SPECIAL EDITION

Reactions

@Risk

version 2.0

The definitive guide to legal issues of insurance and reinsurance of internet, e-commerce and cyber perils

Special Contributing Author

Ty R. Sagalow

of AIG eBusiness Risk Solutions

Edited by

Robert W. Hammesfahr

of Cozen O'Connor

Copublished with:

AIG*e*Business RISK SOLUTIONS℠

A **Reactions** publication

Reactions

@Risk
version 2.0

The dot.com craze has cooled, but the use of the websites for business and the importance of network security have skyrocketed. These trends have made cyber risk one of the greatest corporate exposures to loss. This book provides an excellent education as to the risks of eBusiness, as well as how to mitigate them using risk management and insurance. In fact, the chapter on cyber insurance written by Ty Sagalow, COO at the largest cyber insurer, is the most comprehensive work of its kind, and should be required reading for all risk management professionals.
Phil Norton, Ph.D.,
President, Professional Liability Division, Arthur J. Gallagher & Co.

"A must read for any professional or executive faced with managing e-commerce risks."
Kinsey Carpenter of Carpenter Moore, a leading broker of high tech insurance

"A whole new genre of sophisticated exposures, never before contemplated under traditional bricks and mortar insurances and reinsurances are quickly emerging. The successful understanding and management of these exposures then becomes critical to the broker, risk manager, and insurance and reinsurance underwriter alike. @ Risk is required reading for professionals wishing to become fluent in the new world of cyber exposures."
Harrison D. Oellrich,
Managing Director, Guy Carpenter & Co., Inc.

The burst of the technology bubble hasn't meant the end of the internet. The internet has become part of our daily personal and business lives. All businesses are eBusiness nowadays. This means that every company must address cyber risk management issues as part of their natural due diligence. Specific cyber insurance plays a critical role in this process. @Risk provides good, practical advise on the cyber-insurance issues. Must reading for anyone interested in cyber risk management.
Jill D. Tellez,
ARM,Director, Technology Risk Group, Aon Financial Services, Inc.

"In many respects the insurance industry is starting to set the standards for managing today's technology risks. Increasingly digital risk insurance is being seen as a type of due diligence — for in order for the company to have coverage, they must have already subscribed to certain levels of risk mitigation and be demonstrating best practice. This brings peace of mind to customers, investors, and shareholders alike, but also enables the business to fully leverage their IT investment, secure in the knowledge they are protecting their assets and their reputation."
David Umbers,
Product Development Manager, Safeonline Limited

Since 9/11, every business has had to re-focus on the risks they face. Internet risks, including cyber-terrorism and the related legal and insurance issues, should be a huge priority to corporate executives. A cyber-insurance policy complemented with a D&O insurance policy are must haves. Robert Hammesfahr and Ty Sagalow as experts in the field of cyber-insurance law and insurance provide a very good road map to begin the evaluation of those issues.
Henry L. Whiting, Managing Director,
FINPRO Business Development and I-Risk Practice Leader, Marsh, Inc.

A **Reactions** publication

@Risk
version 2.0

The definitive guide to legal issues of insurance and reinsurance of internet, e-commerce and cyber perils

Special Contributing Author
Ty R. Sagalow
of AIG eBusiness Risk Solutions

Editor and Author
Robert W. Hammesfahr
of Cozen O'Connor

@Risk

version 2.0

The definitive guide to legal issues of insurance and reinsurance of internet, e-commerce and cyber perils

Published by
Reactions Publishing Group Ltd
Euromoney Institutional Investor PLC
Nestor House
Playhouse Yard
London EC4V 5EX, UK
Enquiries: +44 (0)20 7779 8861
Fax: +44 (0)20 77798200
Website: www.reactionsnet.com

Publisher
John Walsh
Tel: +44 (0)20 7779 8184
Email: jwalsh@euromoneyplc.com

Manager, books and reports
Frances Bates
Tel: +44 (0)20 7779 8861
Email: fbates@euromoneyplc.com

Design & production
Kristina Neville
Email: kristina.neville@virgin.net

Director
Edoardo Bounous

Directors
Padraic Fallon (chairman and editor-in-chief); Sir Patrick Sergeant; Richard Ensor (managing director); CJ Sinclair; Neil Osborn; Dan Cohen; Christopher Brown; Gerard Strahan; JP Williams; John Botts; Edoardo Bounous; Colin Jones; The Viscount Rothermere; Simon Brady; Tom Lamont; John Bolsover; Gary Mueller; Diane Alfano

Customer services:
Tel: +44 (0)20 7779 8610

ISBN 1 85564 984 5

Repro and printing by The Manson Group Limited, UK.

About

AIG eBusiness RISK SOLUTIONS SM

AIG eBusiness Risk Solutions (AIGeBRS) is a global leader in identifying, evaluating and managing Internet-related risks. AIGeBRS offers a comprehensive suite of insurance products[1] and risk management services that support eBusiness at its most sensitive touch points: network security, trade credit, identity, and credit card fraud.

AIG eBusiness Risk Solutions is staffed with an experienced and innovative group of insurance and technology specialists who are developing services and insurance products to address the unique issues faced by the most established as well as the newly emerging company created by the emergence of the internet as part of a company's business strategy whether for marketing, communication or eCommerce purposes and the proliferation of technology in the business process.

AIG eBusiness Risk Solutions is a division of AIG's American International Companies. AIG is the leading U.S.-based international insurance and financial services organization and the largest underwriter of commercial and industrial insurance in the United States. Its member companies write a wide range of commercial, personal and life insurance products through a variety of distribution channels in approximately 130 countries and jurisdictions throughout the world. AIG Companies hold the highest rating from the industry's principal rating industries, S&P, Moody's and Best's.

For my information about AIG eBusiness Risk Solutions please visit us at www.aigebrs.com or contact us at:

AIG eBusiness Risk Solutions
80 Pine Street, 8th Floor
New York, NY 10005
Attn:@Risk

Phone: 1-866-826-4974

1 Insurance underwritten by member companies of American International Group, Inc. The description herein is a summary only. It does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for complete details of coverage and exclusions. Coverage may not be available in all states. Issuance of coverage is subject to underwriting. Non insurance products may be provided through independent third parties.

Robert W. Hammesfahr
Ty R. Sagalow

Ty R. Sagalow is Executive Vice-President and Chief Operating Officer of AIG eBusiness Risk Solutions. He joined the American International Group in 1983 and has held several executive and legal positions with the group. As COO of AIG eBusiness Risk Solutions, he is responsible for the insurance products and services offered to mitigate the risks of the New Economy on a worldwide basis. Mr. Sagalow is a worldwide authority on cyber-exposure and insurance and has spoken in many forums including the White House. He has appeared on television with Alexander Haig and given testimony before the United States Senate. He is an author of several works on the subject. Mr. Sagalow is also considered an expert on D&O liability and insurance, and has authored, among other works, "Directors & Officers Insurance Handbook" for the National Association of Corporate Directors (www.nacdonline.org). Mr. Sagalow graduated summa cum laude from Long Island University and cum laude from Georgetown University Law Center. He also holds a Master of Laws degree from New York University.

Robert W. Hammesfahr is a member of Cozen O'Connor, and is one of the leading insurance and reinsurance lawyers in the United States. He was born in Pittsfield, Massachusetts and attended Colgate University, where he received his Bachelor of Arts degree with high distinction, and was elected to Phi Beta Kappa, in 1975. He received his Juris Doctor degree from Northwestern University School of Law in 1978. He is admitted to practice in Illinois and New York, and before the Supreme Court of the United States, the United States Courts of Appeal for the District of Columbia Circuit and the Seventh Circuit, and the United States District Court for the Northern District of Illinois, where he is a member of the Trial Bar. He is the co-author of Punitive Damages: A State-by-State Guide to Law and Practice — 2002 Edition (West Publishing Company 2002 and its predecessors published in 1991, its 1996, 1999, 2000 and 2001 supplement and the original 1988 version), which has also been published in a Japanese language edition, (Hoken-Mainichi Shinbun-sha, Tokyo 1995). He is also the co-author of The Law of Reinsurance Claims, published in the United States by Andrews Professional Books and in Europe by Reactions Publishing Group Ltd., 1994 and its supplement in 1997. He has been the author or co-author of numerous articles in professional and business publications.

Richard L. Blatt

Richard L. Blatt was born in Oak Park, Illinois and attended the University of Illinois, where he received his Bachelor of Arts degree with honors, and was elected to Phi Beta Kappa, in 1962. He received his Juris Doctor degree from the University of Michigan Law School in 1965. He is admitted to practice in Illinois and New York, and before the Supreme Court of the United States, the United States Courts of Appeal for the Third, Fourth and Seventh Circuits, and the United States District Courts for the Northern and Southern Districts of Illinois. He is a member of the Trial Bar of the United States District Court for the Northern District of Illinois. He is the co-author of Punitive Damages: A State-by-State Guide to Law and Practice — 2002 Edition (West Publishing Company 2002 and its predecessors published in 1991, its 1996, 1999, 2000 and 2001 supplement and the original 1988 version), which has also been published in a Japanese language edition, (Hoken-Mainichi Shinbun-sha, Tokyo 1995). He is also the author or co-author of numerous articles in professional and business publications. His practice focus is litigation, litigation management and alternative dispute resolution. Over his distinguished 30 years of practice, he has represented businesses and insurers in a wide variety of major mass tort coverage and other litigation.

Zacarias R. Chacon

Zacarias R. Chacon was born in Hutchinson, Kansas and attended the University of Texas at Austin, where he received his Bachelor of Arts degree with honors in 1978. He received his Juris Doctor degree from the University of Texas School of Law in 1981. Mr. Chacon is admitted to practice in Illinois, and before the United States District Court for the Northern District of Illinois. He is a member of the Illinois Bar, the Northern District of Illinois General and Trial Bar and the bar of the U.S. Court of Appeals for the Seventh Circuit. Mr. Chacon has also been frequently admitted pro hac vice in other states including Kentucky, Indiana, Florida, Michigan, Wisconsin and Minnesota. His areas of practice include first property coverage, arson and fraud investigations and commercial property liability defense. Mr. Chacon is conversant in Spanish.

Gregory D. Hopp

Gregory D. Hopp was born in Winchester, Massachusetts and attended the University of Illinois, where he graduated with distinction and honors in Political Science in 1981. He has been litigating major cases throughout the United States involving coverage, fraud and reinsurance issues and is well known as a leading trial lawyer. He received his Juris Doctor degree from the University of Michigan Law School in 1984. He is admitted to practice in Illinois, and before the United States Supreme Court, the United States Court of Appeals for the Third Circuit and the United States District Courts for the Northern District of Illinois and the Eastern District of Michigan.

Andrew B. Katz

Andrew B. Katz is a registered patent attorney who represents clients of all sizes in a wide-range of business and intellectual property matters. He is a co-chair of Cozen O'Connor's intellectual property department. He was born in Philadelphia, Pennsylvania. He attended Lafayette College, where he graduated in 1986. He received his Juris Doctor degree from George Washington University Law School in 1989. He is admitted to practice in Pennsylvania and the District of Columbia. He has authored several articles pertaining to intellectual property protection on such topics as the effect of new top-level domains on trademark law ("Stay Grounded in Web Land Grab," Information Week, February 12, 2001), the impact of software patents on small businesses ("State Street May Place Start-ups In Peril," Tech Trends, New York Law Journal, Vol. 2. No. 9, January 19, 1999), and commercializing new technologies developed with government funding ("Looking For A Partner? You May Want Uncle Sam," Washington Business Journal Vol. 17 No. 11, July 24-30, 1998).

Kevin M. Mattessich

Kevin M. Mattessich was born in Bryn Mawr, Pennsylvania. He attended Boston College in Chestnut Hill, Massachusetts, where he graduated cum laude in 1982. He received his Juris Doctor degree from the Catholic University of America — Columbus School of Law in 1985. Kevin is a member of the Torts and Insurance Practice Section of the American Bar Association and the Professional Liability Underwriters Society. He has served as a member of the Fraud Section of the Criminal Division in the United States Department of Justice in Washington, D.C. from 1992-1994. Kevin has also frequently lectured on various insurance law and white-collar fraud issues. In 1994, he was called to testify before the United States Senate Judiciary Committee concerning health care/insurance fraud issues.

Lori S. Nugent

Lori S. Nugent was born in Peoria, Illinois. She attended Knox College in Galesburg, Illinois, where she graduated with distinction and honors in Political Science in 1984. She received her Juris Doctor degree from Northwestern University School of Law in 1987. She is admitted to practice in Illinois, and before the United States Court of Appeals for the Seventh Circuit and the United States District Court for the Northern District of Illinois. She is the co-author of Punitive Damages: A State-by-State Guide to Law and Practice — 2002 Edition (West Publishing Company 2002 and its predecessors published in 1991, its 1996, 1999, 2000 and 2001 supplement and the original 1988 version), which has also been published in a Japanese language edition, (Hoken-Mainichi Shinbun-sha, Tokyo 1995). Her practice focuses on insurance, reinsurance and punitive damages matters. She has a particular interest in Internet, e-commerce and information technology matters and has developed computer software errors & omission policies, offensive and defensive patent infringement policies and other specialty products.

Jeffrey I. Pasek

Jeffrey I. Pasek was born in Pittsburgh, Pennsylvania and attended the University of Pittsburgh, where he graduated magna cum laude in 1973. He received his Juris Doctor degree from the University of Pennsylvania in 1976. Jeff is admitted to practice in Pennsylvania, New Jersey and New York, and has tried cases and argued appeals in the federal courts throughout the United States, including before the United States Supreme Court. Jeff chairs the Labor and Employment Law Department at Cozen O'Connor. He is the author of numerous articles and is called upon regularly as a speaker in continuing legal education programs regarding labor and employment law and legal ethics.

Marc A. Polansky

Marc A. Polansky was born in Altoona, Pennsylvania and attended the University of Maryland where he earned his Bachelor of Arts degree in Economics and Political Science in 1989. He earned his Juris Doctor degree from Chicago-Kent College of Law in 1994. Mr. Polansky is admitted to practice in Illinois, and before the United States District Court for the Northern District of Illinois. He is a member of the Chicago Bar Association and the Illinois Bar Association. His areas of practice include first party coverage, arson and fraud investigations, fraudulent personal injury defense and commercial property liability defense.

Leah D. Setzen

Leah D. Setzen was born in Hinsdale, Illinois and attended the University of Illinois at Champaign-Urbana where she earned her Bachelor of Arts degree magna cum laude and with departmental distinction in Speech Communications, and was elected to Phi Beta Kappa, in 1997. She earned her Juris Doctor degree cum laude from the University of Illinois College of Law in 2000. Ms. Setzen is admitted to practice in Illinois, and before the United States District Court for the Northern District of Illinois. She is a member of the Chicago Bar Association, the Illinois State Bar Association, and the DuPage County Bar Association. Her areas of practice include insurance, reinsurance, technology and punitive damages matters.

Technological improvements alone cannot safeguard a company's digital risks. Whether managing the risk of a computer virus, electronic theft of confidential information or the loss of business interruption due to a computer attack, a Total Risk Management Approach is required which combines best in class technology, risk information and insurance. Fortunately, the insurance industry has begun to address cyber-risk management needs through the development of detailed expertise and the creation of specialized products and services to manage those risks.

Ty R. Sagalow
Chief Operating Officer
AIG eBusiness Risk Solutions

Introduction
Managing the Risks of eBusiness

When the Internet was introduced as a new channel for commerce and communications its promise was enticing: a borderless global economy enabling companies to instantly bridge their internal networks with business partners and customers around the world with the click of a mouse. Yet in that instant of connectivity were created amorphous and various layers of risk.

The reality is, security technologies and corporate policies have not kept pace with developments in communication and information technologies. New security vulnerabilities are discovered even as systems are being deployed. Solutions are fashioned just to have more creative hacking methods created. In the end, it is much like a driver changing a tire on a moving vehicle. Competitive pressures necessitate that companies forge ahead with their e-business initiatives: there are risks associated with not venturing into a potentially rewarding but uncharted terrain. Yet no company wants the thankless task of trying to restore public confidence once a hacker attack has brought an enterprise network to its knees.

Ironically, the very characteristics that compel companies to embrace the Internet – its ability to connect to anyone, anywhere, at any time – are the same ones that create new potential liabilities and other financial losses when problems occur. For example, how does a company leverage its vast new data stores while protecting consumer privacy? How does a company take advantage of

improvements in technological communications without making itself vulnerable to the newest Internet Melissa Virus or "Love Bug"? Even the content of a company's web site can be a source of legal and financial danger. Add to that the fact that foreign countries have their own jurisdictions and legal remedies, and the complexity of managing global e-business risk grows exponentially.

Nevertheless, the rewards of the Internet are too enticing to sidestep. Today, it is only the foolish company who foregoes having some type of web presence or refusing to use email as a method of communication. A vast percentage of companies use the Internet to conduct some type of eCommerce and this percentage grows everyday. Emerging technologies like mobile commerce, digital signatures, and peer-to-peer networking are expected to further streamline inter-corporate communications. B2B marketplaces continue to emerge with their promise to provide a new foundation for business procurement efficiencies. Yet many such enabling technologies are only in the early stages of enterprise-wide adoption. So a gap remains in the e-business risk management strategies of even the most progressive enterprises, and that gap can negatively impact a company's bottom line.

Fortunately, security solutions and information continue to improve as enterprises have increasingly adopted tighter e-business security policies and procedures. However, technological improvements alone cannot safeguard a company's digital risks. Whether managing the risk of a computer virus, electronic theft of confidential information or the loss of business interruption due to a computer attack, a Total Risk Management Approach is required combining Technology, Risk Information and Insurance. Fortunately, the insurance industry has begun to address cyber-risk management needs through the development of detailed expertise and the creation of specialized products and services to manage those risks. Today, AIG eBusiness Risk Solutions is leading the way in this effort. This informative book is designed to educate on the risks of an Internet world and through an understanding of both traditional and specialized insurance enable the reader to better manage those risks.

Introduction to E-Commerce

"Insurance is key to a secure cyberspace and to continued deployment of information technology. The internet must not only be built, operated and defended but insured."

Introduction to E-Commerce

Table of Sections

1.1 Introduction

1.2 United States Department of Commerce Reports
- 1.2.1 Introduction to Reports
- 1.2.2 The Emerging Digital Economy II Report
- 1.2.3 The Report
- 1.2.4 The Electronic Revolution

1.3 What Exactly is the Internet?

1.4 What is E-Commerce?

1.5 Problems Facing the Legal Community

1.6 E-Risks: New Insurance Needs

1.1 Introduction

"Information technology pervades all aspects of our daily lives, of our national lives. Its presence is felt almost every moment of every day, by every American. It pervades everything from a shipment of goods, to communications, to emergency services, and the delivery of water and electricity to our homes. All of these aspects of our life depend on a complex network of critical infrastructure information systems. Protecting this infrastructure is critically important.

Disrupt it, destroy it or shut down these information networks, and you shut down America as we know it and as we live it and as we experience it every day. We need to prevent disruptions; and when they occur, we need to make sure they are infrequent, short and manageable. This is an enormously difficult challenge. It is a technical challenge, because we must always remain one step ahead of the hackers.

It is a legal challenge, because this effort raises cutting-edge questions of both privacy and civil liberties. It is a political challenge, because the government must act in partnership with the private sector, since most of the assets that are involved in this effort are owned by the private sector, which owns and operates the vast majority of America's critical infrastructure"[1]

— Tom Ridge
— Director of Homeland Security

"…I'm so delighted that the President has asked me to worry about the war next time, the future security of the United States through cyberspace. Our economy, our national defense, increasingly our very way of life, depends upon the operation, secure and safe operation of critical infrastructures, that in turn depend on cyberspace.

America has built cyberspace, and America must now defend cyberspace. But it can only do that in partnership with industry."

— Richard Clarke
— Special Advisor to the President for Cyber Security

1 New Counter-Terrorism and CyberSpace Security Positions, Announcement of the Office of the Press Secretary for President George W. Bush (Oct. 9, 2001).

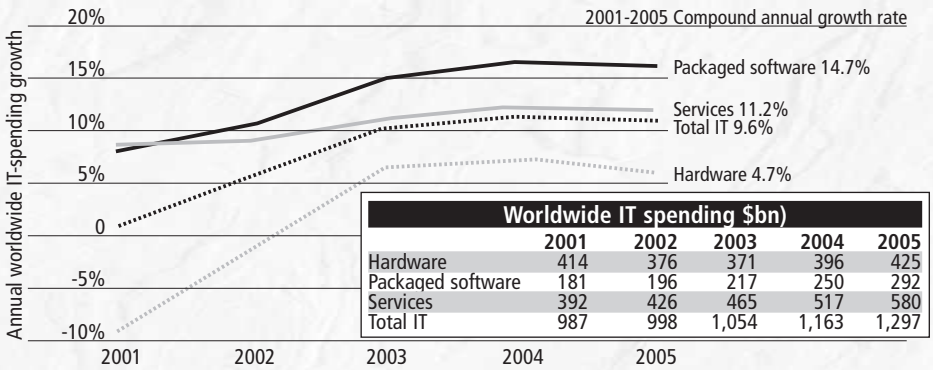
Insurance is key to a secure cyberspace and to continued deployment of information technology. American businesses and consumers must not only use cyberspace and defend it, they must insure it. As Jack Welch, former Chief Executive Officer of General Electric, explained in his book, *Jack: Straight From the Gut*[2], so-called old economy companies are the real beneficiaries of the Internet and information technology:

> In the dot.com atmosphere of the late 1990s, everyone was quick to write off the big, old companies. Everything was focused on anyone starting a new Internet business. One thing that I never fell for was the popular line 'old versus new economy.' People were only buying and selling goods over the Internet — just as they did a hundred years ago from a wagon. The only difference was technology.[3]

Welch goes on to say that digitization was a concept that re-energized General Electric and reduced buying costs, selling costs, and internal paperwork. These same reasons are why many companies are turning toward electronic commerce today. In fact, capital spending on Information Technology ("IT") and the Internet is continuing to grow at an astounding, rapid pace, notwithstanding the recession during the past year, as well as the World Trade Center attacks and related war on terrorism.

Worldwide IT spending growth

Tech sectors are expected to stage a mild recovery in 2002.
Optimistic forecasts put them back at boom-time rates by 2004.



Worldwide IT spending $bn)	2001	2002	2003	2004	2005
Hardware	414	376	371	396	425
Packaged software	181	196	217	250	292
Services	392	426	465	517	580
Total IT	987	998	1,054	1,163	1,297

Source: IDC

2 John F. Welch, Jr., Jack: Straight from the Gut (2001).
3 Id. at 342.

Most of the growth in the United States has been in businesses with fewer than 500 employees. For such companies, insurance should be of particular interest since any large loss may create a business crisis if no insurance exists. However, given the law of large numbers in the insurance industry, a large loss to one policyholder may be small in the context of premiums from many similarly situated policyholders. Although actuarial certainty can vary, insurers with large capital bases are in a better position to evaluate price and pay risks that are insurable. For companies with high rates of return or with other capital needs, insurance can maximize economic returns or free capital that is otherwise needed.

The commercial risks presented by the Internet need to be mapped and analyzed. The cyber insurance risks of an organization should be assessed based upon the volume and type of its e-mails; its Web site activities; the electronic connections it has with its customers, suppliers, employees, and other public and private organizations; the quality and type of its cyber assets and intellectual property; and the type of computer, telecommunication, Web and other related equipment it maintains. However, the most critical factors in assessing an organization's cyber risks are the organization's quality, structure, and type of business. These factors are judged based upon management's commitment to sound business procedures and practices and the quality of the organization's technology staff and vendors. Any past history of service interruptions attacks and claims also need to be considered, as well as the history of similarly situated organizations.

Insurers are in a unique position to compare and evaluate cyber insurance risks. Further, except for the very largest policyholders, insurers have financial strength that overshadows individual policyholders, and insurers are regulated to ensure that adequate capitalization for risks exists. Finally, insurance companies have substantial claim departments with technical expertise and legal resources that rarely are matched by any one insured.

Despite the advantages of maintaining special insurance for these types of risks, the fact is that few in the so-called "new" economy, not even computer security technologists, acknowledge the role of insurance in alleviating the risks associated with doing business in the virtual world. For example, in his book "Netscape Time," Netscape's co-founder and Chairman Jim Clark describes his fears regarding the exposures Netscape faced in the start-up period. Interestingly, there is no mention of insurance in the history of Netscape story. While it is unclear if any insurance was purchased, insurance could have allayed Clark's greatest worries.

Likewise, a survey of the leading books on Internet security and cyber security shows little or no appreciation for the role of insurance. According to a recent report by the Computer Science and Telecommunication Board of the National Research Council, U.S. computer systems are increasingly vulnerable to cyber attacks, and experts estimate that U.S. companies spent $12.3 billion to clean up damage from computer viruses in 2001. Further, the report notes that damages from viruses and worms could be worse in 2002. Given this dire prediction, it is not surprising that

IDC, a provider of data, analysis, and advisory services, estimates that spending on Internet security services totaled $5.1 billion in 2000 and is likely to grow to $14.2 billion by 2005. In this context, insurers are understandably careful in risking their capital, despite the increasing pressure of policyholders seeking coverage.

The CSI/FBI annual survey of computer crimes is used by many computer experts to understand and appreciate the scope of cyber security risks. The magnitude of the survey continues to grow. In 2000, the survey included 273 organizations, of which 42% reported the extent of their losses. Those organizations that reported claimed some $265 million in losses in 2000, including $67 million in theft of proprietary information and $5 million in financial fraud[4]. Ninety percent of those surveyed detected cyber attacks during the past year. Moreover, few participants reported no attacks, and many more reported third-party attacks than in previous years. In total, the aggregate loss in the CSI/FBI survey over a four-year period was $626,309,795[5]. Yet this substantial amount becomes much less substantial when compared to recent cyber security breaches. For example, the aggregate CSI/FBI loss is only slightly more than two times the estimated cost of a single individual's computer hacking spree (Kevin Mitnick — $292 million), and not even 40% of the estimated cost of the 2000 "I LOVE YOU" computer worm[6].

In the book *White-Hat Security Arsenal — Tackling Threats*[7], author Aviel Rubin, an AT&T computer security expert, states as follows:

> Ask a security specialist, a bank manager, an IT manager of a large organization, and a CEO how much damage is caused every year by computer security breaches, and you will get many different answers. Obviously, security experts have an incentive to make the problem seem as large as possible. …While security professionals have a stake in increasing awareness of computer security incidents, corporations often feel that their very existence depends on covering up any incidents lest their customers find out about them and lose confidence in them[8].

Rubin goes on to describe how companies fear stigmatization from public or customer knowledge of a compromise in their systems, victimization by extortion or blackmail, the loss of sensitive databases and confidential data, initiation of false financial transactions, denial of service attacks, false advertising and publicity attacks, and other incidents. He then concludes:

4 Richard Power, Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace, 41 (Queue Corp. 2000).
5 Id. at 43.
6 Id. at 43, 148.
7 Ariel D. Rubin, White-Hat Security Arsenal (Addison Wesley 2001).
8 Id. at 3.

> One thing you know for sure is that the actual damage is much greater than any amount disclosed by anyone. Nobody has any incentive to artificially inflate the amount of damage caused by cyber attack (except, of course, security professionals)[9].

While the damages are difficult to quantify, virtually every computer user, Web site host, and network administrator has become familiar with viruses, worms, Trojan horses, time or logic bombs, and malware or malicious software code, as well as hacking, cracking, sniffing, spoofing, and other means of unauthorized access. For example, in *Hacking Exposed — Network Security Secrets and Solutions*[10], the authors describe at length how computer systems are cased by foot printing, scanning, and enumeration, and how hacking occurs via system, network, and software corruption. Further, in Tangled Web, author Richard Power lists the main types of cyber crime as follows:

- unauthorized access by insiders such as employees;
- system penetration by outsiders;
- theft of proprietary information, e.g. a user ID and password or a million-dollar trade secret;
- financial fraud via computers;
- sabotage of data or networks;
- disruption of network traffic, e.g., resulting from denial of service attacks;
- creation and distribution of computer viruses, Trojan horses, or other types of malicious code;
- software piracy;
- identity theft; or
- hardware theft, e.g., theft of a laptop.[11]

There is no doubt that these types of incidents are increasing in frequency. The Computer Emergency Response Team at Carnegie Mellon University Coordinating Center ("CERT/CC") reports that in 2001 there were 52,000 incidents reports. This compares to 21,756 in 2000 and 9,859 in 1999.[12]

9 Id. at 6.
10 Joel Scambray et al., Hacking Exposed – Network Security Secrets and Solutions (2d ed. Osborne/McGraw-Hill 2001).
11 Supra, note 4, at 4.
12 CERT/CC Statistics 1988-2991, http://www.cert.org/Stats/cert – Stats.html.

Number of Incidents reported to CERT/CC, 1990-2001												
Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859	21,756	52,658

These losses arise from any one of a number of incidents, such as authorized or unauthorized access; faulty or unreliable equipment, software, encryption, certificates or credentials; or human error. Consequently, a leading computer security expert has succinctly stated:

> Managing risk is continuous: You either accept it, reduce it, or insure against it.
>
> Eventually there will be two types of network insurance. The first type is the obvious one: Someone breaks into your network and causes damage, and you want the insurance company to compensate you for your loss. But the second type is even more important: Someone breaks into your network and wreaks havoc with your customers, their proprietary information, and their reputations. The third-party liability can be huge. Not only is it a breach of fiduciary responsibility, but the resulting lawsuits could easily exceed the net worth of the attacked company.[13]

The thesis of this book is that the risks of Internet and e-commerce businesses must be identified and understood. Once these risks are explained, the book considers how specific insurance products can be purchased to address several key areas of exposure, thereby allowing capital providers, directors, officers, and employees of Internet and e-commerce entities to develop their businesses free from unnecessary worries. This is not to say that every type of risk is insurable (or that the price of the insurance will be acceptable to every business), but rather that many of the risks created by these exposures can be reduced significantly.

Another section of this book describes the legal bases for the types of claims likely to arise and the insurance coverages available to protect against digital or cyber losses. Legal trends already indicate that both frivolous and valid claims will be made against Information Age businesses. While earthquakes, hurricanes, tornadoes, fires, and accidents constitute most traditional insurance risks, the possibility of a cyber catastrophic event is equally possible. Those who understand these risks can develop guidelines and loss-control procedures to control them.

The book also addresses reinsurance issues. For insurers and reinsurers, genuine underwriting issues and threats of horrible losses are regularly raised by scaremongers. Reinsurers can provide balance-sheet protection and capacity so that, should the virtual equivalent of a major tidal wave occur, i.e., a cyber Tsunami, a ceding insurer will have adequate reinsurance assets to pay the claims without impairing the insurer's surplus.

13 Bruce Schneier, Secrets & Lies – Digital Security in a Networked World 385, 386 (Wiley Computer Publishing 2002).

This book is primarily targeted to those risks arising under the laws of the United States; as a result, the cases and legislation discussed are decisions of the United States courts and Congress. For more information regarding e-commerce in the international arena, a valuable resource is *E-Commerce: A Guide to the Law of Electronic Business* (Stephen York & Kenneth Chia, eds., 1999).

1.2 United States Department of Commerce Reports

Before the risks of Internet business and e-commerce can be understood, the vast and pervasive scope of this "new" economy must first be appreciated. At this point in time, virtually every American (and indeed, most every person on earth) is aware of the role of the Internet in business practices, and in society as a whole. However, many still fail to understand the significance of the Internet's immeasurable growth in such a short period of time. Thus, a review of this stellar rise will provide today's e-commerce participants with the appropriate background for understanding why these technology risks must be addressed. In this context, the impact of the Internet and e-commerce is astounding as evidenced by several reports issued by the United States Department of Commerce. These reports describe the impact of information technology on the gross national product of the United States and its increasing impact outside of the United States.

1.2.1 Introduction to Reports

The United States Department of Commerce, a federal agency, is charged with measuring and reporting economic data in the United States. To date, the Department of Commerce has released three reports on the Internet and e-commerce: "The Emerging Digital Economy," "The Emerging Digital Economy II," and "Digital Economy 2000." These reports trace the profound impact that the digitalization of the United States is having on the U.S. economy. For the purposes of this chapter, the second report provides the most relevant information. Where appropriate, information from the third report is also cited. The Department of Commerce has also released three reports titled "Falling through the Net," which trace Internet usage patterns in the United States across various demographic groups and geographic locations.

1.2.2 The Emerging Digital Economy II Report

On June 22, 1999, the Department of Commerce released its second report concerning the status of the new economy.[14] The report, issued by the Office of Policy Development of the Economic and Statistics

14 David Henry et al., The Emerging Digital Economy II, (visited Sept. 21, 1999), http://www.ntia.doc.gov/ntiahome/fttn99/execsummary.html>; see generally http://www.ecommerce.gov/ede/chapter1.html>; http://www.ecommerce.gov/ede/chapter2.html>; http://www.ecommerce.gov/ede/chapter3.html>; http://www.ecommerce.gov/ede/chapter4.html>

Administration of the Department of Commerce, begins with a statement by William M. Daley, Former Secretary of the United States Department of Commerce.[15] The executive summary notes that:

- E-commerce and information technology industries ("IT") are evolving at breathtaking speeds, altering every facet of American society.
- The growth of e-commerce is surpassing the previous year's most optimistic projections.
- IT industries (industries producing computer and communication technologies), while accounting for only 8% of the U.S. GDP, contributed to 35% of the nation's real economic growth. Furthermore, these industries brought down overall inflation by 0.7 percentage points.
- From 1990 to 1997, IT-producing industries and the goods-producing subgroup of IT companies have experienced extraordinary productivity gains of 10.4% and 23.9% average annual growth respectively.
- By the year 2006, the Department of Commerce predicts that over 50% of the U.S. workforce will be employed by either major producers or intensive users of IT products and services.
- Finally, in one of the most telling and sweeping conclusions, the executive summary notes that:

> The pervasiveness of information technology, the variety of its benefits to producers and consumers, and the speed of economic change in the digital era have tested the limits of established indices of economic performance.

In effect, the U.S. government has been unable, thus far, to measure the Information Age revolution.

Since issuing the report, the Department of Commerce pledged to move the department from a paper-based government bureaucracy to an all-digital department by 2002.[16] Currently, the Commerce Department's homepage receives 2.5 million hits each day.[17] Further, all of the patent and trademark records, including those dating back to the founding days of the United States, are now online.[18]

15 Executive Summary, The Emerging Digital Economy II, http://www.ntia.doc.gov/ntiahome/fttn99/execsummary.html.

16 U.S. Commerce Secretary Daley to Deliver Digital Department, United States Government Electronic Commerce Policy, Aug. 13, 1999, http://www.ecommerce.gov/. Secretary Daley stated that, "The Department of Commerce is using the web to entirely change the way we deliver information. What E-Bay has done for auctions, we are trying to do for government. I am setting the goal that by the year 2002, the Commerce Department will be truly an e-commerce department." Id.

17 Id.

18 See http://www.uspto.gov/patft/index.html.

1.2.3 The Report

The report consists of four chapters titled "Electronic Commerce In The Digital Economy," "Information Technology Industries," "Contribution of Information Technology to Gross Product Originating Per Worker and Labor Markets in the Digital Economy" and "Labor Markets In The Digital Economy." These chapters provide stark statistics of the changes underway in the business community.

In the first chapter, "Electronic Commerce In The Digital Economy," the Department of Commerce reports that between 1998 and 1999, the number of Web users worldwide increased by 55%, Web hosts increased by 46%, Web servers increased by 128% and new Web address registrations increased by 137%. While the number of users, services, and products continues to grow exponentially, so do the revenues in the computer industry. Internet service providers (ISPs) are reportedly growing at a compound annual rate of 28% . Additionally, revenues from advertising more than doubled between 1997 and 1998, "suggest[ing] the growing importance that businesses are placing on this new way of reaching customers."

While more than half of the estimated 171 million Internet users worldwide are in the United States and Canada, the report notes that this figure is rapidly diminishing as other countries join the global Internet economy. The report cites the recent digitalization of Europe, calling this area the "'fastest growing and most interesting market for Internet development' outside of North America." European nations are not alone in their growing use of the Internet. By 2003, Asia-Pacific, including Japan, will overtake the United States as the largest Internet-subscribing market.[19] While this growth may be impressive, the report also details that many countries are constrained by the lack of a critical infrastructure. As such, it may be some time before a true digitalization of the world occurs. Nonetheless, the study cites that, "[a]s the Internet moves the world toward truly global markets, it seems likely that Internet transactions will grow large enough to measurably impact trade flows. However, the size and direction of those impacts remain uncertain."

Chapter 2, "Information Technology Industries," delineates the types of businesses that comprise the IT industry and traces their impact on the U.S. economy. The report breaks down the IT industry into four principal categories. The first, called "Hardware Industries," includes the following industries:

- Businesses that build computer and computer-related equipment;
- Businesses engaged in the wholesale or retail trade of computers or computer equipment;
- Businesses that create calculating and office machines;

19 Asia-Pacific Internet Market to Overtake U.S. By 2003, The Industry Standard, Aug. 6, 2001, http://www.thestandard.com/article/0,1902,28494,00.html.

- Businesses that create magnetic and optical recording media;
- Businesses that create electron tubes, printed circuit boards, semiconductors, or passive electronic components; and
- Businesses that create industrial instruments for measuring electricity, and other laboratory analytical instruments.

The second group is designated as "Software/Services Industries" and includes:

- Computer programming services;
- Prepackaged software;
- Wholesale or retail trade of software;
- Computer integrated systems design;
- Computer processing, data preparation;
- Information retrieval services;
- Computer services management;
- Computer rental and leasing; and
- Computer maintenance and repair.

The third group, designated as "The Communications Equipment Industry," includes companies producing household audio and video equipment, telephone and telegraph equipment, and radio communications equipment. The last group, "Communications Services Industries," includes businesses providing telephone and telegraph communications, radio and television broadcasting, and cable or other pay television services. All four of these subgroups comprising the IT industry accounted for more than 8% of the total economy in 2000.[20]

Of these four groups, the "Services and Software" industry witnessed the most notable growth. Between 1993 and 1999, this industry grew approximately 10.7% per year. The "Hardware" subgroup of the IT industry also made significant gains, growing an average of 14.2% during those

20 Patricia Buckley et al., Digital Economy 2000, http://www.esa.doc.gov/de2K.htm.

same years. The U.S. economy at large, in contrast, experienced only a 5% increase during the same period.

One of the more unanticipated effects of the IT industry's growth was the effect on inflation. The report notes that:

> During both 1996 and 1997, the prices in the IT sector fell by 7 percent. As a result, overall inflation was 1.9 percent compared with the 2.6 percent inflation in the non-IT producing sector of the economy, a difference of 0.7 percentage points. But the contribution that IT makes to keeping inflation down goes beyond that 0.7 percentage points. The steep declines in IT prices in 1996 and 1997 meant that overall inflation dropped by 0.4 percentage points (from 2.3 and 1.9 percent) even as inflation in the non-IT producing sectors of the economy declined by 0.2 percentage points (from 2.3 percent to 1.9 percent).

Equally important was the IT industry's contribution to real growth of the economy. The report states that while the share of the economy attributable to IT-producing industries grew from 6 to 8% from 1993 to 1998 in terms of dollars, these numbers do not tell the whole story. In terms of real growth, IT industries contributed more than one third to the growth of real output for the overall economy.

IT-Producing Industries: Contribution To Real Economic Growth

	1993	1994	1995	1996	1997 (estimate only)	1998 (estimate only)
Changes in Real Gross Domestic Income (GDI) (in percentage points)	2.2	4.1	2.9	3.5	4.2	4.1
IT Contribution	0.6	0.6	1.2	1.5	1.2	1.2
All Other Industries	1.6	3.5	1.7	2.0	3.0	2.9
IT Portion of GDI Change (2) ÷	26	15	41	42	28	29

Over this same period, IT industries also made significant contributions to U.S. foreign trade. The total combined exports and imports of goods by IT-producing industries rose 11.7% annually versus 8.1% from goods for all other industries. Computer services trade exports and imports grew at 13.2% per year.[21] Overall, the IT-producing industry's contribution to the $1.5 trillion commodity

21 Within services trade, the most notable of growth came in computer-related services. This industry grew at a rate of 25% per year, nearly two and a half times the average rate of growth in services trade overall.

trade flow rose from 16% to 19%. Moreover, increases in both exports and imports raised the negative balance in goods trade by IT-producing industries from $33 billion to $55 billion from 1993 to 1998.

In the third chapter, "Contribution of Information Technology To Gross Product Originating Per Worker," the report "evaluates the impacts of information technology by comparing trends in growth rates in the total private non-farm economy and across three major industry groups defined as IT-producing, IT-using, and non-IT intensive."

An IT-using industry is defined as having either IT capital stock as a share of total equipment stock (net of depreciation) or IT investment per employee. The top 15 industries in terms of IT net capital stock shares include:

- Telecommunications
- Radio and TV broadcasting
- Security and commodity brokers
- Health services
- Motion pictures
- Other services, n.e.c.
- Business services
- Holding and investment services
- Legal services
- Wholesale trade
- Real estate
- Insurance carriers
- Instruments and related products
- Depository institutions
- Insurance agents and brokers

The top 15 industries in terms of IT investment are:

- Telecommunications
- Nondepository institutions
- Pipelines, except natural gas
- Radio and TV broadcasting
- Electric, gas, and sanitary services
- Petroleum and coal products
- Real estate
- Chemicals and allied products
- Insurance carriers

- Depository institutions
- Holding and investment offices
- Railroad transportation
- Wholesale trade
- Motion pictures
- Electronic and other equipment

In contrast to IT-producing industries, which grew between 1990 and 1997, IT-using industries declined 0.1% on average over the same period. However, among goods industries, the report notes that those industries that "make more intensive use of IT inputs had faster improvements in GPO/W than that of non-IT intensive industries." Among services industries, however, those making more intensive use of IT inputs had worse results than other service industries.

Chapter four, "Labor Markets In The Digital Economy," focuses primarily on the effects of the IT industry on employment, wages, and skill requirement and labor market imbalances. Overall, employment growth in the IT-producing industries outpaced average employment growth. From 1989 to 1997 employment in IT industries grew at 2.4% annually versus 1.7% for all other private industries.[22] Since 1996, IT industries have added 350,000 jobs, a one year increase of 7.7% compared with average employment growth of about 3%. These numbers are expected to outpace average employment growth over the next several years.

1.2.4 The Electronic Revolution

Some suggest with some hyperbole that the Electronic Revolution may have the impact of the Industrial Revolution.[23] The Industrial Revolution changed the world from agrarian-based societies to modern industrialized nations. When English Parliament passed the Enclosure Acts that helped spark the Industrial Revolution, few people could envision the enormous changes that were about to happen. Similarly, few could have predicted that the Internet would have such a profound impact in such a short period of time. Consider how long it took these products to be used by 50 million people:

- Radio — 38 years;
- Television — 13 years;
- Cable television — 10 years[24]

22 While jobs in IT-producing industries grew more slowly than overall employment in 1993 and 1994, they increased dramatically in 1995 and thereafter, growing at an average annual rate of 6.5 percent. Patricia Buckley et al., supra note 22.

23 Larry Irving, Assistant Secretary for Communications and Information, U.S. Department of Commerce stated, "the rise of Internet and e-commerce may have as profound an effect [as the Industrial Revolution]. It has enabled us to take part in a global economy and accelerated, beyond all previous dreams, the way we do business and communicate." Larry Irving, The E-Commerce Revolution: The Respective Roles For Industry and Government, 1998 Harbinger Users Conference , Aug. 24, 1998, http://www.ntia/doc.gov/ntiahome/speeches/harbin.htm.

24 Phillip S. Renaud, Electronic Commerce & Transaction Exposures, (May 20, 1999) (unpublished TIX Seminar Series for Insurance Professionals, on file with The Limited, Inc.).

Since the Internet was discovered within the last decade by commercial users, it is estimated that over 100 countries and more than 300 million users have connected to the Internet worldwide.[25] The United States alone accounted for more than 52% of those users in 1999.[26] Only one year later, the United States and Canada together accounted for less than 50 percent of all Internet users worldwide.[27]

This figure highlights a continuing reduction in the gap between users worldwide and the United States and Canada as the Internet expands globally. In 1997, Canada and the United States accounted for 62%[28]. In 1999, that number was somewhere between 52% and 57%[29]. By 2005, non-U.S. Web users will comprise 700 million of the total one billion users worldwide.

No less impressive is the rate at which new technology is being created for the Internet. Some 80% of the technology products on the market today did not exist 18 months ago. The surge of Internet sites within the last decade is equally staggering. In 1994 there were approximately 3,000 sites in the world.[31] In January 2000, more than 1 billion unique pages existed on the Internet.[32]

1.3 What Exactly Is The Internet?

There are many descriptions or definitions of the Internet. A basic user of the Internet might describe the Internet as a means to communicate via e-mail[33], net-conferences, or a way to access information on almost every imaginable subject by "surfing" the net. To an experienced user, the Internet is a vast pool of interconnected data and resources that exist in "cyber-space," ready to be accessed by anyone with a computer, a modem, and a telephone line. To an online retail store or technologist, other descriptions might apply.

The Internet is a global network of computers that allows one to communicate with others by sending data from one computer to another. There is no single owner of the Internet, only individual users, Web site operators, and service providers that supply the hardware i.e. computers, telephone and telecommunication, routers, and other equipment, and software to enable a user to access the Internet. Essentially anyone can access the Internet for information or to create his or her own Web site.

25 Patricia Buckley et al., supra note 20.
26 Win Trese, The Internet Index #24, in The Internet Index, May 31, 1999, http://www.openmarket.com/intindex/99-05.htm.
27 Patricia Buckley et al., supra note 20.
28 Loel McPhee & Jeremy Lieb, Internet Users Top 92 Million In The U.S. and Canada, June 23, 1999, http://www.commerce.net/research/free-report/99_22_26_n.html.
29 Id.
30 October 1999 Internet Economy Indicators, The Internet Economy Indicators, Oct. 29, 1999, http://www.internetindicators.com/global.html.
31 Larry Irving, Voice On The Net: The Promise and the Challenges Ahead, 1998 Voice on the New Conference, Sept. 17, 1998 [hereinafter Voice On The Net] http://www.ntia.doc/gov/ntiahome/speeches/von91798.htm.
32 Inktomi, Inktomi WebMap, Press Release, Jan. 2000, http://www.inktomi.com/webmap.
33 E-mail or electronic mail is a way to send messages from one computer to another electronically.

1.4 What is E-Commerce?

Electronic commerce, or e-commerce, refers to the process of doing business electronically. E-commerce involves at least two parties and is usually either a business-to-consumer transaction or a business-to-business transaction. The American Law Institute formulated the following definition:

> [E-commerce is an electronic transaction] ... in which the parties, or their intermediaries, contemplate that an agreement may be formed through the use of electronic messages or responses, whether or not either party anticipates that the information or records exchanged will be reviewed by an individual.[34]

The benefits of e-commerce can be significant for both consumers and businesses. For the consumer, the benefits include access to retailers 24 hours a day, the ability to compare prices instantaneously, and the freedom to shop outside of their geographic location. For businesses, e-commerce also offers significant rewards. The Internet provides companies with an effective and low-cost way to advertise their products, as compared to the more traditional forms of advertising such as television, magazines, and newspapers. Unlike traditional advertising, the Internet is not limited to distribution in specific geographical areas.

In the United States, which accounts for 95% of consumer purchases on the Internet, e-commerce generated $301 billion in 1998.[35] The revenue totals for U.S. businesses in 1999 were projected to reach $507 billion, surpassing all previous expectations.[36] According to the U.S. Department of Commerce, e-commerce is expected to generate $3.2 trillion in revenue by 2003 and account for 6% of the GDP by 2005.[37] These figures are not altogether surprising considering that it was estimated that consumers would purchase more than 100 million computers in 1999.[38] The statistics overleaf illustrate the various services, revenues, and numbers of people employed in the Internet industry:[39]

34 Uniform Commercial Code Revised Article 2B Licenses -- With Comments (Dec. 1, 1995 Draft) 2B-102(a)(17).
35 Elizabeth Wasserman, Texas Study: E-Commerce Surging, Oct. 27, 1999, The Industry Standard, <http://www.thestandard.com/article/0,1902,7230,00.html.
36 Id.
37 Larry Irving, supra note 31, at http://www.ntia/doc.gov/ntiahome/speeches/harbin.htm.
38 Bill Gates, Letter to Microsoft Shareholders, Annual Report, <http://www.microsoft.com>.
39 Maryann Jones Thompson, Behind The Numbers: Cisco/UT Internet Economy Indicators Study, The Industry Standard, June 20, 1999, <http://www.thestandard.com/metrics/display/0,1283,913,00.html>.

Layer	Description	Companies Included	Internet Revenues	Internet Jobs
Internet Infrastructure	Provides products that create or enable an IP network infrastructure	Net backbones, USPs, hardware and software makers, security vendors	$115.0 bn	372,462
Internet Applications	Creates applications that enable business over an IP network	Consultants, commerce-applications vendors, Web-development software makers, search-engine software	$56.3 bn	230,629
Internet Intermediary	Facilitates the meeting of buyers and sellers online	Online brokerages, ad networks, portals or content aggregators, online travel agents, market makers	$58.2 bn	252,473
Internet Commerce	Sells products over the Internet	Web retailers, subscription-based sites, manufacturers selling online, entertainment and professional services	$101.9 bn	481,990
1999 Totals	—	—	$301.4 bn (adjusted for double-counting across layers)	1,203,799

1.5 Problems Facing The Legal Community

Compounding the uncertainties facing businesses and the insurance industry is the fact that the law is relatively new and unsettled in the area of e-commerce. While the traditional concepts of law and business have evolved simultaneously over many years, the Internet throws a new twist in many of the old legal concepts. Some potential problem areas include:

- Writings — As the law requires certain contracts and transactions be reduced to writing, the question posed by e-commerce is, what constitutes a writing in an electronic transaction?
- Proof — What sort of proof problems are inherent when data can be altered undetectably?
- Jurisdiction — How will the problems of jurisdiction be resolved in light of the fact that the Internet has no geographical boundaries?
- Offer and Acceptance — When is an offer made to form a contract in an online transaction? How may that offer be accepted?

Though some of these issues have already been addressed by the Information Security Committee of the American Bar Association Section of Science and Technology, the National Information Infrastructure (prepared by the U.S. Commerce Department), and the American Law Institute, many have yet to be presented in a court of law. Until these issues are addressed by the courts, the law offers little guidance for businesses and the insurance industry.

1.6 E-Risks: New Insurance Needs

While the Internet and e-commerce offer promising new means by which to conduct business, they also offer a wide range of risks and exposures for businesses. Though some of these risks may be covered by traditional insurance protection, such as a commercial general liability policy, an errors and omissions policy, or fidelity bonds, many are not. An insurance underwriter's perspective on the risks associated with the Internet and their impact on the field of insurance is offered below.

Cyber-Risk Management and Insurance[40]

by Ty R. Sagalow[41]
CEO and Executive Vice President, AIG eBusiness Risk Solutions

Introduction

Traditional approaches to Internet and network security attempted to achieve the goal of the elimination of risk factors through the complete prevention of system compromise through technical and procedural means. It is becoming increasingly clear that such a model is too simple for the increasingly complex world of the Internet. There is simply no magic bullet for computer security; no amount of time or money can create a perfectly hardened system. Insurance must play a part. However, insurance alone cannot act alone as a risk mitigation tool since the front line of defense must always be a complete information security program and security tools and products. It is only through leveraging both approaches in a complementary fashion that an

40 Modified and excepted from *Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security* by Carol A. Siegel, Ty R. Sagalow, & Paul Serritella. The views and policy interpretations expressed in this work by the authors are their own and do not necessarily represent those of American International Group, Inc. or any of its subsidiaries, business units, or affiliates.

41 The author is the Executive Vice-President and Chief Operating Officer of AIG eBusiness Risk Solutions, a division of AIG's American International Companies and a global leader in identifying, evaluating and managing Internet Related Risks. American International Group, Inc. (AIG) is the leading U.S. based international insurance and financial services organization and the largest underwriter of commercial and industrial insurance in the United States. The views and policy interpretations expressed in this work by the author are his own and do not necessarily represent those of American International Group, Inc. or any of its subsidiaries, business units or affiliates. No policy interpretation contained herein should be relied upon by any person in the interpretation of that person's insurance policy. Persons should always seek the advice of counsel or a professional insurance broker before purchasing any insurance product.

organization can reach the greatest degree of risk reduction and control. Thus, today, the optimal model requires a program of understanding, mitigation on and transfer of risk through the use of integrating technology, processes, and insurance – i.e., a risk management approach. Risk management requires a continuous cycle of assessment, mitigation, insurance, detection and remediation:

Assess: An assessment means conducting a comprehensive evaluation of the security in an organization. It usually covers diverse aspects ranging from physical security to network vulnerabilities. Assessments should include penetration testing of key enterprise systems and interviews with security and IT management staff. The assessment should evaluate people, processes, technology, and financial management. The completed assessment should then be used to determine what technology and processes should be implemented to mitigate the risks exposed. They should be done periodically in order to determine new vulnerabilities and to develop a baseline for future analysis to create consistency and objectivity.

Mitigate: Mitigation is the series of actions taken in order to reduce risk, minimize chances of an incident occurring, or limit the impact of any breach that does occur. Mitigation includes creating and implementing policies that ensure high levels of security. Security policies, once created, require procedures that ensure compliance. Mitigation also includes determining and using the right set of technologies to address the threats that the organization faces and implementing financial risk mitigation and transfer mechanisms.

Insure: Insurance is a key risk transfer mechanism that allows organizations to be protected financially in the event of loss or damage. A quality insurance program can also provide superior loss prevention and analysis recommendations, and often offer premium discounts for the purchase of certain security products and services from companies known to the insurer that dovetail into a company's own risk assessment program. Initially, determining potential loss and business impact due to a security breach allows organizations to choose the right policy for their specific needs. The insurance component then complements the technical solutions and policy procedures. A vital step is choosing the right insurance carrier by seeking companies with specific underwriting and claims units with expertise in the area of information security, top financial ratings, and global reach. The right carrier should offer a suite of policies for companies to choose from which can provide adequate coverage.

Detect: Detection implies constant monitoring of assets to discover any unusual activity. Usually this is done by implementing a 24 hour, seven days a week, monitoring system that immediately identifies and prevents any potential intrusion. Additionally, anti-virus solutions allow companies to detect new viruses or worms as they appear. Detection also includes analyzing logs to determine any past events that were missed and specification of action to prevent future misses. Part of detection is the appointment of a team in charge of incident response.

Remediate: Remediation is the tactical response to vulnerabilities that assessments discover. This involves understanding the report that the assessment yields and prioritizing the areas of vulnerability that need immediate attention. The right tactic and solution for the most efficient closing of these holes must be chosen and implemented. Remediation should follow an established, recurring procedure to address these vulnerabilities periodically.

Finally, the whole process starts again with an assessment of the company's vulnerabilities, including an understanding of a previously unknown threat.

Types of Security Risks

The threat from computer crime and other information security breaches continues to increase exponentially. One logical method for categorizing financial loss is to separate loss into three general areas of risk: First Party Financial Risk, which is direct financial loss not arising from a third party claim, called First Party Security Risks; Third Party Financial Risk, which involves a company's legal liabilities to others, called Third Party Security Risks; and Reputation Risk, which includes the less quantifiable damages such as those arising from a loss of reputation and brand identity. These risks, in turn, arise from the particular cyber-activities. Cyber-activities can include having a Web site presence, email, Internet professional services such as Web design or hosting, network data storage, and e-commerce (i.e., purchase or sale of goods/services over the Internet).

First Party Security Risks include financial loss arising from damage, destruction, or corruption of a company's information assets, i.e., data. Information assets, whether in the form of customer lists and privacy information, business strategies, competitor information, product formulas, or other trade secrets vital to the success of a business, are the real assets of the 21st Century. Their proper protection and quantification is key to a successful company. Malicious code transmissions and computer viruses, whether launched by a disgruntled employee, overzealous competitor, cyber-criminal, or prankster, can result in enormous costs of recollection and recovery.

A second type of First Party Security Risk is the risk of loss of revenue following a successful Denial-of-Service ("DOS") attack. In February 2000, a distributed DOS attack was launched against some of the most sophisticated Web sites, including Yahoo, Buy.com, CNN, and others, resulting in $1.2 billion in lost revenue and related damages, according to the Yankee Group. Finally, First Party Security Risk can arise from the theft of trade secrets.

Third Party Security Risk can manifest itself in a number of different types of legal liability claims against a company, its directors and officers, or employees. These risks can arise from the company's presence on the Web, its rendering of professional services, the transmission of malicious code, a DOS attack, or theft of the company's customer information.

The very content of a company's Web site can result in allegations of copyright and trademark infringement, libel, or invasion of privacy claims. The claims need not even arise from the visual part of a Web page but can and often do, arise out of the content of a site's meta-tags, the invisible part of a Web page used by search engines. If a company renders Internet-related professional services to others, this too can be a source of liability. Customers or others who allege that such services, such as Web design or hosting, were rendered in a negligent manner or in violation of a contractual agreement may find relief in the court system.

Third party claims are imaginable directly arising from a failure of security. A company that negligently or through the actions of a disgruntled employee transmits a computer virus to its customers or other email recipients may be open to allegations of negligent security practices. The accidental transmission of a DOS attack can pose similar legal liabilities. In addition, if a company has made itself legally obligated to its customers to maintain its Web site on a continuous basis, a DOS attack shutting down the Web site could result in claims by its customers. A wise legal department will make sure that the company's customer agreements specifically permit the company to shut down its Web site for any reason at any time without incurring legal liability.

Other potential third party claims can arise from the theft of customer information such as credit card information, financial information, health information, or other personal data. For example, theft of credit card information could result in a variety of potential lawsuits, whether from the card issuing companies that must undergo the expense of reissuing, the card holders themselves, or even the Web merchants that later become the victims of the fraudulent use of the stolen credit cards. As discussed later, certain industries such as financial institutions and health care companies have specific regulatory obligations to guard their customer data.

Directors and Officers ("D&Os") face unique, and potentially personal, liabilities arising out of their fiduciary duties. In addition to case law or common law obligations, D&Os can have obligations under various statutory laws such as the Securities Act of 1933 and the Securities Exchange Act of 1934. Certain industries may also have specific statutory obligations such as those imposed on financial institutions under the Gramm-Leach-Bliley Act ("GLBA"), discussed in detail later.

Perhaps the most difficult and yet one of the most important risks to understand is the intangible risk of damage to the company's reputation. Will customers give a company their credit card numbers once they read in the paper that the company's database of credit card numbers was hacked? Will top employees remain at a company so damaged? And, what will be the reaction of the company's shareholders? Again, the best way to analyze reputation risk is to attempt to quantify it. What is the expected loss of future business revenue? What is the expected loss of market capitalization? Can shareholder class or derivative actions be foreseen and, if so, what can the expected financial cost of those actions be in terms of lawyer fees and potential settlement amounts?

GLBA/HIPAA

Title V of the Gramm-Leach-Bliley Act ("GLBA") imposes new requirements on the ways in which consumer data is handled by financial services companies. The primary focus of Title V, and the area which has received the most attention, is the sharing of personal data between organizations and their non-affiliated business partners and agencies. Consumers must be given notice of the ways in which their data is used and of their right to "opt-out" of any data sharing plan. Title V also requires financial services organizations to provide adequate security for systems that handle customer data. Security guidelines require the creation and documentation of detailed data security programs addressing both physical and logical access to data, risk assessment and mitigation programs, and employee training in the new security controls. Third party contractors of financial services firms must also comply with the GLBA regulations.

On February 1, 2001, the Department of the Treasury, Federal Reserve System, and Federal Deposit Insurance Corporation issued interagency regulations in part requiring financial institutions to do the following:

- Develop and execute an Information Security Program.
- Conduct regular tests of key controls of the Information Security Program. These tests should be conducted by an independent third party or staff independent of those who develop or maintain the program.
- Protect against destruction, loss, or damage to customer information, including encrypting customer information while in transit or storage on networks.
- Involve the Board of Directors, or appropriate committee of the Board, to oversee and execute all of the above.

Since the responsibility for developing specific guidelines for compliance was delegated to the various federal and state agencies overseeing commercial and financial services, and some of these guidelines are still in the process of being issued, it is possible that different guidelines for GLBA compliance will develop between different states and different financial services industries.

The Health Insurance Portability and Accountability Act ("HIPAA") will force similar controls on data privacy and security within the health care industry. As part of HIPAA regulations, health care providers, health plans, and clearinghouses are responsible for protecting the security of client health information. As with GLBA, customer medical data is subject to controls on distribution and usage, and controls must be established to protect the privacy of customer data. Data must also be classified according to a standard classification system to allow greater portability of health data

between providers and health plans. Specific guidelines on security controls for medical information have not yet been issued. HIPAA regulations are enforced through the Department of Health and Human Services.

As GLBA and HIPAA regulations are finalized and enforced, regulators will be auditing those organizations that handle medical or financial data to confirm compliance. Failure to comply can be classified as an unfair trade practice and may result in fines or criminal action. Furthermore, firms that do not comply with privacy regulations may be vulnerable to class action law suits from clients or third-party partners. These regulations represent an entirely new type of exposure for certain types of organizations as they increase the scope of their IT operations.

Cyber-terrorism

The potential for cyber-terrorism deserves special mention. After the attacks of 9/11/01, it is clear that no area of the world is protected from a potential terrorist act. The Internet plays a critical role in the economic stability of our national infrastructure. Financial transactions, running of utilities and manufacturing plants, and much more are dependent upon a working Internet. Fortunately, companies are coming together in newly formed entities such as Information Sharing and Analysis Centers to determine their interdependency vulnerabilities and plan for the worse. It is also fortunate that the weapons used by a cyber-terrorist do not differ much from those of a cyber-criminal or other hacker. Thus, the same risk management formula that discussed above should be implemented for the risk of cyber-terrorism.

Insurance for Cyber-risks

Insurance, when property placed, can serve two important purposes. First, it can provide positive reinforcement for good behavior by adjusting the availability and affordability of insurance depending upon the quality of an insured's Internet security program. It can also condition the continuation of such insurance on the maintenance of that quality. Second, insurance will transfer the financial risk of a covered event from a company's balance sheet to that of the insurer.

The logical first step in evaluating potential insurance solutions is to review the company's traditional insurance program. These policies should be examined in connection with a company's particular risks to determine whether any gap exists. Given that traditional policies were written for a world that no longer exists, it is not surprising that these policies are almost always found to be inadequate to address today's cyber-needs. This is not due to any defect in these time-honored policies but simply due to the fact that with the advent of the new economy risks, there has developed a need for specialized insurance to meet these new risks.

One of the main reasons why traditional policies such as Property and Commercial General Liability ("CGL") do not provide much coverage for cyber-risks is they understand the definition of the term "property" to mean tangible property and not data. Property policies also focus on physical perils such as fire and windstorm. Business Interruption insurance is sold as part of a Property policy and covers, for example, lost revenue when a business burns down in a fire. It will not, however, cover e-revenue loss due to a DOS attack. Even "computer crime" policies usually do not cover loss other than for money, securities, and other tangible property. This is not to say that traditional insurance can never be helpful with respect to cyber-risks. A mismanagement claim against a company's directors and officers arising from cyber-events will generally be covered under the company's D&O insurance policy to the same extent as a non-cyber claim. For companies that render professional services to others for a fee, such as financial institutions, those that fail to reasonably render those services due to a cyber risk may find customer claims to be covered under their Professional Liability policy. (Internet professional companies should still seek to purchase a specific Internet professional liability insurance policy.)

Specific Cyber-Liability and Property Loss Policies

The inquiry detailed above illustrates the extreme dangers associated with relying upon traditional insurance policies to provide broad coverage for 21st Century cyber-risks. Regrettably, at present there are only a few specific policies providing express coverage for all the risks of cyber-space. One should be counseled against buying an insurance product simply because it has the name "Internet" or "cyber" in it. So-called Internet Insurance policies vary widely with some providing relatively little real coverage. A properly crafted Internet-risk program should contain multiple products within a suite concept, permitting a company to choose which risks to cover depending upon where it is in its internet maturity curve.[42] A suite should provide at least 6 coverages. These coverages may be summarized as follows:

Web Content Liability provides coverage for claims arising out of the content of a Web site (including the invisible meta-tags content) such as libel, slander, copyright, and trademark infringement.

Internet Professional Liability provides coverage for claims arising out of the performance of professional services. Coverage usually includes Web publishing activities as well as pure Internet services such as being an Internet Service Provider, host, or Web designer. Any professional service conducted over the Internet can usually be added to the policy.

42 One carrier's example of this concept can be found at www.aignetadvantage.com.

Network Security Coverage comes in two basic types:

- **Third Party Coverage** provides liability coverage arising from a failure of the insured's security to prevent unauthorized use or access of its network. This important coverage would apply, subject to the policy's full terms, to claims arising from the transmission of a computer virus (such as the "Love Bug" or "NIMDA" virus), theft of a customer's information (most notably including credit card information), and so-called DOS liability. In the last year alone, there have been reported countless cases of this type of misconduct.

- **First Party Coverage** provides, upon a covered event, reimbursement for loss arising out of the altering, copying, misappropriating, corrupting, destroying, disrupting, deleting, damaging, or theft of information assets, whether or not criminal. Typically the policy will cover the cost of replacing, reproducing, recreating, restoring, or recollecting. In case of theft of a trade secret (a broadly defined term), the policy will either pay or be capped at the endorsed negotiated amount.
  First Party Coverage also provides reimbursement for lost e-revenue as a result of a covered event. Here the policy will provide coverage for the period of recovery plus an extended business interruption period. Some policies also provide coverage for dependent business interruption, meaning loss of e-revenue as a result of a computer attack on a third party business (such as a supplier) upon which the insured's business depends.

Cyber-extortion provides reimbursement of investigation costs, and sometimes the extortion demand itself, in the event of a covered cyber-extortion threat. These threats, which usually take the form of a demand for "consulting fees" to prevent the release of hacked information or to prevent the extortion from carrying out a threat to shut down the victims' Web site, are all too common.

Public Relations or Crisis-communication coverage provides reimbursement up to $50,000 for use of public relation firms to rebuild an enterprise's reputation with customers, employees, and shareholders following a computer attack.

Criminal Reward funds coverage provides reimbursement up to $50,000 for information leading to the arrest and conviction of a cyber-criminal. Given that many cyber-criminals hack into sites for "bragging rights," this unique insurance provision may create a most-welcomed chilling effect.

Loss Prevention Services

Another important feature of a quality cyber-risk insurance program is its loss prevention services. Typically these services could include anything from free online self-assessment program and free educational CDs, to a full-fledged onsite security assessment, usually based on ISO 17799. Some insurers may also add other services such as an internal or external network scan or

other services. The good news is that these services are valuable, costing up to $50,000. The bad news is that the insurance applicant usually has to pay for the services, sometimes regardless of whether it ends up buying the policy! Beginning in 2001, one carrier has arranged to pay for these services as part of the application process. This is welcomed news. It can only be hoped that more insurers follow this lead.

Conclusion

The optimal model to address the risks of Internet security must combine technology, process, and insurance. This risk management approach permits companies to address successfully a range of different risk exposures, from direct attack on system resources to unintentional acts of copyright infringement. In some cases, technical controls have been devised that help address these threats; in others, procedural and audit controls must be implemented. Because these threats cannot be completely removed, however, insurance coverage represents an essential tool in providing such non-technical controls and a major innovation in the conception of risk management in general. Traditional insurance is not up the task of dealing with today's cyber-risks. Thus, insurance programs should include a combination of traditional insurance and specific cyber-risk insurance. A comprehensive policy backed by a specialized insurer with top financial marks and global reach allows organizations to lessen the damage caused by a successful exploit, and better manage costs related to loss of business and reputation.

Cyber Insurance

By Ty R. Sagalow[1]

Table of Sections

1 Executive Summary of Chapter

2 Introduction to Cyber Insurance

3 General Legal Principals
- 3.1 First Party and Third Party Coverages
- 3.2 Claims Made and Occurrence Coverages
- 3.3 The Application Process
- 3.4 Risk Assessment Services
- 3.5 Choosing the Right Carrier

4 The Typical Policy
- 4.1 The Insuring Agreement
- 4.2 Definitions
- 4.3 Exclusions
- 4.4 Limits of Liability
- 4.5 Retentions and Waiting Periods
- 4.6 General Conditions
- 4.7 Endorsements

Continues

1 The author is the Executive Vice-President and Chief Operating Officer of AIG eBusiness Risk Solutions, a division of AIG's American International Companies and a global leader in identifying, evaluating and managing Internet Related Risks. American International Group, Inc. (AIG) is the leading U.S. based international insurance and financial services organization and the largest underwriter of commercial and industrial insurance in the United States. The views and policy interpretations expressed in this work by the author are his own and do not necessarily represent those of American International Group, Inc. or any of its subsidiaries, business units or affiliates. No policy interpretation contained herein should be relied upon by any person in the interpretation of that person's insurance policy. Persons should always seek the advice of counsel or a professional insurance broker before purchasing any insurance product.

Table of Sections (continued)

5 Claims Handling and Coverage Issues
- 5.1 Claims and Incidents
- 5.2 Notice Provisions
- 5.3 Potential Claims and Incidents
- 5.4 Valuation
- 5.5 Duties Under the Policy
- 5.6 Defense Counsel Issues
- 5.7 Settlement

6 Hypothetical Cases

7 Coverage of Hypothetical Cases

8 Conclusion

9 Checklist of Main Points

1 Executive Summary of Chapter

This chapter addresses specialized cyber insurance policies. This type of policy grew out of the existence of an Internet world. As chief technology officers began to understand that there was no magic technology bullet that could eliminate the risks associated with online activity and as risk managers came to understand that traditional insurance policies like Comprehensive General Liability ("CGL") and Property did not cover the vast percentage of Internet exposures, companies called upon insurance carriers to fill the gap.

This chapter addresses the general legal principals applicable to cyber insurance policies, followed by provisions of a typical policy. After reviewing the claims handling and coverage issues potentially applicable to cyber insurance, hypothetical cases are discussed.

2 Introduction to Cyber Insurance

The CSI *2001 Computer Crime and Security Survey*[2] confirms that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting. According to the survey, 85% of respondents detected computer security breaches within the last 12 months, and the total amount of financial loss reported by those who could quantify the loss amounted to $377,828,700, more than $2,000,000 per event.

The financial toll of mass cyber-events is almost beyond belief:

- February 2000 Denial of Service attacks – Estimated Damage: $1.2 billion (Yankee Group)
- "Love Bug" Virus – Estimated Damage: $10 billion (Best's Review)
- "Melissa" Virus – Estimated Damage: $80 million (Best's Review)
- Code Red- Estimated 200,000 computers infected
- NIMDA – Estimated Damage: $500 million (Reuters)

There is no magic technology bullet that can eliminate these and other cyber-risks. Cyber insurance, therefore, plays an essential part of a cyber risk management program.[3]

2 See http://www.gocsi.com for additional information.

3 For a detailed discussion of the total Cyber Risk Management approach, including non-insurance elements, see Chapter 1 of this book.

A quality cyber insurance program should contain three components. First, the program should assist the applicant with its risk assessment. Thus, the carrier should offer robust and generally free loss prevention services. Some of these services should be available regardless of whether the applicant decides to buy insurance. Second, the policy itself should cover up to nine general coverage needs, including both first party and third party coverages (see 4 infra.). Third, the carrier should provide post-incident funding for such things as public relation fees and criminal reward funds. These three components can be further detailed as follows:

Loss Prevention Services

This should include free assessments, potentially including on-site assessments, as well as financial assistance in purchasing recommended security products and services from third party providers. (For more details, also see 3.4 *infra.*)

Insurance Coverage

A robust cyber insurance policy contains the following six coverages in a suite format, permitting the applicant to choose some or all of the coverage parts:

- **Web Content Liability** provides coverage for claims arising out of the content of a Web site (including the invisible meta-tags content) such as libel, slander, copyright, and trademark infringement.

- **Internet Professional Liability** provides coverage for claims arising out of the performing of professional services. Coverage usually includes both Web publishing activities as well as pure Internet services such as being an ISP, host or Web designer. Any professional service conducted over the Internet can usually be added to the policy.

- **Network Security Third Party Coverage** provides liability coverage arising from a failure of the insured's security to prevent unauthorized use or access of its network. This important coverage would apply, subject to the policy's full terms, to claims arising from the transmission of a computer virus (such as the "Love Bug" or NIMDA virus), theft of a customer's information (most notably including credit card information), and so-called Denial of Service ("DOS") liability. In the last year alone countless incidents of this type of misconduct have been reported.

- **Network Security First Party Property Coverage** provides, upon a covered event, reimbursement for loss arising out of the altering, copying, misappropriating, corrupting, destroying, disrupting, deleting, damaging, or theft of information assets, criminal or not. Typically the policy will cover

the cost of replacing, reproducing, recreating, restoring, or recollecting. In case of theft of a trade secret (a broadly defined term), the policy will either pay or be capped at the endorsed negotiated amount.

- **Network Security First Party Business Interruption Coverage** provides reimbursement for lost e-revenue as a result of a covered event. Here the policy will provide coverage for the period of recovery plus an extended business interruption period. Some policies also provide coverage for dependent business interruption, meaning loss of e-revenue as a result of a computer attack on a third party business (such as a supplier) upon which the insured's business depends.

- **Cyber-Extortion** provides reimbursement of investigation costs, and sometimes the extortion demand itself, in the event of a covered cyber-extortion threat. These threats, which usually take the form of a demand for "consulting fees" to prevent the release of hacked information or to prevent the extortion from carrying out a threat to shut down the victims' Web site, are all too common.

Post Incident Support Funds

Finally, Post Incident Support Funds should include:

- **Public Relations or Crisis-Communication** coverage provides reimbursement up to $50,000 for use of public relation firms to re-build an enterprise's reputation with customers, employees, and shareholders following a computer attack.

- **Criminal Reward Funds** coverage provides reimbursement up to $50,000 for information leading to the arrest and conviction of a cyber-criminal. Given that many cyber-criminals hack into sites for "bragging rights," this unique insurance provision may create a most-welcomed chilling effect.

- **Business Interruption Extra Expense** coverage provides reimbursement for certain temporary extraordinary expenses incurred as a covered event such as the cost of a temporary third party hosting facility.

3 General Legal Principals

The scope of a typical cyber insurance policy is varied because, in reality, there is no typical cyber insurance policy. However, at its ultimate, cyber insurance is intended to cover a wide range of legal liability claims arising out of a business' use of the Internet whether for advertising or marketing purposes, communications, or e-commerce. Legal liabilities can arise under federal, state, or foreign

statutory or case law. Finally, a quality policy will also address "first party" financial and even reputation loss suffered by a company in the event of a computer attack.

3.1 First Party and Third Party Coverages

Insurance policies are commonly divided into first party and third party policies. Sometimes, but this is rare, an insurance policy will contain both types of coverages. Such is the case with cyber insurance.

Third party coverage or a third party insurance policy will typically pay "those amounts that you are legally liable" arising out of a covered "claim." The term "claim" in a third party insurance policy is not meant to refer to the "claim" made against the insurance, but rather the claim made by a third party against the insured seeking relief due to an "act, error or omission" or "wrongful act" allegedly done by the insured. Depending upon the definition of "claim" in the policy, the policy might only cover civil lawsuits. Broader definitions of claims cover written demands even if a lawsuit has not been commenced and might include some administrative and criminal proceedings. Loss, which is typically covered under a third party contract, includes defense costs (sometime the carrier will hire the lawyer for the insured, sometimes the insured has to do it), settlements to which the carrier consents, and judgments.

Similarly, first party policies or coverages represent financial losses a person or company can suffer not arising from any claim a third party may have against it. First party coverage can be itself divided into two main groups: Property and Business Interruption. In the brick-and-mortar world, Property policies typically cover damage or destruction of tangible property (like a building) due to a physical peril (like a fire). Theft of a tangible asset (most typically money or securities) is also a subject of Property-like policies typically called Fidelity or Crime policies/bonds. Business Interruption coverage in the brick-and-mortar world covers the loss of revenue due to a Property event. For example, the loss of book sales profits because a book store burned down in a fire. The concept of property damage and business interruption are closely aligned and, indeed, are typically in the same policy form.

In the world of cyber insurance policies, Property coverage means the financial loss arising from damage, destruction or corruption of intangible assets, i.e., data. (Data is generally not covered in brick-and-mortar, i.e., traditional, Property policies.) Theft of data (which generally takes the form of copying) would equally be a subject for first party cyber-property coverages. Similarly, first party cyber-business interruption loosely means the net loss of Internet revenue due to, for example, a denial-of-service computer attack. In both cases, the insured peril is some kind of computer attack, which is itself a broadly defined phrase.

3.2 Claims Made and Occurrence Coverages

In the third party coverage world, policies can be written on a "claims made" or "occurrence" basis. A "claims made" form covers claims made against the insured during the policy period even if the "act, error or omission" which gave rise to the claim occurred prior to a policy period.[4] For example, if the board of a company filed a financial statement with the Securities and Exchange Commission which is later alleged to have contained fraudulent statements, coverage will be provided by the policy if the shareholder lawsuit commences against the board during the policy period, even if the financial statement was filed with the Securities Exchange and Commission prior to the inception date of the policy period, subject to other terms of the policy. Most claims made policies include the ability under some circumstances to report the claim after the policy period as long as the "wrongful act" occurred prior to the end of the policy period (known as the Extended Reporting Provision ("ERP") or Discovery clause). Similarly, most claims made policies include the ability under some circumstances to report incidents that have not yet resulted in an actual claim but which the insured believes may in the future.

In contrast, an "occurrence" policy will provide, subject to its terms, conditions, and exclusions, insurance for a claim against an insured arising from an insured event occurring during the policy period. In this instance, it doesn't matter if the claim is made after the policy has expired.

Claims made policies typically are used in the more specialized policy areas such as directors and officers liability and employment practices liability. In cyber-risk policies, it is the format used for network security liability. Occurrence policies are typically used in the more traditional lines such as CGL and Auto. In cyber-risk policies, some carriers have this option for the Web content or media portions of their policies.

3.3. The Application Process

The length and complexity of the application process for cyber insurance depends greatly on how much and what type of cyber insurance the applicant applies for. On one end of the scale, a policy providing only Web content liability may require answering a few "yes or no" questions on a Web-based application and getting a quote from the underwriter within a day or two. In the very near future, some carriers will offer completely Web-based application, quoting, and binding processes.

On the other end of the scale, a high limit full coverage cyber policy providing insurance for both first and third party coverages might include a three step process: (1) complete an application containing both insurance and technology questions, (2) take an online security assessment, and (3)

4 Of course, the claim would be subject to the other terms, conditions, and exclusions of the policy, including provisions related to how far back the carrier will allow the act, error or omission to have taken place for coverage to apply.

undergo an onsite security assessment. In reality, steps (2) and (3) should be seen as an added value by the carrier consistent with a company's ongoing security assessment processes. As discussed below, these services should be given free of charge to the applicant whether or not it ends up buying insurance.

The key to a smooth application process is getting the right people to talk to the right people. More specifically, questions about insurance can be answered by the company's risk manager or broker. However, questions dealing with technology should immediately been sent to the company's chief technology or information officer. If the company outsources its security then the outsourced company working together with the appropriate company employee should answer the questions. The flip side is equally important. As will be discussed, it is critical to have a knowledgeable and experienced underwriter to receive the answers and to be available for meetings or phone calls if more clarity is needed from the carrier or more information is desired from the applicant.

An underwriter equipped with a complete application and related documents (such as assessments) should be able to give a quote within one to ten days, depending upon the complexity of the insurance desired. Even assuming the requirement of an onsite assessment, the entire process from application to quote should be able to be done within 30 days.

3.4 Risk Assessment Services

An insurance program that consists of an application, a policy, and a check (hopefully) in the event of a covered claim should be considered wholly inadequate. A program this narrow eventually leads to high premiums, difficult claim payouts, and negative feelings between insured and carrier. The first obligation of the insurance relationship is to assist the company in preventing or lowering the risk of a loss in the first place. How well an insurer does this is the best first indication of its value. A quality risk assessment service program contains the following elements:

- Free online assessment;

- Free onsite assessment conducted by a qualified *third party* independent provider. The reputation and experience of the third party provider is a company's second indication of the value of the insurer. Since the carrier is paying for the assessment, it may condition its availability on the company applying for a certain level of insurance. However, the carrier should NOT condition the assessment (or its free nature) on whether the company ultimately buys the insurance. The third party provider should be a company with global abilities; and

- An alliance with multiple technology companies providing high quality security products and services. The insurer should offer insurance premium discounts for the purchase of recommended security products and services from recognized third party providers. While the carrier does not

guarantee these products and services or take direct legal liability if they fail, in purchasing them an insured will know that the carrier believes that the insured has lowered both parties' risk. In effect, they are subsidizing the cost of the purchase. Discounts can typically range from 5 to 15%.

3.5 Choosing the Right Carrier

The critical decision of which carrier to choose cannot be over-emphasized. It is a company's first decision and, possibly, its most important. Cyber insurance is a new line of business, and few insurers have fully committed to it. Yet, a full commitment is exactly what an insured requires if it is to minimize potential losses, obtain swift and appropriate insurance recovery, and, finally, repair any damage to its reputation and build for the future.

Recommended standards for a cyber insurance carrier are represented in the following chart:

Quality	Preferred or Minimum Threshold
Financial Strength	Triple-A from Standard & Poor
Experience	At least two years in a dedicated, specialized unit composed of underwriters, claims, technologists, and legal professionals
Capacity	Defined as amount of limits a single carrier can offer, minimum acceptable: $25,000,000
Territory	Global presence with employees and law firm contacts throughout the U.S., Europe, Asia, Middle East, and South America
Underwriting	Flexible and Knowledgeable
Staff/Structure	Underwriters, claims, technologists, and legal professionals in a dedicated unit. Head of unit should be a seasoned professional with minimum of 15 yrs of insurance experience
Claims Philosophy	Customer focused and willing to meet with client both before and after claim
Policy Form	Suite permitting insured to choose the right type of coverage including third and first party insurance
Loss Prevention	Array of services, most importantly including FREE onsite security assessments conducted by well-established third party (worldwide) security assessment firms

4 The Typical Policy

Cyber-insurance is so new that a typical policy does not exist. Companies need to be aware that the appearance of the word "cyber" or "Internet" in an insurance policy title means little. A quality policy should contain at least six coverages and three post-incident support funds from which the applicant may choose some or all. (See, generally, section 2, *supra*.)

With the above caveat in mind, an cyber-insurance policy will most likely contain a *declarations page*, which serves to highlight the basic coverage points of the policy such as its effective and expiration dates, limits of liability, coverage grants, retentions or deductibles, etc. After the declarations page, the policy itself follows. Typically, this begins with one or more *insuring clauses*, which serve to state the basic grant of insurance; *definitions*, which can serve to expand or restrict coverage; *exclusions*, which serve to indicate those areas in which insurance coverage cannot be granted; and finally, other conditions, which include a discussion of the policy's limits of liability, self-insured retentions or deductibles, rights and obligations of the parties in the event of an actual claim, arbitration and valuation clauses, among other provisions. Following the "guts" of the policy, there may be one or more endorsements. Endorsements are used either to comply with specific state requirements or to further customize the policy based on the negotiation of the parties to a particular contract. It is important to understand that a quality carrier should be open to the specific needs of a potential insured. The willingness and ability to manuscript changes to its basic policy form if needed by the applicant and if consistent with the carrier's underwriting discipline is another important factor in deciding among carriers.

4.1. The Insuring Clause

As stated above, the insuring clause or insuring agreement is the basic grant of coverage under the policy. When well-written it should serve to give the reader the gist of what insurance the policy is granting. In a comprehensive cyber-policy, there should actually be several insuring agreements, including both first party and third party coverages. Quality insurance programs will then offer the applicant the ability to choose one or all of the coverages depending upon their needs. A comprehensive cyber-insurance policy will have seven insuring agreements as follows:

1. Web Content or Media Liability

2. Internet Professional Liability

3. Network Security Liability

4. Cyber-Extortion

5. First Party Property and Business Interruption (either as one combined agreement or two separate agreements)

6. Post Incident Public Relations or Crisis Communication Fees

7. Post Incident Criminal Rewards Funds

Following the seven insuring clauses is an insuring clause dealing with coverage for the costs of defending covered claims.

Each insuring clause is discussed in turn.

4.1.1 Web Content or Media Liability Insuring Agreement

A sample Web Content insuring agreement is reproduced below:[5]

A. Media Liability Coverage

> We shall pay on your behalf those amounts, in excess of the applicable Retention, you are legally obligated to pay, including content-based liability and liability assumed under contract, as damages, resulting from any claim(s) made against you for your wrongful act(s) in the display of Internet media. Such wrongful act(s) must occur during the policy period.

The above is a typical third party coverage grant that promises to "pay on your behalf those amounts…you are legally obligated to pay" others. The insured's legal obligation must arise from a claim made against it arising from its wrongful act in the display of Internet media, which caused damages to another. The full meaning of this statement can be understood only by reviewing the defined terms. (This policy in the Appendix bolds its defined terms making them easier to recognize.) A discussion of key definitions follows this section, see 4.2, *infra*.

Note that this particular Web content coverage grant is on an occurrence basis. This can seen by the last line in the clause, which states that the wrongful act must occur during the policy period. While Web content insuring agreements can be written in either occurrence or claims made formats, most insureds prefer the occurrence format as being more historically consistent with other media type insurance policies.

5 For simplicity and policy structure consistency, unless otherwise noted, all policy references are from form 77576 (6/01), AIG netAdvantage Complete℠, from American International Companies. A full copy of that form is included in the appendix to this book.

Finally, note that the insuring clause talks of the insurer paying for damages for which the insured is legally responsible. Coverage for the costs of defending the claim is dealt with in a separate section.

4.1.2 Internet Professional Liability Insuring Agreement

A sample Internet Professional Liability insuring agreement is reproduced below:

B. Professional Services Liability

(1) We shall pay on your behalf those amounts, in excess of the applicable Retention, you are legally obligated to pay, as damages, resulting from any claim(s) first made against you and reported to us in writing during the policy period or Extended Reporting Period (if applicable), for your wrongful act(s). Such wrongful act(s) must occur on or after the Retroactive Date and be in your performance of:
a. Internet technology services; or
b. Internet professional services (other than Internet media services).

(2) We shall pay on your behalf those amounts, in excess of the applicable Retention, you are legally obligated to pay, including content-based liability and liability assumed under contract, as damages, resulting from any claim(s) made against you for your wrongful act(s) in your performance of Internet media services. Such wrongful act(s) must occur during the policy period.

This somewhat complicated insuring agreement provides insurance for three different types of professional services: Internet technology services, Internet professional services, and Internet media services.

The first clause reads similar to the Web content third party liability clause (see 4.1.1, *supra*) by indicating that the policy shall "pay on your behalf those amounts … you are obligated to pay" arising from a "wrongful act" the insured has allegedly committed against another. However, unlike the Web content clause, this insuring agreement uses the claims made format. Notice the requirement that the claims must be "first made against you … during the policy period." Also, unlike an occurrence grant of insurance, which requires the wrongful act to have happened during the policy period, the claims made format only requires that the wrongful act occur after the "Retroactive Date," a date usually coinciding with the inception date of the first cyber-policy purchased from the carrier. Like most claims made clauses, this indicates that claims can also be made against an insured during an "extended reporting clause." The terms "Internet technology services" and "Internet professional services" will be addressed infra.

The second clause grants coverage for claims arising from the third type of Internet professional services, referred to as "Internet media services." This clause uses the occurrence format, no doubt to be consistent with the Web media insuring clause reviewed earlier. It is important not to confuse "Web content" insurance coverage with "Internet media services" insurance coverage. The former is a base insuring need for anyone who has a Web site and essentially focuses on Web advertising exposure. It does not arise from or require that the insured render any type of media or publishing professional services. The Internet media services coverage grant is for those companies providing professional publishing or media services to others.

4.1.3 Security Liability Insuring Agreement

A sample network Security Liability insuring agreement is reproduced below:

C. Security Liability Coverage

> We shall pay on your behalf those amounts, in excess of the applicable Retention, you are legally obligated to pay, as damages, resulting from any claim(s) first made against you and reported to us in writing during the policy period or Extended Reporting Period (if applicable) for your wrongful act(s). Such wrongful act(s) must occur on or after the Retroactive Date set forth in the Declarations and result in a failure of security of your computer system.

This insuring grant uses the now familiar third party liability language, "pay on your behalf those amounts … you are legally obligated to pay." The format used is "claims made." At this point, it also becomes clear that it is convenient to use universal terms, such as "wrongful acts," in a policy containing multiple third party coverage sections with the definition of wrongful act becoming a key to understanding the differences between the clauses. Note, finally, that the nature of this coverage is also evidenced by the fact that coverage requires a "failure of security" of the insured's computer system.

4.1.4 Cyber-Extortion Insuring Agreement

A sample cyber-extortion insuring agreement is reproduced below:

D. Cyber-Extortion Coverage

> We shall indemnify you for those amounts, in excess of the applicable Retention, you pay as extortion monies resulting from an extortion claim first made against you and reported to us in writing during the policy period.

This insuring agreement is a slight variation from the straight third party claims made coverage language seen earlier. Here the carrier is indemnifying the insured rather than paying on its behalf. Usually due to public policy concerns, the policy requires the insured to first pay the extortion demand and then seek reimbursement from the carrier. Also in this clause the term "extortion monies" is substituted for "damages," and "extortion claim" is substituted for "claim." Finally, it should be noted that the theory behind cyber-extortion insurance is that often it is cheaper for both the insured and the insurer to deal with a cyber-extortion threat up front (including coverage for investigation costs) rather than ignore the threat and then be forced to deal with the financial consequences of an actual computer attack should be threat be successfully implemented.

4.1.5 Network Security Property Damage and Business Interruption Insuring Agreement

A sample network security property damage and business interruption insuring agreement, called in this policy Asset and Income Protection, is reproduced below:

E. Asset and Income Protection Coverage

> We shall pay direct loss, which you suffer, in excess of the applicable Retention, resulting from injury to your information assets first occurring during the policy period. We will also pay direct loss in the form of Internet business interruption and Internet extra expense. In all cases, such loss must first occur during the policy period and result from a failure of security of your computer system that also first occurs during the policy period.

Absent from this insuring clause is the "pay on behalf amounts you are legally obligated to pay" language of the other insuring agreements. The reason is that this insuring clause grants first party coverage for insured events. If an insured suffers an event described in the clause, it can seek reimbursement for its financial loss by submitting a "proof of loss" to the carrier on a timely basis. There is no requirement that the event result in any claim by a third party against the insured.

The covered losses are an "injury to your information assets," meaning damage or theft of a company's data as well Internet business interruption and related coverages like Internet extra expense, arising from a failure of security. (These phrases will be discussed in more detail in our discussions of the definition section of a cyber-policy, see generally 4.2, *infra*.) These losses must occur as a result of a failure of security. Finally, note that typical of first party policies, the events must occur during the policy period.

4.1.6 Criminal Reward Fund Insuring Agreement

A sample Criminal Reward Fund insuring agreement promises to pay up to $50,000 in the insurer's discretion "as a criminal reward fund for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act related to any coverage under this policy." While there are many reasons why computer attacks are launched, a fairly common reason is for bragging rights. By creating a reward fund, the carrier hopes to create a chilling effect against bragging and, in turn, prevent those attacks launched for bragging rights. Given the young age of many hackers today, it can only be hoped that this technique will be successful. Finally, note that this feature is most useful when made available by a worldwide insurance company with contacts at federal, local, and foreign law enforcement agencies.

4.1.7 Crisis Management

A sample crisis management or crisis communication insuring agreement promises to pay up to $50,000 for "crisis expenses in connection with a crisis event first occurring during the policy period." Crisis expenses are essentially fees for public relations companies hired to restore confidence to a company's employees, shareholders, and customers after a successful computer attack. Recognizing the need for post-incident reputation support is an important indicator of the quality of a cyber insurance policy.

4.1.8 Costs of Defense and Duty to Defend

As is the case with many professional liability forms, cyber insurance policy forms usually grant insurance for the cost of defending the claim. This is an essential element of coverage.

Cyber insurance policies typically include a "duty to defend." This is generally favorable to insureds because it states that insurer must provide a defend against allegations even "if the suit is groundless or fraudulent." This includes the hiring of an attorney (see 5.6, supra) and payment of his or her legal fees, excess of any self-insured retention or deductible.

Please note that defense costs are included within the limit of liability of the policy and therefore should be handled with care since payments for defense costs reduce the available limit for settlement and judgments.

This insuring clause will be revisited in a discussion of defense counsel and settlements issues, see 5.6 and 5.7, *infra*.

4.2 Definitions

The definitions in a cyber insurance policy play a key role in determining coverage under a claim. While many policy readers will immediately jump to the exclusion section of a policy to evaluate whether the basic grants of coverage under the insuring clauses have been narrowed, the definition section can be as fruitful as the exclusion section in determining the scope of the policy. Depending upon how terms are defined, coverage under the policy may be greatly restricted or expanded by the definition section.

For the purposes of this analysis, key definitions generally applicable to a sample cyber-policy will first be reviewed, then key definitions applicable to only certain insuring clauses will be considered.

4.2.1 General Definitions

Key definitions, at least with respect to the third party insuring clauses, include "claim," "claim expenses," "damages," and "insured." Another key definition, "wrongful acts," is best discussed in connection with specific insuring agreements.

"Claim" is, for obvious reasons, a critical definition. Properly written, the term "claim" will include lawsuits as well as pre-suit written demands. A failure to include written demands in the definition of "claim" should be considered a negative feature.

An acceptable definition of "claim" might read as follows:

Claim means:

(1) A demand for money, services, non-monetary or injunctive relief; or
(2) A suit (including a civil, criminal or arbitration proceeding) for monetary or non-monetary relief.

This sample definition contains some extremely favorable features such as the inclusion of non-monetary as well as monetary relief (a good example of a claim for non-monetary relief is a demand to change the content of a company's Web site because it allegedly violates another's person copyright), as well as coverage for criminal and arbitration proceedings.

"Claim expenses" (sometimes called "defense expenses," or "costs, charges, and expenses of defense") are the cost of legal fees and related costs associated with the defense or investigation of a covered claim. To be covered, claim expenses must be consented to by the insurer and should include most appeal bonds premiums in cases where an appeal is undertaken with the approval of the insurer. Salary, overhead, and other compensation of the insured's employees are not covered.

"Damages" represent the indemnity payment the carrier will make as a result of a covered judgment after trial or a settlement to which the carrier has consented. A highly desirable feature in this definition is if punitive and exemplary damages are covered where permitted by law. Finally, both pre-judgment as well as post-judgment interest should be covered.

"Damages" is also a good example of a definition that includes limitations. Many times seen by the insurer as a clarification of intent, a policy will indicate that damages for which the insured is not legally liable – such as if the insured consents to a settlement on the condition that the plaintiff will only seek to recover from the carrier – are not covered. This would also be excluded by the consent to settlement clauses in the policy. In addition, the carrier may take this opportunity to clarify that the policy is not intended to put the insured in a better position than where it began by, for example, paying for improvements or enhancements to its company's programs. Finally, damages cannot include amounts that are prohibited by law, such as punitive damages in those states where they are uninsurable as a matter of public policy.

A definition of damages that includes all of the above features would be as follows:

> Damages means that part of loss consisting of any amount that you shall be legally required to pay because of judgments, arbitration awards or the like rendered against you, or for settlements negotiated by us with your written consent; provided that damages shall not include any amounts for which you are not financially liable or for which there is no legal recourse against you, the costs and expenses of complying with any injunctive or other form of equitable relief, or matters that may be deemed uninsurable under the law.

Damages shall also include:

(1) Punitive, exemplary and multiple damages (where insurable by law);

(2) Pre-judgment interest;

(3) Post-judgment interest that accrues after entry of judgment and before we have paid, offered to pay or deposited in court that part of the judgment within the applicable Limit of Liability; and

(4) Damages by reason of content-based liability or liability assumed under contract.

The seemingly innocent definition of insured (sometimes written as the even more innocently sounding phrase "you") can be more complicated than it initially appears. For example, an expansive definition of insured should include:

(1) The policyholder (sometimes called the Named Insured);

(2) Any past, present, or future subsidiary of the policy holder for acts committed while it was a subsidiary (depending upon their size, coverage for future subsidiaries may require an additional premium to add them to the policy);

(3) Any past, present or future director, officer or employee while acting in their capacity as such;

(4) Leased workers (usually itself a defined term);

(5) Independent contractors with respect to publishing or media claims; and

(6) Other persons or entities that are added by endorsement.

4.2.2 Web Content Liability Definitions

In addition to the general definitions just discussed, insuring agreement definitions relevant to the Web content liability part of the sample cyber insurance policy also include references to "wrongful act" and "Internet media."

"Internet media" should include any material displayed on an Internet site whether the material is created by the insured or others and whether the material is an advertisement for the insured's own good and services or the good and services of another company. A definition that accomplishes this might state:

> Internet media means any material on your Internet site, including advertising. Advertising means the material in any publicity or promotion including branding, co-branding, sponsorships and/or endorsements on your own behalf or for others on your Internet site.

A key definition in any third party liability coverage is that of "wrongful act." For Web content and other media liability exposures, the term "wrongful act" essentially means any act, error, or omission that results in copyright or trademark infringement, defamation, libel, slander, or invasion of privacy. The sample definition includes this and more:

> Wrongful act(s) means:
> Any actual or alleged breach of duty, neglect, act, error, misstatement, misleading statement, omission that results in:

(1) Any form of defamation or other tort related to disparagement or harm to character, including libel, slander, product disparagement, trade libel, infliction of emotional distress, outrage or outrageous conduct;

(2) An infringement of copyright, domain name, title, slogan, trademark, trade name, trade dress, mark or service name, or any form of improper deep-linking or framing; plagiarism, piracy or misappropriation of ideas under implied contract or other misappropriation of property rights, ideas or information; or

(3) Any form of invasion, infringement or interference with rights of privacy or publicity, including false light, public disclosure of private facts, intrusion and commercial appropriation of name, persona or likeness.

Especially attractive about the sample definition is the express reference to domain name, deep-linking and framing as potentially covered wrongful acts.

4.2.3 Internet Professional Liability Definitions

The previous discussion discussed the definitions of "claim," "insured," "damages," and "claim expenses." Definitions relevant to the Internet professional liability part of the sample cyber insurance policy also include references to "wrongful act" and three different kinds of "professional services."

For the professional liability part of the cyber-insurance policy, the term "wrongful act" essentially means an act, error, or omission in the rendering or failure to render professional services to others. The term "professional services," in turn, means the three kinds of professional services listed: Internet professional services, Internet technology services, and Internet media services.

Some professional services companies mistakenly believe that all their liabilities must inherently arise out of their professional services and thus all of their legal exposures will be covered by a professional services liability insuring agreement or policy. Regardless of how broad a professional liability coverage grant is written, certain errors, like accidentally sending a virus to a supplier, would not be covered under this insuring grant.

The sample policy's definition of wrongful act for the Internet professional liability insuring agreement is:

> any actual or alleged breach of duty, neglect, act, error, misstatement, misleading statement, omission in the rendering of or failure to render professional services to others, including a failure that results in or from a specified event.

The express reference to a "specified event" is a positive feature. "Specified events" are unauthorized access or use of a computer system, virus transmissions, or DOS attacks. This phrase is meant to confirm that professional service errors that either result in one of these network security failures OR results from (having both elements is especially favorable) one of these network security failures is expressly meant to be covered by the policy subject to its other terms, conditions, and exclusions.

The term "Internet professional services" is defined as a list of services commonly provided by Internet professionals. While the list is usually broad, it is important that insurance applicants review the list of covered services to make sure that the types of services they perform are on the list. Quality policies will include a catch-all item that allows additional services to be added by endorsement.

"Internet technology services" means the technology, hardware, software, and related services that a company renders in connection with its Internet professional services. An example of this would be the creation of customized software done in connection with hosting, Web design, or other covered professional services.

The sample policy defines "Internet media services" as "consulting, advertising, webcasting, electronic publishing, transmission, republication, retransmission, utterance, dissemination, distribution, serialization, creation, production, origination, exhibition, displaying, researching or preparation of material in connection with your Internet professional services."

4.2.4 Network Security Liability Definitions

Definitions relevant to the network security liability part of the sample cyber insurance policy include references to "wrongful act" and the concept of a "failure of security," including the definition of "computer attack."

For the network security part of the cyber insurance policy, the term "wrongful act" essentially means, an act, error, or omission that results in a computer attack, including the theft of customer information, transmission of a computer virus, or DOS attack.

The sample policy defines "wrongful act" for the purposes of this clause as follows:

> any actual or alleged breach of duty, act, error or omission involving your computer system, which results in:
>
> (1) Unauthorized use or unauthorized access (including a computer attack);

(2) Disclosure of confidential or private information concerning your customer, client or other third party;

(3) Transmission of a malicious code; or

(4) Denial of service.

The definition provides a useful roadmap to the types of network security claims that can be faced by an organization. Important especially to financial institutions, healthcare organizations and e-tailers is the express coverage for computer attacks resulting in disclosure of customer confidential information. An express reference to this type of liability is a positive feature.

The definition of "wrongful act" refers to other important definitions, possibly the most important of which is "computer attack." It is especially important for the term "computer attack" to be broadly written in a cyber insurance policy and must include attacks brought by both insiders and outsiders and cover attacks regardless of the motive of the attacker. Again, the sample definition is useful:

> Computer attack means unauthorized access, unauthorized use or transmission of a malicious code which alters, copies, misappropriates, corrupts, destroys, disrupts, deletes or damages your computer system whether intentional or unintentional, hostile or otherwise and regardless of whether the perpetrator is motivated for profit. Computer attack shall include denial of service as a result of any of the aforementioned intentional conduct.

The essence of the network security coverage is the failure of the security of a company to prevent a computer attack. "Security" should be broadly defined:

> Security includes, without limitation, firewalls, filters, DMZ's, computer virus protection software, intrusion detection, the electronic use of passwords or similar identification of authorized users. Security also includes your specific written policies and procedures relating to the theft of a password or access code by non-electronic means.

The concept of how this failure of security takes place is important. Of course, failure can be a result of a failure in hardware, software, or firmware to stop an attack. However, history has shown that many computer attacks are a result of so-called "social engineering," the ability to access a company's computer system by taking advantage of its manmade flaws. By far the most common example of this is the "non-electronic" theft of passwords. Accordingly, network security insurance policies should contain an express reference to this type of event. An acceptable phraseology for this concept is:

> Failure shall also include such inability caused by a theft of a password or access code by non-electronic means in violation of your specific, written security policies and procedures.

4.2.5 Cyber-extortion Definitions

The previous section analyzed the definitions of "claim," "insured," "damages," and "claim expenses." The relevant definitions for the cyber-extortion coverage are derivatives of these.

An "extortion claim" essentially is a claim that takes the form of a threat to commit an intentional computer attack. Extortion expenses are the costs, essentially investigation expenses by a qualified firm, to determine the validity and level of threat of the extortion demand. Extortion monies are the actual payments to the extortionist. For coverage to apply, extortion expenses and extortion monies must be consented to by the insurer. The purpose of paying the extortion monies is to avoid a larger loss in data damage or business interruption that the carrier would otherwise have to pay.

4.2.6 Cyber-property damage or Asset Protection Definitions

The concept of a failure of security has been previously discussed (see, 4.2.4, *supra*.) Other key definitions in the asset protection insuring agreement are "loss" and "injury to information assets."

"Injury to information assets" essentially means the damage, destruction, corruption, copying, or theft of data or other information assets. The sample policy defines the concept as follows:

> Injury means the altering, copying, misappropriating, corrupting, destroying, disrupting, deleting, damaging or theft of information assets, whether or not criminal or intentional. Information assets means your computer system including the electronic data stored therein. Electronic data includes, without limitation, customer lists and information, financial, credit card, competitive, and confidential or private information stored electronically. Information assets shall only include trade secrets if such coverage is specifically provided by written endorsement to this policy. Information assets shall also include the capacity of your computer system or its components to be available to its users, including but not limited to memory, bandwidth, processor time, use of communication facilities and any other computer-connected equipment.

Favorable features in the sample policy definition indicate that the computer attack need not be criminal or intentional, as well as the reference to bandwidth as an information asset. Also note that theft (which usually takes the form of copying) of an information asset dovetails into the policy's

requirements for trade secret coverage. Trade secret is a broad term essentially including any data that has independent value from not being generally known. The value of a trade secret can be source of great argument between the carrier and the insured at the time of a claim. The best method to handle this potential conflict is a policy requirement to schedule trade secrets by endorsement with an indication of their value.

Assuming there is an injury to your information assets that meets the other requirements of the policy, it is important to know how the carrier determines loss. "Loss" for the purposes of this insuring agreement is essentially defined as the cost to replace, reproduce, recreate, restore or recollect information assets (known as the five "R"s), or if none of that is possible, then the cost of making that determination. The sample policy states the concept as follows:

> With respect to injury to your information assets under coverage E, the actual and necessary costs you incur for replacing, reproducing, recreating, or restoring your information assets; provided, however:
>
> a. if such information assets cannot be replaced, reproduced, recreated or restored, but can be recollected, then loss shall mean only the actual cost for recollection of the data; and
>
> b if such information assets cannot be replaced, reproduced, recreated, restored or recollected, then loss shall mean only the actual cost to reach this determination; and
>
> c. in all events, if such information assets are trade secrets, then loss shall mean the amount set forth in section V.E. (N.B. Section V.E. indicates the value of a trade secret shall be the amount scheduled for the trade secret.)

4.2.7 Cyber-business interruption or Income Protection Definitions

Other key definitions in the business interruption insuring agreement are "loss" and the various kinds of "internet business interruption."

The definition of business interruption in cyber-insurance policies is not substantially different than its brick-and-mortar cousins. The main difference between the policies is not so much as how they define business interruption as what is the triggering event leading to the business interruption. In traditional property policies, there must be direct physical loss, for example, a fire or windstorm. In cyber-policies, the triggering event is a computer attack resulting from a failure of Internet and network security.

Nevertheless, it is useful to review the concept of business interruption from a definitional viewpoint. Most quality cyber insurance policies will, in fact, have three types of covered business interruption: Internet business interruption, extended Internet business interruption, and dependent Internet business interruption.

"Internet business interruption" (which is also used to define loss) is essentially defined as "actual loss you sustain during the period of recovery due to the disruption, interruption, delay, or suspension of your ability to conduct your business on the Internet as a result of a failure." "Period of Recovery" essentially means "the length of time starting with the actual disruption, interruption, delay, or suspension of your ability to conduct your business on the Internet and ending with the resumption of your normal ability to conduct your business on the Internet."

A favorable feature of the policy language quoted above is that the period of recovery is not capped or limited to a maximum number of days.

It is important that business interruption coverage is not restricted to those companies operating on a net profit. Accordingly, a favorable feature of a cyber insurance policy is the inclusion of language indicating the companies with a net loss can still suffer business interruption expenses. The sample policy handles this issue by using the following language:

> In the event that at the time of loss you are in a net loss position before income taxes, we will determine the extent to which the continuing fixed charges and expenses, including ordinary payroll, would have been earned by subtracting the net loss from the reasonable and necessary charges and expenses that necessarily will continue.

In addition to basic Internet business interruption, quality cyber policies will also provide Internet extended business interruption, whose purpose is to extend coverage beyond the date in which the company "resumes the normal ability to conduct your business on the Internet" until such date the company is operating at "the level which would generate the Internet business interruption amount that would have existed if the covered loss had not occurred." Extended business interruption is usually capped at a maximum of 90 days.

Quality cyber insurance policies will include the concept of dependent business interruption. This feature provides coverage for business interruption loss resulting from a failure of security of a company on which the insured is dependent. An example of this might be the shutting down of an insured's ISP or host due to a failure of security of that company resulting in business interruption loss of the insured company.

Finally, quality cyber insurance policies will also include coverage for Internet extra expense, whose purpose is to reimburse the insured for certain temporary expenses incurred solely as a result

of undergoing an insured event. A good example of this is the temporary leasing of a third party hosting facility while the insured's hosting facility is being reconstituted.

4.2.8 Criminal Reward and Crisis Communication Funds Definitions

There are no special definitions associated with the criminal reward fund feature of a typical cyber insurance policy. Assuming the requirements of the insuring clause are met (see 4.1.6, *supra*), a reward fund up to $50,000 paid for by the carrier may be available under the policy.

Specific definitions associated with the crisis communications or crisis management insuring agreement include crisis event, crisis expenses, and crisis management firm. The concepts are intertwined.

Essentially, a crisis event is any event the company with the consent of the insurer believes has resulted in or is "reasonably likely to result in" an otherwise covered claim under this policy. This would include, for example, a covered computer attack or extortion threat. Assuming a crisis event has occurred, the next step is to hire an approved crisis management firm. A list of approved crisis management firms should be available from the carrier. At that point, any fee or expense consented to by the insurer of the approved crisis management firm which is incurred "solely for the purpose of restoring the confidence of your customers and investors in your computer system's security" is eligible for potential coverage under the policy. Maximum fee reimbursement may be as high as $50,000.

4.3 Exclusions

The exclusion section of a cyber insurance policy plays a key role in determining coverage under a claim. Once a reader gets through the insuring agreements providing the basic grant of coverage and the definition section of the policy which determines how the carrier has chosen to define key terms, coverage may still be limited or eliminated by way of one or more exclusions. In most jurisdictions, the insurer, not the insured, has the burden of proving the applicability of an exclusion.

There are four basic reasons why an exclusion may be included in the policy. One, the coverage issue may more properly be a subject matter of another insurance policy already available in the market or a clarification of types of financial loss that do not in the view of the carrier reasonably fall within the insuring agreements. Two, the exclusion may seek to clarify a risk that more properly should rest with the insured. (These would include the so-called "moral hazard" risks.) Three, risks may be excluded because they are seen as potentially so huge that no single insurer could afford to absorb them. Fourth, risks deemed inappropriate for coverage under the basic policy form but might

be open to negotiation for a particular account may also be excluded. It is for this fourth category that counsel should be especially attentive since there may be an opportunity to expand coverage otherwise not existing in the policy.

Examples of some exclusions by type:

1. Physical events such as fire, windstorm, bodily injury, etc.
   Violations under the securities laws, ERISA, or employment practices;
   Patent infringement and/or trade secrets;
   Prior notice, events or claims;
   Pollution.

2. Project planning;
   Foreign nationalization;
   Wear and tear;
   Fraud/Dishonesty;
   Contract;
   Insured v insured;
   Failure to maintain/upgrade security.

3. War, nuclear, terrorism.

4. Cyber-terrorism;
   Retroactive dates.

CAUTION: Applicants should be wary of some exclusions that are beginning to appear in the market. Some of the most restrictive are listed below:

1. Absolute disgruntled employee

This exclusion attempts to exclude most computer attacks brought by employees. Given that at least half of computer attacks are brought by insiders, this could exclude a considerable amount of coverage. Common phraseology includes excluding "any loss or damage resulting from an employee," or "any fraudulent, criminal or malicious conduct by an employee." This phrasing unfairly expands the more common exclusions in a cyber insurance policy for acts of directors, officers, or acts of employees with knowledge of directors or officers.

A similar phraseology that seemingly goes too far excludes "anyone who gains unauthorized access directly through either any computer, computer system or network of yours." This apparently also excludes third parties that access "your computer system."

2. Theft of client information

This exclusion attempts to exclude a fundamental risk facing companies, especially those that safeguard customer credit card, health, or financial information such as e-tailers, financial and healthcare companies. For example, regulations under HIPPA and GLB specifically require affected companies to establish and maintain technological and procedural safeguards against electronic theft of customer information. Common exclusion phraseology would exclude "failure to safeguard the confidentiality of or otherwise prevent from disclosure, any information or data, including electronic data, acquired or developed by you as a result of your e-business activities," or "loss resulting directly or indirectly from the processing of any confidential information including but not limited to trade secret information, computer programs or customer information."

3. Credit card activities

Similar to the theft of customer information exclusions, this exclusion attempts to exclude any loss arising from the insured's credit card activities such as claims brought by third parties arising from the electronic theft of customer credit card information. Common exclusion phraseology would exclude loss arising from "use or purported use of credit, debit, charge, access, convenience, customer identification or other cards," or loss arising from "unauthorized or fraudulent use of any credit, debit, charge or store card."

4. Non-monetary and/or punitive damages

This exclusion (which can sometimes be found in the definition section) narrows coverage to claims alleging "damages." This would exclude the payment of defense costs associated with a claim demanding injunctive relief or other type of non-monetary relief (a common demand in media claims.)

5. Territory

This exclusion (usually found in the conditions section) excludes claims brought in or alleging wrongful acts in a particular area of the world. The strongest exclusions exclude all U.S., or conversely, all non-U.S. jurisdictions. Given the global nature of the Internet, a cyber insurance policy should be as close to world-wide as possible.

6. Social engineering

A popular type of computer attack is initiated by the non-electronic theft of passwords or other authorized employee identification. This so called "social engineering" attack is an important coverage under the policy. Common phraseology of a social engineering exclusion might exclude attacks by "anyone who gains unauthorized access directly through the physical possession of any password or other security code."

4.4 Limits of Liability

A cyber insurance policy might have several limits of liability. For example, there may be a limit under each insuring agreement, or specified limits for certain types of coverage. In all cases, there will be an overall limit of liability that represents the maximum amount the insurer will pay for covered losses under the policy. Premiums can often be reduced by an insured accepting smaller limits of liability for those insuring agreements for which less coverage is needed. For example, an insured that has a limited amount of e-business revenue may be able to lower its premium by requesting a lower limit of liability for e-business interruption coverage and a higher limit of liability for the third party liability coverage. Some policies may also include a maximum limit for any single claim. Similarly, a policy might cap the amount the insurer will pay for every "hour of business interruption loss."

It is important to understand that an insurer's obligation to pay loss may cease before the limit of liability has been exhausted. For example, it is typical that violations of the insured's obligation to consent to a settlement or other extreme failure to cooperate may result in the carrier no longer having an obligation to pay loss for a given claim.

Finally, with respect to the third party coverage, like other professional liability type policies, the costs of defense are included within the limit of liability. It is therefore in the insured's best interest to ensure that only necessary and reasonable costs, charges, and expenses of defense are incurred, as amounts expended on defense reduce the available pot for any potential settlement or judgment.

4.5 Retentions and Waiting Periods

Retentions, whether taking the form of time or money, are used to better share the risk between the insured and the insurer. Before the insurer must pay loss, the amount of the applicable retention must be exhausted. Because this is meant to encourage the insured to take responsibility for managing its cyber risk, the retention must usually be borne by the insured and therefore is not insured. Retentions are usually applied per claim or loss.

With respect to the third party coverages and first party property coverage under the policy, the retention amount is simply the amount of dollar loss that the policy would otherwise cover that must be incurred and paid by the insured before the insurer pays. With respect to business interruption coverage, the policy might have both a dollar retention and a waiting period retention. A common version of this concept applies the greater of the dollar retention or the amount of loss incurred under the waiting period retention. For example, an insured that suffers a DOS attack, causing it to go down for 15 hours and suffering $1.5 million in business interruption loss spread evenly over the 15 hours, that has a policy with a $250,000/12 hour retention, would determine its covered loss as follows:

> Retention = Greater of $250,000 or $1.2 million (12 hours times $100,000 per hour). Covered loss is $300,000.

Caution: If the policy also has a "per hour" business interruption maximum limit (see, 4.4, *supra*) of $10,000 per hour, coverage under the policy might be limited to $30,000 (15hrs – 12hrs x $10,000).

The insurer has no obligation to pay any loss within the applicable retention. If it decides to do so, the insured must immediately reimburse the insurer. The flip side of this is a useful provision in some policies permitting the insured to settle any claim where the total amount of loss falls within the retention. The sample policy states this concept as follows:

> You may settle any claim or suit to which this insurance applies provided that you do so (i) on behalf of all insureds, and (ii) without incurring loss in excess of any and all applicable Retentions.

4.6 General Conditions

The general conditions of a policy sets forth various other responsibilities and rights of the parties. A typical policy might contain the following provisions in this part of the policy:

- Claim Reporting
- Cooperation and Association
- Territory
- Dispute Resolution
- Other insurance
- Cancellation
- Extending Reporting Periods or Discovery
- Notice of Circumstances
- Organization Changes

The first two provisions will be considered in the next section. As to the others, please note the following:

Territory: As previously mentioned, a cyber insurance policy should be as worldwide as possible both with respect to where claims are brought as well as where loss or wrongful acts occur.

Dispute Resolution: Despite the best of intentions by both parties, there may be occasions of disagreement between the insured and the insurer as to coverage. Whenever possible, the resolution of such disputes should occur in a business atmosphere with the avoidance of litigation. Cyber policies will frequently have a dispute resolution provision or provisions that might suggest or require alternative dispute resolution forums ("ADR"). Sample language may be as follows:

> Any controversy arising out of or relating to this policy or its breach shall first be submitted to alternative dispute resolution ("ADR") in accordance with the rules of the American Arbitration Association or the Defense Research Institute. The ADR shall be held in New York, New York unless otherwise agreed to by both parties. Each party shall jointly and equally bear with the other party the expense of the alternative dispute resolution. Either we or you may elect the type of ADR, either non-binding mediation or binding arbitration.

Other Insurance: Standard language might state that the policy is "excess of any other valid and collectible insurance." It is important that the provision states both valid AND collectible to avoid the insurance being excess of uncollectible insurance of insurers, for example, in receivership. Beyond this, a carrier might be willing to amend the provision to specifically state that the cyber insurance policy is meant to be the primary insurance policy for cyber-risks. On the other hand, a carrier might also be willing to state that the policy is "excess and difference-in-conditions" ("DIC") over scheduled other insurance policies the insured might have. While the "excess/DIC" position may reduce premium since the carrier might believe that other insurance policies may end up paying first, it can cause difficulties in claim situations where the insured (or other insurance carrier) and the cyber-insurer disagree as to whether the non-cyber policy covers the claim. For this reason, the "excess/DIC" modification, while seemingly attractive, might be well avoided.

Cancellation: Typically a cyber insurance policy will permit cancellation by either the insurer or the insured. This ability is not equal with the insured having the ability to cancel at any time for any reason. The insurer usually contractually requires itself to give a period of notice to the insured ranging from as little as 30 days to as much as 90 days before the cancellation can take affect. In addition, the insurer's ability to cancel may be limited by applicable state law, which many times also specifies the reasons why an insurer may cancel a policy. Note that notice periods for cancellations for

non-payments are usually very short, such as ten days. Assuming the cancellation was not made for nonpayment, a return premium for the "unearned" portion of the policy will be owed to the insured. The definition of "unearned" will differ depending upon the party who cancelled the policy.

Extended Reporting Period: Also sometimes known as the "Discovery" clause, the extended reporting provision ("ERP") is a provision that grew out of the "claims made" feature of an insurance policy. This provision grew out of fears that insurers, if they thought a bad claim was about to be made against the insured, would suddenly cancel a claims-made insurance policy, thereby avoiding a covered claim moments before it was made. The extended reporting provision was created to permit the insured, facing such a problem, to automatically buy or be entitled to a free "extended reporting" time to report claims made after the cancellation of the policy alleging wrongful acts occurring before the cancellation. As a result of the "soft market," ERP clauses were typically expanded beyond this original purpose and today, ERP clauses might apply to non-renewals as well as cancellations regardless of who cancels/non-renews. ERP clauses offer reporting periods as much as three years after the policy ends, although six months/1 year is more usual. The sample policy gives a free 90-day extended reporting period followed by a fee-based period of up to three years.

4.7 Endorsements

Terms, conditions, and exclusions of insurance sometimes may be modified for a particular account as a result of an individual negotiation between the parties. As previously discussed, one of the characteristics a potential insurance applicant should look for in an insurance carrier is flexibility and expertise. Of course, certain terms cannot be changed either because they are legally mandated or because to do so would so shift the exposure to the carrier as to make the contract unprofitable. As indicated in section 4.3, certain exclusions, such as cyber-terrorism, might be modifiable by endorsement. Some states might also require the carrier to add one or more endorsements to its policy as a condition of the state approving the policy for "admitted" use. These state modifications usually impact the cancellation/non-renewal and ERP provisions, but might also affect other provisions such as dispute resolution.

5 Claims Handling and Coverage Issues

An important part of the policy, as well as the overall insured-insurer relationship, is the rights and obligations of the parties when it comes to a claim or loss. Provisions impacting this will include whether the carrier has or does not have a duty to defend, whether defense is included in the limit, claim reporting provisions, cooperation and assistance provisions, whether the insured has the right to submit non-claim incidents and, finally, provisions relating to settlement. With respect to first party coverages, provisions relating to proof of loss and valuation come into play.

5.1 Claims and Incidents

All third party liability policies will permit, indeed, require the insured to submit to the insurer a claim against an insured for which coverage is sought. However, most claims-made contracts will also permit the submission of a "notice of circumstances," which is a useful provision since it allows an insured, who is concerned that an incident which has occurred might lead to a claim, to anchor coverage even though no claim has been yet made. If a claim is made in the future, even after the policy expires, the policy in effect when the notice of circumstances was submitted is triggered. However, some policies may actually require that the insured submit all circumstances that it believes might lead to a claim. Be very careful of this type of provision, since failure to do so (or what is perceived by the carrier as a failure) may result in coverage being denied for the claim if it is later made.

5.2 Notice Provisions

Notice provisions of a cyber insurance policy usually require that the insured report a claim as soon as practicable after it is made. Claims made sections also require that the claim be reported during the policy period or extended reporting period. With respect to coverage under the first party sections of the policy, a similar rule applies requiring the reporting of a loss or a failure of security. In cases of a computer attack, the policy may also require the insured to report the incident to the appropriate law enforcement agency. Finally, with respect to first party coverages, the insured must submit a "proof of loss" during the required time, usually 90 days after the loss occurs or is discovered. (A "discovery" rule is preferred for obvious reasons.)

5.3. Potential Claims and Incidents

As mentioned earlier, due to the fear that a carrier would "jump ship" when it believed that a claim would soon be made against an insured under a claims-made policy format, these types of policies historically permitted insureds to submit incidents or events which has not yet resulted in a claim but may do so in the future. The value of this type of provision is to anchor coverage in the policy in existence at the time of the notice regardless of whether the insured or the insurer chooses to continue coverage at the end of the policy period.

CAUTION: THESE PROVISIONS SHOULD BE WRITTEN SO AS TO PERMIT BUT NOT REQUIRE INSUREDS TO SUBMIT NON-CLAIMS INCIDENTS.

5.4 Valuation

Valuation under a cyber insurance policy usually refers to the amount of "loss" under the first party coverages. Of course, loss must also be valued under the third party components but here this usually refers to the reasonableness of a potential settlement offer or the reasonableness of defense costs expenses. These items are dealt with in sections 5.6 and 5.7 of this chapter.

With respect to first party loss, valuation of trade secrets has been discussed earlier. When done properly, this would be on a "stated value" basis, i.e. the parties would agree in advance of the inception date of the policy what the insured trade secrets are and what their value is if destroyed or stolen. With respect to business interruption coverage, the valuation is made pursuant to the definition of business interruption discussed in section 4.2.7. Finally, with respect to loss arising out of the damage, destruction or corruption of data, value is considered to be the costs associated with replacing or recollecting that data pursuant to the definition of loss discussed in section 4.2.6.

Nevertheless there are circumstances where both parties, despite their best intentions, might disagree on the valuation placed on a first party loss. To manage such circumstances, a properly written cyber insurance policy will insert an appraisal provision whose goal is to create an efficient objective procedure to determine the value of the item disputed. The sample policy is, again, instructive on the proper language to be used:

> Under coverage E, you and we each have the right to demand that the amount of loss be determined by appraisal. If either you or we make a written demand for appraisal, each will select a competent independent appraiser and notify the other of the appraiser's identity within 20 days of the receipt of the written demand. The two appraisers will then select a competent, impartial umpire. The appraisers will then determine and state separately the amount of each loss. If the appraisers submit a written report and there is an agreement to use the same, the amount agreed upon will be the amount of the loss. If the appraisers fail to agree, within a reasonable time, they will submit only their differences to the umpire. Written agreement so itemized and signed by any two of these three sets the amount of the loss. Each appraiser will be paid by the party selecting the appraiser. Other expenses of the appraisal and the compensation of the umpire will be paid equally by you and us. If there is an appraisal, we will still retain our right to deny coverage.

5.5 Duties Under the Policy

As is the case with any contract, both parties have rights and obligations. These rights and obligations can appear in various parts of the policy such as:

1. Notice and Cooperation

2. Defense provisions

3. Dispute Resolution and Settlement

Defense, Dispute Resolution and Settlement is discussed in the following two sections. This section will discuss the first item of the above list: Notice and Cooperation.

So that the insurer may be in a reasonable position in terms of understanding, defending, settling and valuing loss under the policy, the insured must assist and cooperate with the insurer with respect to claims. In addition, the insured is expected to be an active participant in the application process and to be forthcoming with all information that an insurer may reasonably need to know in order to make a decision to offer coverage and to decide on what terms to offer.

With respect to a claim or loss, these obligations usually include the obligation to assist in:

1. any investigation of a claim, loss, or circumstance (including submission to an examination by the insurer or their designee, under oath if required);

2. making settlements;

3. enforcing any legal rights that the insurer or insured may have against anyone who may be liable to the insured;

4. attending depositions, hearings and trials;

5. securing and giving evidence, and obtaining the attendance of witnesses;

6. any inspection or survey conducted by the insurer pursuant to this policy; and

7. any investigation of any extortion claim, payment of any extortion monies that the insurer deems to be reasonable and necessary to terminate or end the extortion claim and subsequent attempts, if any, by the insurer to recover part or all of such extortion monies.

5.6 Defense Counsel Issues

In section 4.1, it was noted that defense provisions are part of the insuring agreements in a cyber insurance policy. Defense counsel issues generally only relate to the third party coverages under the policy. Cyber insurance policies are usually written on a "duty to defend" basis. Most insureds find this to be a positive feature since the law generally states that an insurer's duty to defend a claim is broader than its duty to indemnify. Put another way, an insurer has the obligation to defend claims even though the allegations are fraudulent, groundless or otherwise without merit. In addition, in many jurisdictions the insurer may have an obligation to defend all allegations in a complaint even if there is only a single allegation that might be covered under the policy.

A potentially thorny issue arising from the obligation of an insurer to hire and pay (excess of the retention) counsel to defend a claim is when there is a disagreement as to the quality or cost of the counsel, especially when expenses are expected to fall within a self-insured retention or when the carrier is operating under a "reservation of rights" letter. A reservation of rights letter is one that indicates that coverage under the policy may not exist for the claim, in part or in whole, but that the insurer will continue to defend the claim until such time, if any, that the non-coverage position can be determined. It is important to understand that this limbo land is not due to the fault of the insurer, but rather usually arises from the fact that certain allegations in the complaint drafted by the plaintiff counsel may trigger coverage issues. For example, a claim might allege both negligent and fraudulent conduct, the latter of which, if shown, might trigger an exclusion under the policy. Even without such allegations, however, insureds may rightly wish before agreeing to the insurance to know of the quality of the law firms the insurer will hire in the event of a claim made against them.

On the positive side, issues as to the quality and cost of defense counsel gives reputable carriers the opportunity to brag about these aspects of their program for which they should be proud.

Accordingly, it is in the best interest of both the insured and the insurer for:

1. Insureds to ask for a list of law firms from which the insurer will choose defense counsel in the event of a claim;

2. Insureds to have an opportunity to interview the law firms and make non-binding recommendations as to which of the listed firms they would prefer;

3. Insurers to negotiate rates that are appropriate for the type and sophistication of the work that needs to be done.

5.7 Settlement

It is in the best interest of both insureds and the insurer to quickly and efficiently settle a claim when such settlement is necessary to avoid higher costs of litigation including future defense expenses or judgments. While it is easy to agree with the preceding sentence in theory, applying it to a given case is more difficult. At times, insurers may wish to settle a claim to which the insured does not wish to settle. At other times, an insured may be anxious to settle a claim to which the insurer does not wish to settle. The amount and impact of any self-insured retention may also play a role.

In general, here are the rules of the game. An insurer who fails to accept a reasonable offer within the policy limits can sometimes be held liable for damages in excess of the policy. Of course, this assumes that the insured has fulfilled its obligations under the policy as well, especially with respect to cooperation and assistance during the claim. And, of course, this assumes the claim is covered under the policy and that there are no other circumstances that would justify an insurer rejecting a settlement demand.

On the flip side, generally, insureds may not refuse to consent to a settlement on which both the insurer and the plaintiff agree. If they do so, the claim must be defended by the insured on an on-going basis and in the event that loss is in excess of the amount which the insurer could have settled the claim (plus defense costs up until that point), the excess becomes the financial responsibility of the insured.

In the event there is a disagreement between the insured and the insurer as to whether to settle a claim or as to whether a proposed settlement is covered under the policy, quality policies will have a Dispute Resolution clause. These clauses can be written in several different ways. The sample policy includes typical language, as follows:

> Any controversy arising out of or relating to this policy or its breach shall first be submitted to alternative dispute resolution ("ADR") in accordance with the rules of the American Arbitration Association or the Defense Research Institute. The ADR shall be held in New York, New York unless otherwise agreed to by both parties. Each party shall jointly and equally bear with the other party the expense of the alternative dispute resolution. Either we or you may elect the type of ADR, either non-binding mediation or binding arbitration.

6 Hypothetical Case

Widget Incorporated sold defense parts to the military. However, since the end of the cold war, the company developed a significant business unit selling military toys. Today, Widget's toy division accounts for most of the company's revenue and most of that revenue comes from selling toys on-line during the Christmas season. Several weeks before Christmas, Widgets Incorporated's CEO was emailed

a warning message from a self-claimed "hactivist". The hackivist indicated opposition to Widget's funding to the military in its fight against terrorism. The hackivist indicated that he had attacked Widget's computer system and stolen 100,000 credit card numbers from Widget's database. If the CEO would kindly deposit $50,000 into a specified swiss bank account, the hackivist would destroy the credit card numbers and tell Widget's chief technology officer how the hack was accomplished. However, if the CEO does not pay the "consulting fee" requested, the hackivist would publicize the credit card numbers on the web and also launch a "denial-of-service" attack against Widget causing its computer system and web site to shut down. Widget gets 50% of its income during the Christmas season and almost 40% of that revenue comes from purchases made on the web. All in all, Widget expected to receive $10M in on-line revenue between the date of the email and December 26th.

Despite the potential loss of revenue, Widget's CEO decided not to give in. Three days later, Widget's computer systems and internet site suffered a distributed denial-of-service attack and was shut down. Also 25,000 of Widget's customers' credit card numbers were publicized on the web. After a week, Widget was able to get its web site running again. However, by then the fact of the attack and exposure of credit card numbers chilled customers from buying their Christmas toys. Plus, Widget's general counsel reports lawsuits by the credit card issuers (who spent approximately $150 per card to reissue), a class action by credit card holders who paid up to $50 of the fraudulent charges and several merchants who suffered financial loss after accepting the stolen credit card numbers.

According to Widget's CFO, Widget suffered the following financial losses:

1. Cost to investigate extortion threat: $10,000

2. Cost to retrieve damaged data: $50,000

3 Cost of lost on-line revenue during week shutdown: $700,000

4 Cost of lost on-line revenue after site recovery: $60,000 per week (12 weeks)

5. Defense expenses of three lawsuits: $30,000 per week (52 weeks of litigation before settlement)

6. Expected settlement of three lawsuits: $2,500,000

7. Cost of outside PR agent after crisis: $25,000

7 Coverage of Hypothetical Case

Widget Incorporated suffered at least five types of financial loss in our hypothetical: Extortion expenses, Property (data) damage, eRevenue Business Interruption, Third Party litigation costs (defense and settlement) and public relations expenses.

Subject to the specific terms, conditions and exclusions of the policy, all of these financial losses would be covered under a quality cyber-insurance policy.

If Widget had a cyber-insurance policy, the carrier might well hire an expert cyber-extortionist investigator to determine the level of the hackivists's threat and the potential financial loss to Widget if the threat went unanswered. By the relatively low cost of Widget's cyber-investigation, this was probably not done. One potential outcome of such an investigation might have been the payment of the extortion demand followed by the posting of a criminal reward for the cyber-criminal's eventual capture and imprisonment. It is likely that the costs associated with this resolution would have been much lower that the financial costs Widget ended up suffering.

The first party component of the policy would generally cover both the costs of restoring the damaged data ($50,000) as well as the lost revenue during the week that the Widget's web site was down due to the denial-of-service attack ($700,000) assuming that Widget could not have reasonably gotten its site up in a shorter period. The policy will also cover the future lost of revenue ($60,000 per week) up to the period of the "extended period of recovery" which is up to 90 days in a quality policy. Please note that the carrier would not pay those amounts incurred during the policy's "waiting period retention", a period of between 12 to 48 hours depending upon the policy. (Thus if Widget's $700,000 loss was spread evenly over the week, the first $50,000 to $200,000 would be the responsible of the insured.)

Assuming that the claims were properly reported and the other terms and conditions of the policy were satisfied, the policy would respond to the three lawsuits, hiring counsel, paying legal expenses as well as any settlement or judgment. Again, loss would be paid excess of the applicable retention. Total litigation cost if all three claims were settled after a year of litigation: $4,060,000.

Finally, a quality cyber-insurance policy would also recommend a public relations firm for Widget paying the $25,000 public relations fee.

Total Policy Payments: $5,000,000 plus.

Coverage would, of course, be dependent upon the terms, conditions and exclusions of the policy. One interesting exclusion potentially triggered by the facts of our hypothetical is the war/terrorism exclusion. Under the facts presented, an insurer might be able to argue that the attack

was done as part of or in response to the war on terrorism. Conversely, the insured might argue that despite the reference in the email by the "hackivist" that he is acting in defense of terrorists, the fact that he would go away for a payment of $50,000 means that the attack was in reality a simple cyber-crime for profit. It is for this reason, that insureds are best served by a cyber-policy with expressed cyber-terrorism coverage even if such coverage increased the overall cost of the policy.

8 Conclusion

Today, every company is using the Internet in some way as part of its business strategy whether for communication (email), marketing (web presence), professional services or full e-commerce. Such activities result in new and largely untested exposures. Financial loss arising from such exposures include both first party loss from damage to data or loss of eRevenue, due to a computer attack, as well as third party expenses of claims alleging web content liability, professional service errors and omissions and network security liability.

Neither technology nor insurance alone can sufficiently respond to these potential losses. Rather a total Risk Management Approach must be implemented combining best in class technology and insurance. Traditional insurance policies written for a world of tangible property and traditional litigation theories is inadequate to provide coverage for e-risks.

In evaluating potential insurance solutions, the first step is to evaluate a potential insurer. A number of characteristics should be examined including expertise, experience, financial strength and global reach.

A cyber-insurance program should contain free security assessments, six kinds of insurance coverage and three post-incident support funds. Coverages should include both first party damage to data and loss of eRevenue, as well as third party coverages for web content, professional E&O and network security. Since there is no standard form for this type of insurance, each carrier's form must be carefully examined.

9 Checklist of Main Points

- Frequency and Severity of computer attacks and other cyber-risks is increasing at a dramatic pace.
- To handle such exposures companies must adopt a total Risk Management Approach combining technology and insurance operating under a "cycle of risk management": Assessment, Mitigation, Insurance, Detection, Remediation, Reassessment as discussed in chapter 1.

- Traditional insurance policies like Comprehensive General Liability and Property are inadequate when it comes to covering cyber-risks.

- The choice of insurance carrier is critical. Characteristics to look for include: a 2 year track record as a dedicated unit composed of underwriters, claims, legal and technology professionals as well as a triple-A financial rating, $25 million of limits capacity, superior loss prevention services, global presence, and robust policy form.

- Loss prevention services available from the cyber-insurance carrier should include free on-line security assessments, premium discounts for the purchase of supported technology products and services and either low cost or free on-site assessments regardless of whether an insurance purchase is made.

- Cyber insurance policies vary widely among insurers as the market is still relatively young. Because of this variance, special care is required in reviewing terms and conditions. A quality cyber insurance policy will offer:

  - Six insuring agreements: Web Content, Professional E&O and Network Security legal liability, Cyber-extortion, First Party Data/Property and eRevenue Business Interruption.
  - Broad definitions including those of: “claim” (to include non-monetary damage), “loss” (to include punitive damages), “wrongful act” (to include non-negligent acts), “insured”, “computer attack” (to include acts regardless of motive or intent and regardless of whether launched by an employee or outsider), “business interruption” (to include net loss situations).
  - No automatic exclusion for theft of company or customer information.
  - No automatic exclusion for credit card operations.
  - No automatic exclusion for losses caused by insiders.
  - Some “social engineering” loss coverage.
  - Either no hourly sublimit or a high hourly sublimit for eRevenue business interruption
  - Availability to submit “notices of circumstances” as a pre-claim notice to the carrier.
  - A extended reporting provision or discovery clause for claims coverage.
  - A dispute resolution procedure, preferably with a choice of options.