unique, a business's shift from a storefront to an expanded Internet business operation increases the scope and magnitude of risks and losses. *Id. See also* Whitney, *supra* note 28, at 143 ("[t]hese exposures have been changed by the severity, the global scale and the potential number of claimants.").

A. Traditional Insurance Contracts Insure Physical Property Against Physical Perils

The drafters of existing, traditional first party policies did not anticipate the public embrace of the parallel world called cyberspace. These traditional insurance policies generally aim to protect tangible property from the perils of a physical world; they suit a world with a corporeal quality. In some instances, the policies do not insure the property that an e-business values. For example, while a property policy will likely insure computer hardware and software in its physical form,[39] some policies provide that property does not include "[t]he cost to research, replace, or restore the information on valuable papers and records, including those which exist on electronic or magnetic media."[40] Thus, the effort to replace or restore data and other valuable computer stored information may not constitute covered property under a traditional policy. Yet, for many e-businesses, the electronic storage and management of documents and information may constitute the equivalent of valuable inventory.

If a named-peril policy is purchased, the narrow causes of losses particular to e-businesses, such as the damage caused by the insertions of malicious codes and viruses, the theft of computer time or services through unauthorized use and access, and the losses related to programming and operating mistakes, may not be covered.[41] While the common perils of the physical world, such as fire and flood, can damage a computer, these are not the principal perils e-businesses fear.

A traditional all-risk[42] policy also has coverage infirmities, although in principle, an all-risk policy form covers any peril that is not expressly

---

39. *See* INS. SERVS. OFFICE, INC., BUILDING AND PERSONAL PROPERTY COVERAGE FORM CP 00 10 06 95, at 1 (1994) [hereinafter ISO, BUILDING FORM].

40. *See id.* at 2. A limited coverage extension is available for up to $2,500 to research, replace or restore lost information. *Id.* at 5.

41. INS. SERVS. OFFICE, INC., CAUSES OF LOSS – BASIC FORM CP 10 10 06 95, at 1 (1994) and INS. SERVS. OFFICE, INC., CAUSES OF LOSS – BROAD FORM CP 10 20 06 95, at 1 (1994) (fire; lightning; explosion; windstorm or hail; smoke; aircraft or vehicles; riot or civil commotion; vandalism (willful and malicious damage to, or destruction of, described property); sprinkler linkage; sinkhole collapse; volcanic action). Arguably, a virus could be characterized as vandalism, but the cost to restore information may not be a covered loss.

42. For example, ISO's Causes of Loss-Special Form is an "all-risk" policy. INS. SERVS. OFFICE, INC., CAUSES OF LOSS – SPECIAL FORM CP 10 30 06 95, at 1 (1994) [hereinafter ISO, SPECIAL FORM]; Sawyer v. Farm Bureau Mut. Ins. Co., No. 21267, 2000 WL 1728486, at *2 (S.D. Nov. 21, 2000).

excluded or limited.[43] These policies sometimes limit coverage for loss or damage to "valuable papers and records" including "film, tape, disc, drum, cell or other data processing,"[44] and therefore will be of limited use if the principal injury is the loss of intangibles stored on a computer. And, where an all-risk policy limits coverage for losses caused by "faulty, inadequate or defective design, specifications, [or] workmanship"[45] unless a named peril results, it may not cover the kinds of loss that programming errors cause. Furthermore, although employees are the greatest source of loss for an e-business,[46] losses due to employee theft, dishonesty and crimes are often expressly excluded under an all-risk policy.[47]

One of the greatest obstacles to coverage in either all-risk or named peril policies is the required trigger of actual loss, common to traditional policies. Generally, first party property coverage is triggered only where "direct physical loss of or damage" occurs to covered property.[48] Direct

---

43. An "all risk" policy "covers the insured for damage to the subject matter of the policy from all causes except those specifically excepted in the policy." ROBERT H. JERRY, II, UNDERSTANDING INSURANCE LAW § 60A, at 337 (2d ed. 1996). As Jerry notes, while all-risk policies have some advantages, "[c]overage under all-risk policies is hardly absolute. . . . [E]xclusions can take away much of what the all-risk policy gives. These exclusions are often very difficult to understand and apply; the expectations of the insured who thinks 'all-risk' coverage means the insurer will reimburse loss are often disappointed." *Id.* at 338.

An all-risk policy critically shifts the burden of proof in favor of the insured with regard to coverage.

> [U]nder a specified-risk policy [the insured] must establish not only that a loss occurred but also that the loss was caused by one of the specified covered perils. Once this showing is made, the burden shifts to the insurer to show an applicable exclusion, if any. In contrast, the all-risk insured needs to establish only that a loss occurred; the burden then shifts to the insurer to show that the loss was caused by an exception. Thus, where the cause of the loss is difficult to identify and prove, an all-risk policy can be highly beneficial to the insured.

Id. at 339. Nevertheless, under a typical all-risk policy the plaintiff still must initially establish that a fortuitous event constituting physical loss or damage occurred. *See* HRG Dev. Corp. v. Graphic Arts Mut. Ins. Co., 527 N.E.2d 1179, 1180 (Mass. App. Ct. 1988).

44. ISO, SPECIAL FORM, *supra* note 42, at 5.

45. *Id.* at 5, 7. There is coverage if the loss is caused by specified perils – principally those of the broad and basic causes of loss form. *See also* JEFFREY W. STEMPEL, LAW OF INSURANCE CONTRACT DISPUTES § 23.03[a] (2d ed. 2000) (noting that the latent defect exclusion may pose obstacle to coverage in Y2K context).

46. *See supra* notes 18-19 and accompanying text.

47. ISO, SPECIAL FORM, *supra* note 42, at 3.

48. ISO, BUILDING FORM, *supra* note 39, at 1. *See also*, LEE R. RUSS, 10 COUCH ON INSURANCE § 148:46 (3d ed. 2000) (discussing physical loss or damage trigger in property insurance).

physical loss or damage may be difficult to establish when a computer's functioning is disrupted, but there is no perceivable physical loss or damage to the system itself.[49]

Fundamentally, insureds and insurers disagree over whether events such as hacking, program errors, and attacks, cause direct physical loss or damage. Arguably, one can characterize changes within the computer caused by a virus as physical[50] because a magnetic change occurs within the computer's memory, even though the code may or may not produce damage to the computer's hardware or software.[51] However, insurers will argue that these changes do not constitute physical damage, instead characterizing an attack on a computer as "a temporary disruption of intangible electronic information," which produces no physical damage.[52] Certainly, insurance battles over other invisible, subtle forms of damage, such as the presence of asbestos fibers,[53] mold spores,[54] odors[55] and

---

49. *See* Langin, *supra* note 13 (asserting that most courts will hold that there is "no coverage for loss of data if there is no damage to the medium on which data is stored."); Nelson, *supra* note 5.

50. *See, e.g.*, STEMPEL, *supra* note 45, at § 23.07; Cohen & Anderson, *supra* note 3, at 902; Bruce Hillman, *Which Insurance Coverage Has the Cure for Computer Virus Infection Damages?*, NAT'L UNDERWRITER PROP. & CASUALTY-RISK & BENEFITS MGMT. EDITION, May 24, 1999, *available at* 1999 WL 8859468.

51. A virus is a program code that is comprised of bits, binary digits of 0 or 1. ALAN FREEDMAN, THE COMPUTER GLOSSARY 48 (6th ed. 1993). Bits have a physical form: "Within the computer, a bit is physically a memory cell (made up of transistors or one transistor and a capacitor), a magnetic spot on disk or tape or a pulse of high or low voltage travelling through a circuit." *Id.* at 48-49.

52. Walter J. Andrews & Edward J. Grass, *Curing the Fever for Virus Coverage Under Traditional Property Policies*, MEALEY'S CYBER TECH LITIG. REP., Aug. 2000, *available at* http://www.mealeys.com/teccom.html (last visited Nov. 10, 2001) ("[A]t the end of the day when a virus is removed, and even during the infestation, all of the computer systems should be 'physically' unharmed and fully capable of performing their desired functions."). *See* Hann, *supra* note 3, at 75. *Cf.* Hillman, *supra* note 50 (arguing that corruption of files, operating systems and firmware constitutes physical damage).

53. *See, e.g.*, Bd. of Educ. of Township High Sch. Dist. No. 211 v. Int'l Ins. Co., 720 N.E.2d 622, 625-26 (Ill. App. 1999) (presence of friable asbestos fibers constitutes physical injury to property). *But see* Great N. Ins. Co. v. Benjamin Franklin Fed. Sav. & Loan Assoc., 793 F. Supp. 259, 263 (D. Ct. Or. 1999), *aff'd*, 953 F.2d 1387 (9th Cir. 1992).

54. Columbiaknit, Inc. v. Affiliated FM Ins. Co., No. Civ. 98-434-HU, 1999 WL 619100, at *7 (D. Ct. Or. Aug. 4, 1999) (holding insured suffered physical loss where fabric exposed to high humidity following flooding became moldy).

55. *See, e.g.*, W. Fire Ins. Co. v. First Presbyterian Church, 437 P.2d 52 (Colo. 1968) (en banc); Farmers Ins. Co. of Oregon v. Trutanich, 858 P.2d 1332, 1334 (Or. App. 1993) (odor from methamphetamine cooking constituted direct physical loss under property insurance policy).

gasses,[56] in otherwise undamaged property, will assist insureds claiming that insertions of malicious codes and events causing data loss constitute physical loss, even though other computer components are undamaged.

Typical business interruption coverage presents equally formidable obstacles for many of the kinds of losses suffered and is therefore unsuitable for insureds seeking certainty of coverage. While some events may be covered,[57] the traditional business interruption policy is largely ill-equipped to cover the kinds of risks e-businesses face because these policies are similarly grounded in the concepts of physical damage and loss.[58] One thorny dispute here will be whether the interruptions caused by unauthorized intrusions by hackers, insertions of viruses and other malicious codes, or programming errors that disrupt operations is "caused by direct physical loss of or damage to property."[59] Conceptually some kinds of attacks, such as a denial of service attack that disrupts business operations, will be difficult to so characterize because these attacks inundate and overwhelm a computer system, yet leave no trace of physical loss or damage.[60]

E-businesses may find traditional business interruption insurance incompatible with their need to insure against slowdowns and brief interruptions. Traditional business interruption coverage requires that the insured suffer a "distinct suspension of operations,"[61] not merely a lesser event such as a slowdown or a smaller disruption of operations.[62] An e-

---

56. Matzner v. Seaco Ins. Co., No. Civ. A 96-0498-B, 1998 WL 566658, at *6 (Mass. Super. Aug. 12, 1998) (presence of carbon monoxide constitutes direct physical loss or damage).

57. For example, a business income and extra expense policy may pay for losses of business income caused by "direct physical loss of or damage" to Electronic Media and Records. INS. SERVS. OFFICE, INC., BUSINESS INCOME AND EXTRA EXPENSE COVERAGE FORM CP 00 30 06 95, at 6 (1994) (adding limitations on the duration of coverage).

58. *See generally* STEMPEL, *supra* note 45, § 22.02, 22-13-22-16. As in the property context, the cause of losses are either named perils or all risks with limitations and exclusions. *See, e.g.*, ISO, SPECIAL FORM, *supra* note 42, at 1.

59. *Id.*

60. *See* Hann, *supra* note 3, at 75.

61. STEMPEL, *supra* note 45, § 22.02, at 22-14. "To have [Business Interruption] coverage, the policyholder must close the business or a particular store or department because of property damage." *Id.*

62. *See Id.* at 22-24-22-25; Home Indem. Co. v. Hyplains Beef, L.C., 893 F. Supp. 987, 991 (D. Kan. 1995). Some judicial decisions have ameliorated this requirement. *See* Cohen & Anderson, *supra* note 3, at 917 (noting split of authority and commenting that better reasoned opinions find a conflict between the suspension of business clause and the clause requiring mitigation of losses). *Compare* Keetch v. Mut. Enumclaw Ins. Co., 831 P.2d 784 (Wash. Ct. App. 1992) (holding no coverage for mere diminution in level of business), *and*

business may find a lack of coverage for losses due to transitory interruptions that slow, but do not halt business.

Similarly, a significant obstacle to coverage in the crime and employee dishonesty policies is that these policies[63] anticipate damage or theft to physical things. In addition to the theft of money and securities, the principal property insured under a standard crime policy is "any tangible property other than 'money' and 'securities' that has intrinsic value."[64] Thus, misuse or misappropriation of intangible property and losses such as the theft of computer time, services, and data will probably not be covered.[65]

B. Square Pegs in Round Holes, Making Traditional Policies Fit

These traditional insurance contracts are steeped in words that connote physical damage to tangible property. Yet, in the transition from the "bricks and mortar" business model to a "clicks and bricks"[66] business model, insureds will increasingly demand that their traditional insurance contracts cover the conceptually new types of losses that attend e-business. During this transitory period, at least until insurers amend traditional policies by drafting tighter exclusions, claims for coverage under traditional insurance polices may succeed.

As to just how far a court can stretch to find coverage under a traditional insurance contract, *American Guarantee & Liability Insurance*

Hotel Props., Ltd. v. Heritage Ins. Co. of Am., 456 So. 2d 1249 (Fla. Dist. Ct. App. 1984), *with* Am. Med. Imaging Corp. v. St. Paul Fire & Marine Ins. Co., 949 F.2d 690 (3d Cir. 1991) (holding that the obligation to indemnify could arise where insured suffers a reduction in business).

63. There are a variety of endorsements for computer crime and fraud available to include in a conventional insurance policy. *See* Gary J. Valeriano, *Pitfalls in Insurance Coverage for "Computer Crimes,"* 59 DEF. COUNS. J. 511 (1992) (discussing coverage issues under standard crime policies).

64. INS. SERVS. OFFICE, INC., CRIME GENERAL PROVISIONS LOSS SUSTAINED FORM CR 10 00 04 97, at 4 (1996). *See Hyplains*, 893 F. Supp. at 990 (asking but not resolving the "interesting questions" in context of business interruption coverage, "whether there could in fact be a 'direct physical loss' to the electronic data which was allegedly collected but never existed in a tangible form," and whether "it in fact [was] lost or rather did it never come into existence.").

65. Valeriano, *supra* note 63, at 512.

66. Bricks and mortar to clicks and bricks describe a company's transformation from doing business in a physical location to one conducting e-commerce. *See, e.g.*, *TeleTech Awarded Long-Term Contract with Allstate*, PR NEWSWIRE, Feb. 24, 2000, *available at* LEXIS, News Library, Wire Service Stories File ("Teletech continues to break new ground by helping outstanding companies transform from bricks-and-mortar to clicks-and-mortar.").

Co. v. Ingram Micro, Inc.,[67] is insightful. The case sounded an alarm throughout the insurance industry, perhaps because it may serve as a bellwether of decisions in the near future.[68] An examination of how the court reached its determination that the loss of programming in a

---

67. Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. Civ. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000).

68. The case was widely reported in the industry news media drawing considerable negative commentary and predictions of increased exposure. *See, e.g.*, Andrews & Grass, *supra* note 52; Bernard P. Bell, *Newer Twists in Insurance Coverage*, THE NAT'L L.J., Aug. 21, 2000, at C13, C15 (discussing conflicting decisions); Barbara Bowers, *Arizona Ruling on Computer Crashes May Affect Property Insurers*, BEST'S INS. NEWS, June 7, 2000, *available at* 2000 WL 4086485; Bowers, *supra* note 26 (quoting insurance industry executives as watching case "very closely" but considering it "an anomaly"); Cohen & Anderson, *supra* note 3, at 903-04; Adam H. Fleisher, *What's Wrong with Ingram Micro*, 3 NO. 11 MEALEY'S YEAR 2000 REP. 19 (Dec. 2000) (criticizing court's ruling as waving "magic wand," "tortur[ing] the language of a policy to create ambiguities" and "creat[ing] coverage where none was intended"); Craig Harris, *Stretching the Pockets*, 106 CAN. INS. 3, Apr. 1, 2001, *available at* 2001 WL 15727076 (commenting on case's "tortured logic to stretch wordings and make them fit"); *Insurers Keen to Cyber-proof Wordings*, 106 CAN. INS. 6, Feb. 1, 2001, *available at* 2001 WL 15727047 (warning that Canadian courts may look to this decision for guidance); Langin, *supra* note 13, at 33; Léger, *supra* note 35, at 260 (discussing the case and noting insurers regard it as an aberration); John Leming, *E-coverage Alert: Ingram Micro Decision Sets New Precedent*, RISK MGMT. Aug. 2000, at 12 (discussing impact of decision on insurance industry) [hereinafter Leming, *E-coverage*]; John Leming, *Ruling Allows E-commerce Damages*, J. COM., May 31, 2000, at 8 (warning of "profound implications" of the decision); Dave Lenckus, *Insurer Seeks Quick Appeal of Data Coverage Ruling*, BUS. INS., June 12, 2000, at 1, *available at* 2000 WL 8171269 (discussing impact of case); Dave Lenckus, *Loss Prevention to Be Next Focus of Battle Over Data Coverage*, BUS. INS., June 19, 2000, at 1, *available at* 2000 WL 8171296; Diana B. Reitz, *Is Tech Revolution Creating New Cat Risks?*, NAT'L UNDERWRITER PROP. & CASUALTY-RISK & BENEFITS MGMT. EDITION, July 10, 2000, at 6, *available at* 2000 WL 10593435; Wim Mostert, *Physical Damage Find Broader Meaning*, BUS. DAY, June 2000, at 23, *available at* 2000 WL 20229763; *Rethinking the Computer Threat*, HA'ARETZ, May 27, 2001, *available at* 2001 WL 21429318 (warning of increasing insurance rates associated with coverage); Alan S. Rutkin, *Policies Must Be Specific*, BEST'S REV., Oct. 1, 2000, *available at* 2000 WL 22630429 (predicting more cases on this and related issues of coverage); Mark K. Slater et al., *Viruses, Hackers and Outages: Who Pays?*, MEALEY'S EMERGING INS. DISP., June 7, 2000, at 45; Vikki Spencer, *Risk Management: Danger of the Cyber Deep*, CAN. UNDERWRITER, Sept. 1, 2000, at 10, *available at* 2000 WL 16450730; State Survey, *West Zone: Ariz.*[sic] *Computer Case Roils Industry*, INS. ACCT., June 12, 2000, at 5, *available at* 2000 WL 8650196; Ara C. Trembley, *Tech Case Could Cost Insurers*, NAT'L UNDERWRITER PROP. & CASUALTY-RISK & BENEFITS MGMT. EDITION, June 5, 2000, at 1, *available at* 2000 WL 10593339; Brooks White, *E-Cat Property Catastrophe Reinsurance: Is the Cat Out of the Bag?*, MEALEY'S LITIG. REP.: REINSURANCE, Nov. 30, 2000, at 33 (criticizing opinion and warning that "courts faced with significant E-cat losses will in a balkanized fashion decide these cases in favor of local insureds and against insurers").

computer's random access memory (RAM)[69] constituted physical loss or damage demonstrates how far courts may strain to find first party coverage under a traditional policy.

At the time of the litigation, Ingram Micro was a very large distributor of computer hardware and software products, with operations in thirty-one countries. The company offered over 200,000 computer hardware and software products from 1,500 manufacturers to customers in 130 countries through 54 distribution centers.[70] It handled 150,000 or more shipments each day.[71] Ingram Micro reportedly sold approximately $14,000,000 worth of goods in each hour of operation.[72] The company processed and tracked sales, inventory and transactions through the "Impulse system, a world-wide computer network that provide[d] real-time access throughout the company's many locations. . . ."[73] Ingram Micro's data processing and database operations were located in its data center in Tucson, Arizona.[74]

On December 22, 1998, the data center lost power for approximately one half hour due to a faulty fire alarm test procedure.[75] However, even though power was restored, Ingram's mainframe computers "lost all of the programming information that had been stored in their random access memory"[76] and were rendered inoperable. Employees scrambled to reload the lost programming and restored the mainframes to operational status within ninety minutes of the power outage.[77] This, however, did not enable Ingram to resume its business, because the Tucson data center still could

---

69. Random Access Memory is the "workspace" on a computer and "RAM chips require power to maintain their content." FREEDMAN, *supra* note 51, at 436.

70. Ingram Micro Inc.'s Memorandum of Points and Authorities in Support of Motion for Partial Summary Judgment at 3, Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. Civ. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (on file with author) [hereinafter Ingram's Motion]. A description of Ingram Micro is located at http://www.ingrammicro.com (last visited Nov. 10, 2001) [hereinafter Ingram Website].

71. Ingram's Motion, *supra* note 70, at 3.

72. *Id.*

73. *Id.* Ingram, a Fortune 500 company, touts its worldwide presence, same-day shipment guarantee, 24-hour a day accessibility, and real-time ordering system. *See* Ingram Website, Company Biography.

74. Ingram's Motion, *supra* note 70, at 3.

75. Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. Civ. 99-185 TUC ACM, 2000 WL 726789, at *1 (D. Ariz. Apr. 18, 2000). According to the court, the cause turned out to be a "a ground fault in the fire alarm panel." *Id.* Apparently, the building's fire alarm system was being serviced at the time. An emergency power off device was programmed to shut off power to the data center if three fire alarms were suddenly activated. Ingram's Motion, *supra* note 70, at 4.

76. *Am. Guar. & Liab. Ins. Co.*, 2000 WL 726789, at *1.

77. *Id.*

not connect to the Impulse System. Ingram eventually identified the problem as occurring in a matrix switch that had also lost its customized programming, and returned to default settings as a result of the power outage.[78] After bypassing the matrix switch, the Impulse System was finally restored approximately eight hours after the power loss.[79]

The hardware and software at Ingram Micro were not physically damaged in the ordinary sense of the word. While the power outage resulted in a half hour shut down of the mainframe computers, the computers were not damaged when power was restored. However, the RAM within the mainframe computers had lost its stored programming information and returned to a default setting, as it inevitably would do when power was lost.[80] The programs were not damaged and Ingram Micro was able to reload the programs once the power was restored.[81] Likewise, the matrix switch lost its customized programming and returned to its default settings but was not damaged; the customized programming simply needed to be restored.[82]

---

78. Although the court states that the matrix switch malfunctioned, apparently the power outage caused the switch to lose its customized programming and return to its default settings. Ingram Micro only discovered this after consulting with the manufacturers of various computer equipment from the Data Center, and investigating and eliminating several other potential causes. Ingram's Motion, *supra* note 70, at 5-6. "The matrix switch had to be reprogrammed with the necessary custom configurations before communications with the six Impulse locations could be restored." *Am. Guar. & Liab. Ins. Co.*, 2000 WL 726789, at *2.

79. Ingram's Motion, *supra* note 70, at 6.

80. Ingram Micro explained it to the court as follows:

> Computers operate by following instructions contained in various software programs. Computers store this programming information electronically in their volatile random access memory, or RAM, as instructions written in an alphabet of 1's and 0's. These 1's and 0's are stored in the microscopic electronic switches that make up the computer's RAM. The difference between a 1 and a 0 is a difference in voltage. When power to a computer is cut off, all of these 1's and 0's disappear. When power is restored, the switches all set to 0 and remain that way until the programming information is loaded onto the computer again.

Id. at 4 (citations omitted).

81. More attention to loss prevention measures could have averted the problem. Dave Lenckus, *Loss prevention*, *supra* note 68. For approximately $100,000, the company could have installed an "'uninterruptible power supply' that shuts down a computer system 'cleanly' during a power disruption" and "nearly guarantees that data and programming will not be corrupted or lost." *Id.*

82. *Am. Guar. & Liab. Ins. Co.*, 2000 WL 726789, at *2.

In 1998, Ingram Micro purchased an "all-risk" insurance contract with three participating insurers, insuring losses up to about $127,000,000,[83] with limits for service interruption up to $50,000,000.[84] Ingram Micro's premium was over $1,256,137 per annum.[85] Ingram was insured as follows: "The policy insured against 'All Risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring, including general average, salvage charges or other charges, expenses and freight.'"[86]

Ingram Micro gave its insurer timely notice of the business interruption loss, based on its inability to conduct business for approximately eight hours. American denied coverage and filed suit for declaratory relief.[87] The issue before the court on cross-motions for partial summary judgment was "whether a 1998 power outage caused 'direct physical loss or damage from any cause, howsoever or wheresoever occurring' to Ingram's computer system."[88] American argued that Ingram Micro's equipment was not "physically damaged" because the capability of the computer system and the matrix switch "to perform their intended functions remained intact."[89] In fact, American asserted that by returning to its default settings, the system performed precisely as it was designed to do when confronted with a loss of electrical power.[90] Moreover, upon restoration of power, the system was made functional and was not damaged.[91] Ingram Micro, on the other hand, argued that the "loss of use and functionality" of its computers constituted "physical damage" under the terms of the insurance contract.[92]

Despite conflicting expert witnesses on just what constitutes physical damage within the recesses of a computer, the court held that there was no

---

83. Ingram's Motion, *supra* note 70, at 6 (CNA Insurance Company, Allianz Insurance Company, and Zurich-American through its American subsidiary). American's policy covered the larger portion, 70% of a loss up to $105,000,000. *Id.*

84. INGRAM MICRO, INC., PRIMARY ALL RISK POLICY 3 (1998) (on file with author).

85. Ingram's Motion, *supra* note 70, at 6. Ingram actually purchased $127,000,000 of insurance through the three carriers and paid total premiums of $1,256,137.89 for the coverage. *Id.*

86. *Am. Guar. & Liab. Ins. Co.*, 2000 WL 726789, at *1. The insurance contract was not a standard policy. *Id.*

87. *Id.*

88. *Id.*

89. *Id.* at *2.

90. Plaintiff American Guarantee's Response Memorandum in Opposition to Ingram Micro's Motion for Partial Summary Judgment at 3, Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. Civ. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (on file with author).

91. *Id.*

92. *Id.*

genuine issue of material fact on the issue of whether the loss of use of the computer network for eight hours constituted physical damage. The court therefore granted summary judgment to Ingram Micro.[93] In an oblique reference to an insured's reasonable expectations, the court commented, "[a]t a time when computer technology dominates our professional as well as personal lives, the Court must side with Ingram's broader definition of 'physical damage.'"[94] The court then relied upon various federal and state computer crime and fraud statutes to determine what constitutes physical damage to a computer system.[95]

The court's reliance on criminal statutes to define insurance contract terms is troublesome because the definitions within computer crime statutes have little, if any, relevance to discerning the contractual meaning of terms within in an insurance contract.[96] In addition, the court failed to note that these statutes only define what constitutes "damage" to a computer system for criminal purposes, but do not define or require "physical damage."[97] Under these statutes, criminal damage to a computer includes such events as "impairment to the integrity or availability of data, a program, a system, or information,"[98] disruption or degradation of computer services,[99] alteration,[100] "alteration, deletion, or destruction of any part of a computer

93. *Am. Guar. & Liab. Ins. Co.*, 2000 WL 726789, at *3-4. On June 13, 2000, the district court issued an order granting American permission for an interlocutory appeal, but on August 14, 2000, the Court of Appeals for the Ninth Circuit denied the petition for interlocutory appeal. *Id.* The case is now set to proceed to trial. *Id.*

94. *Id.* at *2.

95. *Id.*

96. *Cf.* Retail Sys., Inc. v. CNA Ins. Co., 469 N.W.2d 735, 738 n.1 (Minn. Ct. App. 1991) (noting that tax law cases addressing meaning of tangible property for tax purposes should not govern insurance cases). In the absence of clear definitions, some scholars have also turned to these statutes to define the damage under the insurance contract. *See, e.g.*, Cohen & Anderson, *supra* note 3, at 900.

97. Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000) ("From these definitions, it can be concluded that when a large volume of UBE causes slowdowns or diminishes the capacity of AOL to serve its customers, an 'impairment' has occurred to the 'availability' of AOL's 'system.'"); *cf.* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020-22 (S.D. Ohio 1997) (evaluating trespass claim against defendant who wrongfully sent unsolicited e-mail in violation of terms of contractual agreement with CompuServe and holding that the "demand of disk space and drain of processing power" constitutes "physical dispossession" of the property although there was no "physical damage" to plaintiff's property).

98. *Am. Guar. & Liab. Ins. Co.*, 2000 WL 726789, at *2 (citing 18 U.S.C. § 1030 (West 1999)).

99. *Id.* (citing CONN. GEN. STAT. § 53a-251 (2000)).

100. *Id.* (citing MINN. STAT. § 609.88 (1999)).

system or network,"[101] or alter[ing] or destroy[ing] computer data.[102] Notably absent from these statutes is any requirement that a perpetrator cause any *physical* damage; presumably the awkward fit between these cyber-crimes and crimes of the physical world such as theft, property damage and trespass, initially necessitated these particular statutes.

The court found the insurer's experts' conclusions that no physical damage occurred "unreasonable," and placed the temporary loss of programming information into a physical construct based upon the physical acts required to restore the system:

> In this case, Ingram does allege property damage-that as a result of the power outage, Ingram's computer system and world-wide computer network physically lost the programming information and custom configurations necessary for them to function. Ingram's mainframes were 'physically damaged' for one and one half hours. It wasn't until Ingram employees manually reloaded the lost programming information that the mainframes were 'repaired.' Impulse was 'physically damaged' for eight hours. Ingram employees 'repaired' Impulse by physically bypassing a malfunctioning matrix switch. Until this restorative work was conducted, Ingram's mainframes and Impulse were inoperable.[103]

However, not all courts agree that the loss of use of a computer without discernable damage to its components constitutes physical damage.[104] The

---

101. *Id.* (citing MO. ANN. STAT. § 569.093 (West 1999)).

102. *Id.* (citing N.Y. PENAL § 156.20 (McKinney 1999)).

103. *Id.* at *3. The notion that a computer that does not perform and requires physical effort to repair must have suffered physical damage is very similar to Professor Stempel's assertions in discussing the "physical injury" requirement in the context of Y2K insurance coverage: The year 2000 problem

> is similarly detectable to a computer diagnostician. It can be seen, spotted in the program, is physically represented by lines of programming code, and so on. . . . In addition, the damaged computer system does appear to have material manifestations of injury. The machine will not perform basic tasks. The screen records an error message. The keyboard is locked; only shutting off the power (even though you are not supposed to without first exiting the program) will unlock the system. Overall, this looks like physical injury.

STEMPEL, *supra* note 45, § 23.07, at 23-63.

104. For example, in the liability insurance context, *Seagate Technolgy, Inc. v. St. Paul Fire and Marine Insurance. Co.*, 11 F. Supp. 2d 1150 (N.D. Cal. 1998), held that the insertion of a defective disk drive into another's computer did not cause physical damage to

uncomfortable challenge of conceptualizing cyber-losses as physical also confronts insureds seeking coverage for claims under traditional crime and employee dishonesty policies. Although intangible property may be an information-based company's greatest asset, traditional insurance contracts that insure against losses associated with crime or employee dishonesty also may prove inadequate, because these contracts principally insure against the loss of tangible property.[105] For example, in *Peoples Telephone Co. v. Hartford Fire Insurance*,[106] Peoples filed a claim on its Hartford insurance policy when a dishonest employee stole the company's lists "containing combinations of electronic serial numbers and mobile telephone identification numbers" that allowed access to cellular phones.[107] The dishonest employee sold the list to others who were then able to use the numbers for unauthorized phone calls. Peoples incurred $660,000 in losses related to the unauthorized charges and to deactivating the numbers and installing new ones.[108] *Peoples* held an insurance contract that covered property losses caused by employee dishonesty. The contract covered losses of "'[m]oney', 'securities' and 'property other than money and

---

tangible property as required under the policy, explaining that inserting the part did not inflict physical injury on the host computer because it did not "damage[] other parts of the computer." *Id.* at 1153-55.

105. In the liability coverage arena, the tangible quality of data is also an issue and the outcomes are equally variable. LEE R. RUSS, 9 COUCH ON INSURANCE § 126:40 (3d ed. 2000) ("The issue of whether the erasure of computer tapes constitutes damage to tangible property has not been satisfactorily resolved."); Christopher Vaeth, Annotation, *Loss of Information Stored in Computer System or on Computer Disk Cartridge, Computer Tape, or Similar Computer Storage Media as Within Coverage of Liability Policy*, 85 A.L.R. 4TH 1102 (1991); Taylor & Shirley, *supra* note 3, at 195. In *Retail System, Inc. v. CNA Insurance Cos.*, 469 N.W.2d 735 (Minn. Ct. App. 1991), the court considered whether a computer tape and its data constituted tangible property within the meaning of property damage in a liability policy. The court held that the tape and its valuable data constituted tangible property. *Id.* at 738. However, in *St. Paul Fire & Marine Insurance Co. v. National Computer Systems, Inc.*, 490 N.W.2d 626 (Minn. Ct. App. 1992), the court distinguished *Retail Systems* and held that the misappropriation of proprietary and technical information was not damage to tangible property. *Id.* at 630-31. The court explained that while the "information was in a tangible form . . . the information itself was not tangible." *Id.* at 631.

106. 36 F. Supp. 2d 1335 (S.D. Fla. 1997).

107. *Id.* at 1336. The case is not clear regarding how the data theft occurred or in what form the data was stored. The employee "stole from Peoples' lists containing combinations of electronic serial numbers and mobile telephone identification numbers ('ESN/MIN combinations'), which are necessary to activate and use cellular phones." *Id.* The employee sold the lists to third parties who "used the number combinations to program ('clone') other cellular phones." *Id.*

108. *Id.*

securities.'"[109] The contract defined "property other than money and securities" as "any tangible property other than money and securities that has intrinsic value."[110] In rejecting the insured's claim, the court opined that tangible property "may be felt or touched, and is necessarily corporeal. . . ."[111] Relying on earlier cases that excluded coverage for the intrinsic value of information, concepts, ideas, and designs, the court rejected the notion that the lists were tangible property. The court reasoned, "[i]t is the intangible value and/or information contained in them that prompts the insured to make a claim."[112]

These cases demonstrate the vulnerability insureds face if they only purchase traditional insurance and expect coverage for computer-based risks. These claims will likely be litigated because coverage issues are not clear-cut. In the business interruption area, Ingram prevailed only because the court indulged the broadest reading of the insurance contract and novel arguments.[113] And, although crime, and particularly employee crime, is a major source of Internet business loss,[114] current traditional crime and employee dishonesty policies may prove inadequate to insure an e-business' intangible information assets.[115]

III. MEETING THE NEEDS OF INSUREDS

A. A Transition Period

E-commerce poses risks of both a different kind and magnitude than bricks and mortar business.[116]

---

109. *Id.* at 1337.

110. *Id.*

111. *Id.* (quoting BLACK'S LAW DICTIONARY).

112. *Peoples*, 36 F. Supp. 2d at 1340.

113. Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. Civ. 99-185 TUC ACM, 2000 WL 726789 at *3 (D. Ariz. Apr. 18, 2000).

114. CSI Press Release, *supra* note 12 ("the most serious financial losses occurred through theft of proprietary information . . . and financial fraud").

115. *See* INS. SERVS. OFFICE, INC., COMPUTER FRAUD COVERAGE FORM CR 00 07 10 90, at 1 (1989) (excluding coverage for employee acts and requiring the loss of tangible property with intrinsic value).

116. As one underwriter commented on the increased advertising risks:

> Even if one assumes that business advertising, sales, or customer service on the Internet do not generate any new or unique exposures, one must be aware that the worldwide reach of the Internet does present a heightened risk not present in localized business activities. Since web sites are accessible from anywhere in the world, the possible consequences are greatly magnified compared to any advertising or

Still, over the next few years, insureds will undoubtedly argue that traditional policies should be stretched to cover the new risks that e-commerce creates. In the short run, courts may appropriately strain to find coverage, especially in light of the rules of contract interpretation that generally favor insureds.[117] However, this should be a transitory phenomenon, and correctly so. Given the magnitude of the new risks the Internet has created and its value to insureds, both insureds and insurers should begin to seek a greater degree of certainty regarding coverage.[118] As insurers draft more carefully crafted exclusions and create new insurance products to respond to Internet risks, the industry will achieve the desired certainty of risk and coverage.[119]

Drafting clearer exclusions is probably an inevitable consequence of current coverage uncertainties,[120] especially if insurers follow their historical response to new risks. For example, within the past two decades

---

> sales effort through local television, radio, or print media. Even national programming or print media does not have the capability of reaching an international audience.

Nelson, *supra* note 5. *See also* ANDERSON, *supra* note 33, § 18.06, at 18-36-18-37 (noting that an internet-based business has new risks associated with conducting a global business).

117. *See* STEMPEL, *supra* note 45, at § 4.01-4.10. Ambiguities in insurance contracts are generally interpreted in favor of coverage. Construction doctrines favoring insureds include contra proferentem, unconscionability, reasonable expectations, and contracts of adhesion. *Id. See generally* James M. Fischer, *Why Are Insurance Contracts Subject to Special Rules of Interpretation?: Text Versus Context*, 24 ARIZ. ST. L.J. 995 (1992) (examining and critiquing premises of pro-insured rules of construction).

118. Leming, *E-coverage*, *supra* note 68, at 16 (noting that seeking coverage under traditional policies will result in litigation and e-commerce policies will produce more certainty).

119. The demand for the new products currently available is relatively low; businesses are curious but cautious. Bowers, *supra* note 26. *See generally* Jeffrey A. Siderius, *Insurance for Electronic Data Risks: An Idea Whose Time Has Come?*, MEALEY'S TECH. LITIG. & INS., March 1999; Harris, *supra* note 24, at 1719. Third party coverage has been available for a few years but first-party coverage is relatively new. The premiums for cyber policies are relatively high (approximately $20-25,000 for $10 million coverage) presumably due to a lack of underwriting experience. *See* Anne Gonzales, *Hackers, viruses spur interest in Internet Insurance*, DENV. BUS. J., Aug. 18, 2000, at B-22, *available at* 2000 WL 16620800; Bowers, *supra* note 26 (noting the "challenges of underwriting risks in an arena that has no track record and the difficulty of accurately quantifying losses on anticipated claims in largely unexplored cyberspace").

120. *See* Lenckus, *Loss Prevention*, *supra* note 68 (quoting spokeswoman for the Insurance Information Institute: "There is no doubt that insurers will be putting exclusions into their policies very quickly if this is the way courts are going with this issue. . . ."); Spencer, *supra* note 68 (commenting that future policies will not remain vague regarding cyber-risks); Léger, *supra* note 35, at 260.

the insurance industry responded to the proliferation of environmental claims under the traditional CGL policy,[121] and to the rise in employment related claims[122] by crafting increasingly ironclad exclusionary provisions in the CGL policy. This quick response to judicial decisions mandating unanticipated coverage is not surprising. As Professor Fischer notes, "[n]o other enterprise, to the extent of the insurance industry, collects judicial data (court decisions) and uses them to draft standardized language for industry contracts."[123] Insurers naturally attempt to correct any expansion of liability beyond the underwritten risk the insurer assumed for the premium it set.[124]

Predictably, insurers also will close the gap in coverage created by the tighter exclusions they have drafted by developing new insurance

---

121. The pollution exclusion in standard CGL policies exemplifies the insurer's response to new risks. Increasingly expansive responsibilities for hazardous wastes exposed landowners to new liabilities and resulted in more claims on the CGL. Judicial opinions interpreting the term "accident" in the standard CGL began to hold that the CGL covered harm resulting from gradual leakage of hazardous waste. The industry responded by rewriting the policy several times. *See* Anna Amarandos & Diana Strauss, *Environmental Insurance as a Risk Management Tool*, 15 NAT. RESOURCES & ENVTL. 88, 88-89 (Fall 2000); E. Joshua Rosenkranz, Note, *The Pollution Exclusion Clause Through the Looking Glass*, 74 GEO. L.J. 1237, 1237-41; *see also* STEMPEL, *supra* note 45, § 4.05, at 4-29-4-31; M. Elizabeth Medaglia & Peter A. von Mehren, *Beyond Asbestos and Environmental Litigation: Coverage Disputes in the Twenty-First Century*, 33 TORT & INS. L.J. 1023, 1024 (1998); Thomas M. Reiter & John K. Baillie, *Better Late Than Never: Holding Liability Insurers to Their Bargain Regarding Coverage for Unforeseen, Gradual Pollution Under Pennsylvania Law*, 5 DICK. J. ENVTL. L. & POL'Y 1 (1996); Kimberly A. Richter, Boeing Co. v. Aetna Casualty & Surety Co.: *CERCLA Response Costs Covered "As Damages" Under Comprehensive General Liability Insurance Policies*, 14 U. PUGET SOUND L. Rev. 311, 350 (1991).

122. *See* James E. Scheuermann, *Employment Practices Liability Insurance: Navigating the Hazards When Exploring the Market*, 29 FALL BRIEF 64 (1999). When claims were made on CGL policies to cover new kinds of employment related claims, insurers "quickly realizing that they were paying claims that they originally had no intention of covering, began using 'employment related claims exclusions' in their policy forms. Some . . . carriers were quicker to respond than others, but this position is fairly standard in the [general liability] arena today." Jeffrey P. Klenk, *Emerging Coverage Issues in Employment Practices Liability Insurance: The Industry Perspective on Recent Developments*, 21 W. NEW ENG. L. REV. 323, 324 (1999).

123. Fischer, *supra* note 117, at 995-96.

124. *Id.* at 1023. The insurer's efforts to resist paying claims has long drawn negative comments: "For whom they insure . . . it is sweet to them to take the monies; but when disaster comes, it is otherwise, and each man draws his rump back and strives not to pay." PETER L. BERNSTEIN, AGAINST THE GODS, THE REMARKABLE STORY OF RISK 95 (1998) (quoting a Florentine merchant, Francisco di Marco Datini, writing in the fourteenth century).

products,[125] assuming an appropriate product can be developed.[126] As more insurers respond to new business paradigms by offering new insurance products[127] these products will assume a greater role in the risk management of electronic information-based companies.[128]

More clearly drafted exclusions and the availability of new insurance products will likely alter how courts view the traditional policies as well. After all, if an insured does not purchase a readily available policy that

---

125. For example, in response to the gap in coverage created by increasing claims and legal theories of liability against employers and the more tightly worded CGL exclusions for employment related claims, the industry developed Employment Practices Liability Insurance. *See* Scheuermann, *supra* note 122, at 64-65; Klenk, *supra* note 122, at 325; Francis J. Mootz III, *Foreword* to Symposium, *Employment Practices Liability Insurance and the Changing American Workplace*, 21 W. NEW ENG. L. REV. 245 (1999). Moreover, as the underwriting data became more certain and rates could be more carefully calculated, the policies grew more expansively responsive to insured's needs. Klenk, *supra* note 122, at 325, 333-34.

Similarly, the Year 2000 crisis prompted insurers to write explicit exclusions in standard policies and to write endorsements providing coverage. *See* INS. SERVS. OFFICE, INC., EXCLUSION OF CERTAIN COMPUTER-RELATED LOSSES IL 09 35 08 98, at 1 (1997); INS. SERVS. OFFICE, INC., BUSINESS INCOME AND/OR EXTRA EXPENSE COVERAGE FOR YEAR 2000 COMPUTER-RELATED AND OTHER ELECTRONIC PROBLEMS CP 15 57 08 98, at 1-2 (1997).

126. Uncertainty regarding the magnitude of the risks may pose problems for insurers crafting new policies and underwriting the risks. *See* Lenckus, *Loss Prevention*, *supra* note 68. That was the case in the environmental arena, where there has not been singular success in developing a wholly satisfactory insurance product at an affordable premium. *See* Amarandos & Strauss, *supra* note 121, at 88; Robert D. Chesler, *The Failure of the Comprehensive General Liability Policy and the Rise of Niche Insurance*, 192 N.J. Law. 13, 16 (Aug. 1998); Ann Waeger, *Current Insurance Policies for Insuring Against Environmental Risks*, *in* SE 53 ALI-ABA 205, 207-08 (2000). In the 1980s, after excluding pollution coverage in the CGL, insurers offered environmental coverage for a time, but many "were overwhelmed by the number and cost of the claims presented." *Id.* at 208. As a result, "until three or four years ago, there was virtually no environmental insurance coverage available," and any that was available proved expensive and extremely limited. *Id.* at 209. Recently, insurers have begun offering competitively priced environmental pollution policies to meet market demands. *Id.* at 209, 251.

127. These products, especially first party products, are new, emerging in only the past two or three years. It seems unlikely that the coverage will be written into a standard policy, given the special complexities of underwriting the risks. *See* Conley, *supra* note 21, at 24-25; Whitney, *supra* note 28 (discussing and reporting on whether insurers will eventually write e-commerce risks into standard policies).

128. *See* Léger, *supra* note 35, at 260 (commenting that the proliferation of new insurance products may be unnecessary, and that standard traditional all-risk policies may provide adequate coverage).

clearly provides particular coverage, a court may justifiably conclude that the insured did not intend to purchase that type of coverage.[129]

A final effect of the new products worth noting is that their presence may make the Internet a safer business environment. The availability of insurance has, on occasion, improved an industry's safety by requiring businesses to undertake loss prevention activities, as well as by tying premiums to claims histories.[130] This will likely have a similar effect on Internet security as insurers pool knowledge about risks, identify system-

---

129. *See* Andrews & Grass, *supra* note 52. *See, e.g.*, Magnetic Data, Inc. v. St. Paul Fire & Marine Ins. Co., 442 N.W.2d 153, 156 (Minn. 1989) (commenting that in determining parties' intent and in denying coverage for data loss under a CGL policy, "additional coverage was available for such a loss, but [] it was not purchased"); HRG Dev. Corp. v. Graphic Arts Mut. Ins. Co., 527 N.E.2d 1179, 1180 (Mass. App. Ct. 1988) (declining to read all-risk policy to cover a defect in title to equipment and noting that title insurance was instead available to insured).

130. Insurance may exert a beneficial external force on industry-wide safety. First, insurers are in a unique position to identify risks through the pooling of information. Insurers can also mandate that insureds conduct loss prevention audits or take other steps to detect risks. Insurers can require insureds to take affirmative steps to avoid losses as a condition of insurance, or they can encourage loss prevention by tying it to the premium charged. *See* Jeffrey Kehne, Note, *Encouraging Safety Through Insurance-Based Incentives: Financial Responsibility for Hazardous Waste*, 96 YALE L.J. 403, 405-06 (1986) (citing C. HEIMER, REACTIVE RISK AND RATIONAL ACTION: MANAGING MORAL HAZARD IN INSURANCE CONTRACTS 42-44 (1985)); James T. O'Reilly, *Risks of Assumptions: Impacts of Regulatory Labels Warning Upon Industrial Products Liability*, 37 CATH. U. L. REV. 85, 88 (1987) (noting that the "insurer's desire to avoid product liability exposure has added an important external factor to labeling decisions by chemical manufacturers"); Robert A. Prentice & Mark E. Roszkowski, *"Tort Reform," and the Liability "Revolution": Defending Strict Liability in Tort for Defective Products*, 27 GONZ. L. REV. 251, 275 n.133 (1991-92) (discussing W. Kip Vicusi, *Toward a Diminished Role for Tort Liability: Social Insurance, Government Regulation and Contemporary Risks to Health and Safety*, 6 YALE J. ON REG. 65, 82 (1989)). Fire prevention, aviation, boiler and elevator safety are notable areas in which insurance generated safety improvements have improved overall safety. *See* Kehne, *supra*, at n.12-14 (citations omitted).

Employment claim insurers have taken proactive steps to reduce losses. *See* Scheuermann, *supra* note 122, at 66; Jack S. McCalmon, *Effective Loss Control Techniques for Employment Practices Liabilities: An Assessment of How EPLI Carriers Should Seek to Transform the American Workplace*, 21 W. NEW ENG. L. REV. 447 (1999); Mootz, *supra* note 125, at 247 (noting "the development of sophisticated loss control and risk management techniques" offered by insurers to insureds). Insurers offering pollution coverage also require audits prior to issuing coverage. *See* Waeger, *supra* note 126, at 237.

Insurers can also exert influence on the government to force industries to change. Insurers, for example, "were the leading protagonists throughout the history of the air bag struggle," lobbying the federal government extensively for mandatory air bags in automobiles. Robert Kneuper & Bruce Yandle, *Auto Insurers and the Air Bag*, 61 J. RISK & INS. 107 (1994), *available at* 1994 WL 13386236, at *2.

wide vulnerabilities, demand that insureds undergo pre-qualification audits, and adopt proactive loss prevention strategies.[131]

B. New Products

While there are a number of first and third party e-business insurance contracts on the market today, this Article will examine, for exemplary purposes, the first party portion of Marsh & McLennan's new Net Secure insurance policy.[132] A close examination demonstrates how a policy designed to cover computer risks is fundamentally different from a traditional policy.[133] Whether it will provide a necessary adjunct to

131. Some insurers are requiring extensive system security assessment at the present time, prior to insuring. *See* Ceniceros, *supra* note 35, at 29; Conley, *supra* note 21, at 26 (noting that audits can cost "anywhere from a few thousand dollars to hundreds of thousands"); Hann, *supra* note 3, at 75 (describing security measures and assessment demanded by insurers); Jill Vardy, *Calgary's Jaws to Help Firm Offer Virus Insurance: Anti-Hacker Policies: Announcements Made on Day Love Bug Hit*, NAT'L POST, May 5, 2000, at C-3, *available at* 2000 WL 20309177 (describing security consulting and risk assessment required of by Marsh, Net Secure policyholders); Langin, *supra* note 13, at *5 (advising underwriters, in underwriting new e-business policies, to examine company's anti-virus software, backup tape procedures, and procedures to respond to malicious code attacks); Randy Paar & Jerold Oshinsky, *United States: Insurance Coverage for Losses Arising Out of Use of the Internet*, MONDAQ BUS. BRIEFING, Aug. 2, 2000, *available at* 2000 WL 9238722, at *12 (commenting that some insurers require the purchase of risk management services including "surveillance and intrusion detection software," "changes in passwords," and "computer backups").

132. NET SECURE, PROTECTING YOUR INFORMATION ASSETS AND E-BUSINESS ACTIVITIES 1 (1999) (on file with author).

133. There are other new products on the market. *See* ANDERSON, *supra* note 33, § 18.05, at 18-33-18-37 (describing listing insurers writing specialized insurance policies for electronic commerce and other computer dependent high-tech ventures); Bowers, *supra* note 26, 2001 WL 12285238, at *9-10 (listing major insurance products); Hann, *supra* note 3, at 71-72 (identifying new electronic business policies); Amanda Levin, *Hacker Attacks Spur Web Liability Products*, NAT'L UNDERWRITER PROP. & CASUALTY-RISK & BENEFITS MGMT EDITION, Mar. 15, 2000, at 3, *available at* 2000 WL 10393110 (describing growth of products).

Apparently, drawing lessons from the initial unpopular employment practices policies that were narrow and riddled with "exclusions, high deductibles, high prices, and no loss-control services" these products are broader. *See* Hann, *supra* note 3, at 74 (discussing the Network Risk Management Services policy).

However, the policies (including both first- and third-party coverage) are expensive, especially considering that they are not intended to stand in lieu of traditional policies. Conley, *supra* note 21, at 26 (reporting that "new e-commerce policies offer up to $25 million in coverage at a price somewhere between 2 percent and 3.5 percent of the limits purchased"); Hann, *supra* note 3, at 75 (reporting that Cigna estimates that the policy runs "between $20,000 and $25,000 for a policy with limits of $12 million"); Levin, *supra* note

traditional coverage[134] that insureds desire is not yet known. As with any new insurance product, uncertainty will abound until each provision is litigated and tested.[135] However, at its core, this insurance contract and those like it recognize that intangibles stored on a computer constitute insurable property, that the inability to communicate via a computer is a business interruption even if business is not suspended, and that systems that are networked or dependent on service providers may suffer an interruption even when no physical event occurs at their place of business or on their equipment.

These policies insure against the unique perils associated with a company dependent on e-business, which bear little resemblance to traditional perils. For example, the Net Secure Policy identifies the following as covered computer-based perils:

1. Any inadvertent mistake, error, or omission in the creation, distribution, installation, maintenance, modification, processing, repair, testing, or use of your Computer System;

2. The implantation, introduction, or spread of a Computer Virus;[136]

3. An attack;[137]

133, at 3 (reporting "premiums of about $25,000 to $125,000 for at least $25 million in coverage").

134. Obviously, e-businesses continue to require traditional policies. Like other businesses, they still have tangible property that must be insured, and perils of the physical world can still interrupt their business operations.

135. Notably, these policies have not yet been tested by claims or litigation. ANDERSON, *supra* note 33, § 18.05, at 18-33 (cautioning that these new policies lack a proven "track record," and a company should "carefully evaluate its needs and the proposed policy form, giving particular attention to exclusions and proposed endorsements"); Paar & Oshinsky, *supra* note 131, at *12 (commenting, "[t]here is little loss experience or construction of the new policy wording and, therefore, there is less certainty regarding the scope of coverage afforded by the policies"); *see also* Léger, *supra* note 35, at 260 (noting that no claim has yet been paid perhaps in part because the policies are only a year old).

136. The policy defines a computer virus: "Computer Virus means a corrupting, harmful, or otherwise unauthorized piece of code that infiltrates your Computer System, including a set of unauthorized instructions, programmatic or otherwise, that propagates itself through your Computer System. Computer Virus includes 'Trojan horses', 'worms', and 'time or logic bombs.'" NET SECURE, *supra* note 132, at 2.

137. The policy defines an attack:

> Attack means a hostile action or actions, or a threat of hostile action or actions, that has the intent to affect, alter, copy, corrupt, destroy, disrupt, damage, or provide unauthorized access/unauthorized use of your Computer System including exposing or publicizing your confidential Electronic Data or causing your Electronic Data to be

4. Denial of Service;[138]
5. Unauthorized Access;[139] or
6. Unauthorized Use.[140]

Notably, inadvertent mistakes or errors are included among these named perils, presumably to provide coverage for at least some losses caused by operational mistakes and programming errors,[141] but not the costs to detect and repair the errors themselves.[142] Exclusions from coverage are not unlike those contained in standard first party insurance policies. They include, among other things, wear and tear; electrical failures including power interruptions, surges, failure of telephone or data transmission lines not within the control of the insured; satellite failure; and the insured's use of unproven or expired, canceled or withdrawn software programs.[143]

The nature of the loss that triggers coverage is also specifically tailored to the computer; the policy dispenses entirely with the requirement of physical loss or damage. Coverage is triggered by "direct loss resulting from damage to, or from the affecting, altering, copying, corrupting, distorting, disrupting, or destroying" of electronic data,[144] electronic information assets,[145] electronic computer programs, or electronic data processing media.

> inaccessible. An Attack shall not include unintentional programming errors.

Id. at 1.

138. The policy defines denial of service: "Denial of Service means an Attack on your Computer system that results in the degradation of or loss of access to your Internet and Network Activities or normal use of your Computer System." *Id.* at 2.

139. The policy defines unauthorized access: "Unauthorized Access means the gaining of access to your Computer System by an unauthorized person or persons or an authorized person in an unauthorized manner." *Id.* at 5.

140. The policy defines unauthorized use: "Unauthorized Use means use of your Computer System Resources by an unauthorized person or persons or an authorized person in an unauthorized manner." *Id.*

141. ISO's all-risk policy, on the other hand generally does not cover losses caused by "design, specifications, workmanship, repair." ISO, SPECIAL FORM, *supra* note 42, at 3.

142. *See* NET SECURE, *supra* note 132, at 25.

143. *Id.* at 24-25.

144. "Electronic Data means material converted to a form usable in a Computer System and which is stored on Electronic Data Processing Media for use by Electronic Computer Programs, including Electronic Information Assets." *Id.* at 2.

145. Electronic Information Assets is defined:

> Electronic Information Assets means proprietary material developed or stored as Electronic Data including but not limited to such Electronic Data which [includes] charge, debit, and credit card information;

The business income and extra expense coverage under the Net Secure Policy is also notably different than its traditional counterpart. The policy provides that the insurer will pay for actual loss of business income and extra expense that the insured sustains due to the disruption, interruption, delay, or suspension of the insured's Internet and network activities.[146] Importantly, unlike a traditional policy, the insured need not establish direct physical loss of or damage to property, or that its business was necessarily suspended.[147] Moreover, the business interruption perils include those more closely associated with Internet business, including mistakes, attacks, denial of service, unauthorized access or use, computer crime,[148] extortion,[149] and loss of service.[150]

Another provision uniquely appropriate to e-business is a provision that extends coverage to losses caused by a covered peril that occurs to a "dependent business" rather than to an insured as a matter of course.[151] A

> banking, financial, and investment services account information including Evidences of Debt; proprietary business information and your Trade Secrets; and any other valuable, private, or confidential information important to the business functions of an Insured.

Id. at 3.

146. *Id.* at 23.

147. These provisions might have solved several formidable obstacles in *Home Indemnity Co. v. Hyplains Beef, L.C.*, 893 F. Supp. 987 (D. Kan. 1995). There, the insured, a meat packer, suffered delays, business slowdowns and other losses, when, because of faults in a software program, it could not retrieve data necessary to its operations. *Id.* at 989. Hyplains' claims under the business interruption policy were denied. *Id.* The court concluded that the delays and necessary extra and slower manual work the losses caused did not amount to a suspension of business. *Id.* at 991. The court also questioned whether the irretrievability of electronic data constituted direct physical loss to tangible property. *Id.* at 990.

148. Defined as: "Computer Crime means dishonest, fraudulent, malicious, or criminal use of your Computer System by a perpetrator . . . to affect, alter, copy, corrupt, delete, disrupt, or destroy your Computer System and obtain financial benefit for any party. Computer Crime also includes Information Theft." NET SECURE, *supra* note 132, at 2.

149. Defined as: "Extortion means any threat or connected series of threats to commit a Computer Crime, to introduce, implant or spread a Computer Virus, or to adversely affect your reputation or public standing which you believe will involve a demand for Extortion Monies." *Id.* at 3. *See* Ceniceros, *supra* note 35, at 1 (describing recent extortion attempt and coverage issues).

150. Defined as: "Loss of Service means the inability of a third party, who is authorized to do so, to gain access to your Computer System and conduct normal Internet and Network Activities." NET SECURE, *supra* note 132, at 4.

151. This represents a variation on the contingent business interruption coverage sometimes purchased as a coverage extension for companies who rely on "third parties and supply chains." Gavin Souter, *Risks From Supply Chain Also Demand Attention,* BUS.

dependent business is one that the insured does "not own or operate," but depends on to provide necessary Internet and network activities, to purchase good or services through the Internet or network, to "facilitate or host" the insured's website, or to provide computer services.[152] Essentially, this provision recognizes the interconnectedness and dependencies of e-businesses, and that business interruption may occur, not merely by problems within one's own computing system, but also as a result of events that disrupt those businesses on which the insured depends, such as Internet providers.

The Crime Coverage Part of the Net Secure Policy also marks a departure from traditional insurance contracts. The crime provisions afford coverage for losses and costs arising out of Internet and network activities. The policy will pay for direct financial loss of the insured's money, securities or "any physical assets, electronic data, electronic computer programs, electronic data processing media or electronic information assets."[153] Moreover, the insurance also pays for "actual incurred financial costs or uncollectable financial costs arising out of the theft of the insured's

---

RISK, May 15, 2000, at 26, *available at* 2000 WL 8171150; Paula V. Tarr, *Where Have All the Customers Gone? Business Interruption Coverage for Off-Premises Events*, 30 TRIAL 20, 28-29 (Winter 2001). Typically, these provisions insure for covered causes of losses that occur to described dependent properties. Tarr, *supra*, at 28. Dependent properties are those other businesses on which the insured necessarily depends such as "those who supply materials for the insured, purchase the insured's goods, or attract customers to the insured's business." *Id.* at 29. It provides coverage for actual losses sustained due to necessary suspensions caused by direct physical loss of or damage to dependent property at premises described in the schedule. *Id.* at 24. However, like business interruption coverage generally under a traditional policy, this coverage extension still requires direct physical loss or damage and suspension of the insured's business operations. *Id. See also* Archer Daniels Midland Co. v. Hartford Fire Ins. Co., 243 F.3d 369, 371 (7th Cir. 2001) ("contingent business-interruption coverage goes further [than regular business-interruption insurance], protecting the insured against the consequences of suppliers' problems").

152. NET SECURE, *supra* note 132, at 21.

153. *Id.* at 28. Electronic Information Assets are:

> proprietary material developed or stored as Electronic Data including but not limited to such Electronic Data which is:
>
> - charge, debit, and credit card information;
> - banking, financial, and investment services account information including Evidences of Debt;
> - proprietary business information and your Trade Secrets; and any other valuable, private, or confidential information important to the business functions of an Insured.

Id. at 3. *See also supra* text accompanying note 144.

computer systems resources."[154] Like the property and business interruption counterparts, the crime provisions alter the traditional insurance contracts, by shedding the tangible property limitation and by covering the acts of employees, to the extent company officials were without knowledge of the dishonest acts.[155]

CONCLUSION

The cyberworld is a dangerous place and the risk of financial harm is real; businesses should expect that errors, viruses, online theft, and various other attacks will eventually strike and cause serious damage. This significant risk of fortuitous loss makes insurance an appropriate risk management tool. For now, when insureds suffer losses from these events they will look for coverage under their existing insurance policies. Even without a specialty policy, in the short run, businesses may find success as courts strain to find coverage under traditional insurance contracts for the novel losses suffered by e-businesses. However, insurers will respond to cases like *Ingram Micro* by writing clearer exclusions[156] and by offering computer-dependent businesses certainty of coverage by creating insurance products specifically designed for their unique needs. The market for these products will increase as insureds begin to appreciate the value their Internet technology affords to their business, and the magnitude of the risks they face in cyberspace.

---

154. NET SECURE, *supra* note 132, at 28.

155. *Id.* at 29. *Peoples Telephone Co. v. Hartford Fire Insurance*, 36 F. Supp. 2d 1335 (S.D. Fla. 1997), would only qualify if the lists were accessed through a computer system; problematically, the policy narrowly focused only on computer systems.

156. Léger, *supra* note 35, at 260 (quoting Robert Hartwig, Insurance Information Institute's chief economist commenting on *Ingram Micro*: "[I]f the judge's ruling is upheld, . . . you could expect that property insurance contracts would be rewritten so that this interpretation would never happen again.").