CYBER LIABILITY: UNDERSTANDING TECHNOLOGY LOSSES IN AN AGE OF E-COMMERCE

Suzanne C. Midlige, Esq.
William J. Hoffman, Esq.

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NEW JERSEY 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 5TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

COUGHLIN DUFFY LLP

TABLE OF CONTENTS

I. INTRODUCTION AND BACKGROUND

A. *The Emergence of Cyber Risks*

In today's digital world, where electronic transactions are processed with lightning speed and where companies both large and small typically maintain confidential or proprietary data in electronic format, both the inadvertent loss of data and the theft of data by a new breed of thief -- the cyber-criminal -- pose an ever-increasing risk for unwary businesses. Just ask one of America's largest retail conglomerates, The TJX Companies, Inc. ("TJX"), parent company of TJ Maxx, Marshalls and several other discount retailers operating in the United States and abroad.

Over an 18-month period between July 2005 and December 2006, sophisticated computer hackers stole approximately 46 million credit and debit card numbers belonging to TJX customers in the United States, Canada and Puerto Rico. *See* Joseph Pereira, *Breaking the Code: How Credit Card Data Went Out Wireless Door*, The Wall Street Journal (May 4, 2007). Other estimates have put the number as high as 200 million card numbers stolen from four years' worth of electronic data. *Id.* To make matters even worse, the hackers also stole the social security numbers, military identification numbers and driver's license numbers of approximately 450,000 TJX customers -- the type of information that is a veritable goldmine for identity thieves. *Id.*

TJX has been hit with several consumer class action lawsuits as a result of the breach of its computer network, as well as various investigations from state attorneys' general and a Congressional inquiry. As part of a proposed class action settlement recently announced in late September, TJX has agreed to, among other things, pay the cost of three years' worth of credit monitoring and identity theft insurance to the 450,000

or so customers whose personal information is believed to have been stolen. *See* TJX Settlement Filing (September 22, 2007).[1] While the specific cost of credit monitoring is not set forth in the proposed agreement, the ultimate cost to TJX could be quite significant. Assuming, for example, that the cost of three years of credit monitoring amounts to $300 per person, the cost to TJX would be $67,500,000 if only *half* of the 450,000 individual consumers had their credit reports monitored for fraudulent activity.[2]

That cost is in addition to the $6.5 million in legal fees TJX has agreed to pay to plaintiffs' class counsel, the $30 store vouchers it has agreed to provide to customers who made non-cash purchases during the relevant period, as well as other significant costs the company will incur under the terms of the proposed settlement. *Id.* In its earnings report for the second quarter of 2007, TJX took a $118 million after-tax charge for the quarter to cover current and potential costs arising from the theft, and may record an additional $21 million in non-cash charges in the future. *See* Walaika Haskins, *TJX Asked Too Much, Protected Too Little, Say Canadian Officials*, CRMBuyer (September 26, 2007) available online at http://www.ectnews.com. In addition, estimates are that TJX will spend an estimated total of $125 million on network security improvements as a result of the breach. *Id.*

TJX's experience is not unique, however. Choice Point, Inc. ("Choice Point"), a consumer data broker, experienced a security breach in 2005 that affected more than 140,000 people in all fifty states. Mary J. Hildebrand and Jacqueline Klosek, *Recent Security Breaches Highlight the Important Role of Data Security in Privacy Compliance*

[1] The TJX settlement filing is available online at http://storefrontbacktalk.com/story/092207TJXfiling.php.
[2] Based on our own online research, we estimate the cost of one year's worth of credit monitoring for an individual to cost $150. Using that figure, three years' worth of credit monitoring would amount to $450 per person. In our example above, we used an even lower estimate of $300 per person.

Programs, 17 NO. 5 Intell. Prop. & Tech. L.J. 20 (2005). In order to resolve a suit brought by the Federal Trade Commission, Choice Point agreed to pay $10 million in civil penalties and another $5 million in consumer redress. *See* Warren Agin, *Information Security Law*, 26-3 ABIJ 54 (April 2007). Other corporate victims of lost or stolen data include Bank of America, which lost the personal information, including names and social security numbers, of approximately 1.2 million federal employees; DSW Shoe Warehouse, a retailer from whom 1.4 million credit card numbers were stolen; and TD Ameritrade, an online brokerage from whom cyber-criminals stole the personal information of approximately 6.3 million customers. These are but a few examples of the many companies that have experienced significant cyber-risk losses in recent years, whether as a result of theft, accident or their own inadvertence or carelessness.

In another noteworthy matter, Fidelity Federal Bank and Trust ("Fidelity"), a West Palm Beach-based bank, settled a class action lawsuit brought by Florida motorists for an estimated $50 million, including $10 million in attorneys' fees to plaintiffs' counsel. *See* Jeff Ostrowski, *Tens of Thousands of South Florida Drivers to Get $160 Checks*, Palm Beach Post (December 8, 2006). Fidelity allegedly violated federal anti-stalking legislation, which prohibits companies from buying driver records from state governments, when it purchased the records of approximately 565,000 Florida drivers between 2000 and 2003. *Id.* Fidelity reportedly purchased the information for a penny a name from the Florida Department of Highway Safety and Motor Vehicles, and then used the information to mail out brochures advertising its auto loans. *Id.* The plaintiffs involved in the settlement will each receive $160. *Id.*

It is evident that the recent advances in technology that have driven the growth of e-commerce have also resulted in unforeseen potential liabilities for businesses. Whether through a lack of foresight, a failure to understand and appreciate the potential perils of new technology or, perhaps, an underestimation of the determination of cyber-criminals to gain access to confidential data, many companies have left themselves uninsured against potential losses arising out of the storage of electronic data. Recognizing and acknowledging the presence of those perils will enable a company to protect itself from losses that may arise out of new technologies.

Insurance is one of the most common devices utilized by businesses to safeguard against catastrophic losses. Traditional insurance policies, however, were not designed to protect against the cyber-risks. As a result, many businesses that have, until now, relied solely or primarily on their comprehensive general liability ("CGL") policies will likely find themselves unprotected against the risks presented by many new technologies.

This paper will present an overview of certain technological advancements and the risks those advancements pose to businesses. We will also address the insurance coverage issues presented by so-called "cyber-risks" under a CGL policy and why businesses facing cyber-risk liabilities may find themselves without insurance protection. Moreover, we will discuss cyber-risks from an underwriting and risk management perspective, providing an overview of what may be done to protect against such risks.

While the trials and tribulations of companies such as TJX and other businesses that have fallen victim to lost or stolen data are noteworthy and have been the subject of significant media attention, they do not represent the only examples of cyber-risks that may befall a business in the digital age. For example, a business might inadvertently

post copyrighted content on its website, leading to claims of copyright infringement, or host a chatroom or bulletin board on which, if not monitored vigilantly, potentially defamatory or private information may be posted, resulting in claims for defamation or invasion of privacy. In another scenario, an internet worm or computer virus might shutdown or paralyze a company's computer network or website, resulting in lost sales or a shut-down in operations until the problem is corrected. Moreover, a ripple effect may be felt by other businesses that, for example, may rely on another company's network or website for the placement of orders.

For purposes of the present discussion, we will focus on two potential cyber-risks faced by any business that has a computer network or engages in e-commerce over the internet: lost or stolen data.

B. ***Storage of consumer data as a "cyber-risk"***

For years, large corporations have collected and stored a wide range of consumer information to assist in marketing and sales efforts. Quite often, that information consists of sensitive personal and financial data of consumers, including credit card numbers and, in the United States, social security numbers and other personal, identifying information. New technologies have dramatically decreased the cost of collecting consumer data and storing it electronically. Because of the decreased cost of storage, and the miniaturization of memory devices and their ease of use, many smaller businesses are now utilizing the same tools as some larger companies in the gathering and storing of consumer data.

As demonstrated by the incident involving TJX, the costs of data security breaches are potentially astronomical, and may include the costs of: government and regulatory investigations, government fines or penalties, court orders, injunctive relief,

consumer class action litigation, vendor litigation, damaged business reputation, customer loss, loss of goodwill, shareholder suits and internal investigation costs. *See* John F. Delaney, *Privacy, Data Security, and Outsourcing the Regulatory Framework*, 8444 PLI/Pat 611, 617 (October 24, 2005). A company may even find itself the victim of data extortion after a network security breach, wherein a cyber-criminal holds the stolen data for "ransom." It is also not uncommon for businesses to incur costs on expensive public relations campaigns after a breach in order to improve its public image.

What's more, in light of recently enacted data notification laws, businesses may be required, at their own cost, to notify each and every individual whose personal information may have been lost or stolen. Accordingly, a business can also expect losses and claims that include the cost of notifying the public and individual customers that their personal information or credit card numbers have been stolen and even the cost of paying for credit monitoring on behalf of customers in order to safeguard against identity theft.

C. Storage of a company's own proprietary or essential business information as a "cyber-risk"

In addition to the perils posed by the loss of consumer data and other third-party information, businesses must also act to safeguard their own proprietary business information and other forms of electronic data that are essential to keep their business running smoothly and seamlessly. This can include not only such things as customer lists, project designs and other forms of "intellectual property," but also the computer programs on which business operations run, including accounting software, inventory-tracking software, and the software and programming required to keep assembly lines functioning and e-commerce websites on-line.

D. *Data Notification Laws*

A series of high-profile data breaches in the first half of 2005 prompted U.S. lawmakers to introduce more than a half-dozen bills that would require companies to notify consumers affected by security breaches. David Bank, *Breaches of Customers' Data Trigger Lawsuits*, The Wall Street Journal (July 21, 2005). "Some of the bills have exceptions for encrypted data, and some require companies to report breaches only when they determine there's significant risk to customers." Grant Gross, *2006 in Congress: 'Full Plate' for Tech, Telecom* (December 27, 2005), available online at http://www.itnetcentral.com/article.asp?id=15395&leveli=0&info=home. What some commentators, business leaders and lobbyists have referred to as a "patchwork quilt" of state laws has lead to calls for a national data breach law that preempts state laws. Grant Gross, *Data Breach Bills Unlikely to Pass before 2006* (November 11, 2005), available online at http://www.infoworld.com/article/05/11/11/HNdatabreachbill_1.html. Federal legislation dealing with data breach notification has been introduced in both the House of Representatives and in the Senate, and would require businesses and other organizations to disclose data breaches that result in the loss of consumers' personal information. *See* Brian Krebs, *Data Breaches Spur Congressional Action, Federal Notification Law Would Trump State Measures* (July 18, 2005), available online at http://www.washingtonpost.com/wpdyn/content/article/2005/07/18/AR2005071800613.html. The main objectives of the proposed bills are:

1. Greater protection of and control over the use of key personal data such as Social Security numbers and financial account information;
2. Increased penalties for breaches and facilitating identity theft; and

3. A nationwide standard for notifying consumers when their personal information has been breached. *See* Jeanne Sahadi, *Breaches: Federal Law on the Way? Lawmakers have Proposed Several Bills that Seek to Better Protect Personal Data*, (July 7, 2005), available online at http://money.cnn.com/2005/07/06/pf/security_bills/.

While those bills remain pending before Congress, legislation has already been enacted requiring certain business to properly protect consumer/client data. The Federal Financial Modernization Act, commonly know as Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801 *et seq*., was passed by Congress and signed by President Clinton in November, 1999. The GLBA states, "[i]t is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those consumers' non-public information." 15 U.S.C. § 6801. Section 501(b) of the GLBA mandates that financial institutions develop and implement administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information. Put simply, it requires financial institutions to prevent unauthorized access to non-public, personal information.

The Health Insurance Portability and Accountability Act ("HIPPA") , 42 U.S.C.. § 1320(d) *et seq*., and The Sarbanes-Oxley Act of 2002 ("SOX"), 15 U.S.C. § 7201 *et seq*., are two other federal laws that also mandate that electronically stored consumer/client information be adequately protected.

As mentioned, a number of states (at least 35) have enacted or introduced legislation regarding customer notification of security breaches that result in the

unauthorized release of personal consumer information. California was the first state to enact legislation governing the disclosure and notification of data security breaches to effected consumers. Many states have followed suit, modeling their notification laws after California's. Generally, the legislation requires companies "to notify consumers regarding breach of security in which certain personal information relating to those consumers was, or is reasonably believed to have been, acquired by an unauthorized person." Thomas E. Scanlon, *Overview of Recent State Laws Requiring Notification of Security Breach*, 6 NO. 3 Privacy & Info. L. Rep. 6 (Nov. 2005). Each state's data notification statute, however, is not identical, containing its own nuances.

California's Database Security Breach Notification Act, codified at Cal. Civ. Code § 1798.82 and § 1798.29, and General Security Standard for Businesses, codified at Cal. Civ. Code § 1798.81.5**,** requires companies and government agencies that store personal information on California residents to implement safety procedures that safeguard data and disclose any breach of security to the individuals affected. Cal. Civ. Code § 1798.82 (a) affects any state agency, business, or person that conducts business in California and maintains computerized data that includes personal information. Cal. Civ. Code § 1798.82 (b) states that any breach of the security of the data must be reported in the most expedient manner following the discovery of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Cal. Civ. Code § 1798.82 (e) defines personal information as an individual's last name and first name or initial, in combination with a Social Security number; driver's license or California ID Card number; or account, debit card or credit card number, in combination with any security code, access code or

password that would permit access to the account. Cal. Civ. Code § 1798.82 (g) provides that:

> ‘‘[N]otice’’ may be provided by one of the following methods:
>
> (1) Written notice.
>
> (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
>
> (3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
>
> (A) E-mail notice when the agency has an e-mail address for the subject persons.
>
> (B) Conspicuous posting of the notice on the agency’s Web site page, if the agency maintains one.
>
> (C) Notification to major statewide media.

Failure to promptly notify the information owner or licensee of the data makes the organization liable for civil damages. “The law allows any customer who is injured by a violation of [Cal. Civ. Code § 1798.82] to institute a civil action to recover damages.” Francoise Gilbert, *Information Privacy and Security in California*, 1 NO. ABA SciTech Law. 8 (Fall, 2004). Thus, a company that fails to comply with the notification provisions of Cal. Civ. Code § 1798.82 may face legal action from consumers and, also, from the California Attorney General.

The General Security Standard for Businesses, Cal. Civ. Code § 1798.81, requires that businesses owning or licensing such personal information about a California resident, when held in unencrypted form, implement and maintain reasonable security procedures and practices to protect the personal information from unauthorized access,

use, modification, destruction, or disclosure. California's Database Security Breach Notification Act and General Security Standard for Businesses should have a significant impact on business practices with respect to the protection of electronic data gathered and stored because of the potential for severe penalties. These penalties can be inflicted through class action lawsuits and other penalties and fines that may be levied against the organization for negligence in exercising an inadequate standard of care in protecting the information. In addition, companies face possible additional costs attributable to security breaches, including damage to image, reputation and brand resulting from public awareness of and perception of security breaches, the cost of notifying data owners and the cost of defending lawsuits brought against the company.

Florida passed H.B. 481**,** Fla. Stat. Ann. § 817.568 *et seq*., effective July 1, 2005. Fla. Stat. Ann. § 817.5681(1)(a) provides that "[a] person who conducts business in this state and maintains computerized data in a system that includes personal information provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." There is a forty-five day grace period for notification after the security breach. Fla. Stat. Ann. § 817.5681(b)1 states that if notification to consumers is not performed within this time period, fines of up to $1000 per day for up to thirty days can be imposed. Pursuant to Fla. Stat. Ann. § 817.5681(b)1, if the company does not notify the customers of the breach after the subsequent thirty day period, the fines increase to $50,000 for each thirty day period, up to 180 days. If notification is not made within 225 days, any person required to make notification under Fla. Stat. Ann. § 817.5681(b)2 but fails to do so is

subject to an administrative fine of $500,000. Pursuant to Fla. Stat. Ann. § 817.5681(10)(b), fines of up to $50,000 are specified for failure to document the breach, or for failure to keep records of the breach for up to five years.

Most of the state notification laws track the California or Florida notification statutes by generally defining "personal information" as an individual's name, plus any one or more of the following "data elements:" the individual's Social Security number, driver's license or state identification card number, or account number in combination with a password or other access code for the account, when either the name or the data elements are not encrypted. However, some of the state notification laws apply to a broader range of information. Therefore, companies looking to comply with the consumer notification laws on a nationwide basis should consider increasing security measures for all data elements that any of the states include in the definition of "personal information," to the extent they retain such data elements.

II. INSURANCE COVERAGE FOR CYBER-RISKS UNDER A TYPICAL COMPREHENSIVE GENERAL LIABILITY POLICY

A business exposed to cyber-risks, whether through the collection and storage of consumer data or its own business data, or through its maintenance of its own website, chatroom or internet bulletin board, faces significant financial uncertainty if its sole protection against third party liability is the CGL insurance policy, one of the most pervasive types of insurance purchased by businesses. The CGL policy indemnifies the insured for liability to third parties for bodily injury, property damage, personal injury and advertising injury that is unintended from the perspective of the insured. It provides this coverage under two primary coverage parts; Coverage A, which provides cover for

"bodily injury" or "property damage" liability; and Coverage B, which provides coverage for "personal injury" and "advertising injury" liability.

Losses arising from new technologies do not neatly fit, if at all, within the insuring agreements of traditional CGL policies. Under Coverage A, property damage liability is typically defined as "physical injury to tangible property, including all resulting loss of use of that property," as well as "loss of use of tangible property that is not physically injured." The question thus arises whether electronic data can be considered "tangible" property. Another question is whether cyber-risk exposures in the nature of intellectual property, defamation and invasion of privacy claims are covered under Coverage B. For example, although an invasion of privacy claim is customarily among the specifically-enumerated "personal injury" offenses under a CGL policy, many policies will require a publication or utterance before granting cover for such a claim. Or, to fall under the "advertising injury" coverage grant of Coverage B, there must be a nexus between the policyholder's advertising activities and the offending activity.

In short, there are numerous gaps in coverage for cyber-risks under traditional CGL policies. Moreover, revisions to the CGL policy forms, beginning in 2001, have attempted to specifically limit coverage for cyber-risks. One significant change to the standard-form CGL policy, for example, attempts to expressly exclude electronic data from "tangible" property damage coverage.

It is beyond the scope of this paper to address each and every coverage issue raised by the different potential claims that could arise out of cyber-risk claims, including the potential first-party claims of businesses that experience such things as computer

viruses, hacker attacks and internet service provider outages.[3] To highlight some issues, we discuss the insurance coverage issues potentially implicated in a claim for property damage under Coverage A arising out of a data breach or loss or a claim for personal or advertising injury liability arising out of internet liability that potentially falls under Coverage B.

A. Data held to be "intangible"

Generally, courts interpreting the pre-2001 CGL language have held that data is not "tangible" property and have denied coverage for claims arising out of damaged or lost data. Most CGL policies provide cover only for tangible property damage and Courts in most jurisdictions have expressly held that a standard CGL policy does not provide coverage for loss of "intangible" property. *See, e.g., Guelich v. American Protection Ins. Co.*, 772 P.2d 536 (Wash. Ct. App. 1989); *Columbia Nat. Ins. v. Pacesetter Homes, Inc.*, 532 N.W.2d 1, 6 (Neb. 1995). Until recently, the prevailing view has been that electronic data is not tangible property damage that is covered under a CGL policy. *See, Lucker Mfg. v. Home Ins. Co.,* 23 F.3d 808, 818 (3d Cir. 1994) ("Tangible property is property that can be felt or touched, or property capable of being possessed or realized."); Paul M. Yost, et al*., In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Data,* 54 SMU L. Rev. 2055, 2066-68 (2001).

In *State Auto Prop. and Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp.2d 1113, 1116 (W.D. Okl. 2001), the United States District Court for the Western

[3] Although the terminology varies from policy to policy, first-party coverage provided by most commercial property policies generally requires "physical loss or damage to covered property that results from a covered cause of loss." *See* Robert H. Jerry, *Cybercoverage for Cyber-Risks, An Overview of Insurers' Responses to the Perils of E-Commerce*, 8 Conn. Ins. L. J. 7 (2001/2002). Accordingly, whether there has been damage to tangible, physical property will also be an issue with respect to first-party property policies.

District of Oklahoma held that electronic data is not tangible property for purposes of insurance coverage. Midwest Computers & More ("Midwest") was insured under a business owners' liability policy issued by State Auto Property and Casualty Insurance Company ("State Auto"). *Id.* at 1114. That policy provided coverage for "property damage" to "tangible property," and defined "property damage" as:

> a. Physical injury to tangible property, including all resulting loss of use of that property . . . .; or
>
> b. Loss of use of tangible property that is not physically injured.

[*Id.*]

In 1999, William C. Spray and Patricia Spray, doing business as Spray Appraisals ("Spray"), purchased a computer from Midwest and hired Midwest to perform certain computer services for the business. *Id.* Spray later alleged that Midwest negligently performed its computer service work, allegedly causing Spray to be deprived of the use of its computers and to lose extensive amounts of appraisal data and other business information which was stored on its computer system. *Id.* at 1114-15. When Midwest sought coverage under its business owners' liability policy, State Auto filed suit, seeking a declaratory judgment that it had no duty to defend or indemnify Midwest under the policy. *Id.* at 1115.

Both Midwest and State Auto agreed that the relevant issue to be decided was whether the computer data alleged to have been destroyed by Midwest was "tangible property" within the meaning of the business owners' liability policy. *Id.* The Court, however, determined that this issue alone was not dispositive on the issue of coverage and identified another issue: whether a loss of a computer occurred and, if so, whether the

loss of a computer satisfies the second part of the policy's definition of property damage, namely, loss of use of tangible property that is not physically injured. *Id.*

With respect to the issue of whether the lost data could be considered "tangible" property, the Court stated that the term "tangible" should be given its plain, ordinary and accepted meaning as something "capable of being perceived, especially by the sense of touch . . . capable of being precisely identified or realized by the mind." *Id.* at 1115-16. According to the Court, the ordinary meaning of the term tangible does not fit data stored on a computer disk or tape. *Id.* at 1116. Although the medium that holds the information (*i.e.*, the disk or tape) can be perceived, identified or realized, the information itself cannot be. *Id.* Because data itself cannot be touched, held or sensed by the human mind, the Court held that it cannot be considered tangible property. *Id.*

The Court next turned its attention to the issue of whether the loss of a computer can be considered property damage. Because a computer itself is tangible property, the Court held the "loss of use" of computers as a result of Midwest's alleged negligence to be property damage within the meaning of the policy. *Id.* As discussed in further detail below, however, Midwest was left without coverage after the Court determined that a policy exclusion precluded coverage for the claim at issue. *Id.*

This same reasoning was applied by the United States Court of Appeals for the Fourth Circuit in *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003). Shortly after the internet service provider America Online, Inc. ("AOL") released its Version 5.0 access software in October 1999, it was hit with a number of consumer class action lawsuits in state and federal court in the United States from consumers alleging damage to their computer system and preexisting software. *Id.* at 91. In short,

the consumer complaints alleged that AOL Version 5.0 altered the plaintiffs' existing computer software, disrupted their network connections, caused the loss of stored data and caused their operating systems to crash. *Id.* at 91-92. AOL tendered the defense of the consumer actions to St. Paul Mercury Ins. Co. ("St. Paul"), which denied coverage on the basis that the claims "do not allege damage to 'tangible' property and are not property damage as defined by the St. Paul [commercial general liability] policy." *Id.*

Like the Court in *Midwest Computers*, the Fourth Circuit in *America Online* applied to the term "tangible" its ordinary meaning of something that is capable of being touched and perceived in the physical sense. *Id.* at 94. Thus, it distinguished tangible computer hardware from intangible data, information and instructions. *Id.* at 95. The Court drew a distinction between "data or instructions and the physical machines that give them meaning." *Id.* It reasoned that:

> Instructions to the computer and the data and information processed by it are abstract ideas in the minds of the programmer and the user. The switches and the magnetic disks are media, as would be paper and pencil. Loss of software or damage to software thus is not damage to hardware, but to the idea, its logic, and its consistency with other ideas and logic. Of course, without any code and instructions, the hardware consists simply of millions of electronic switches, circuits and drives that can be turned on or off but that cannot function as a computer. To a user, such a computer would be "dead." But regardless of whether the software is rendered unusable, the hardware remains available for instructions and recording.
>
> [*Id.* at 95-96.]

The Court also analogized hardware to a tangible pad lock and data to the intangible combination to the lock: although the lock may be unusable without the combination, it is not physically damaged. *Id.* at 96.

It was in this light that the Court examined the allegations made by the consumer plaintiffs and determined that "[e]ven though a few . . . complaints [were] vague enough to suppose initially that the plaintiffs complain of damage to physical property, a closer look . . . reveals that the plaintiffs actually complain of damage to software." *Id.* at 97. Accordingly, it determined that the software problems did not amount to physical damage to tangible property for purposes of CGL coverage. *Id.* at 97-98.

Having determined that consumer claims did not allege physical injury to tangible property, the Court shifted its attention to AOL's contention that the consumers' loss of use of their computers constituted covered property damage. *Id.* at 98. The District Court sitting below had agreed with AOL that the consumers' loss of use of hardware was property damage within the meaning of the policy, but denied coverage based on the policy's "impaired property" exclusion. *Id.* As discussed in further detail below, the Fourth Circuit, on appeal, upheld the application of the impaired property exclusion as a bar to coverage, but declined to address the issue of whether the consumers' alleged loss of use of their computers was a tangible loss. *Id.* at 99.

B. Data held to be "tangible"

A minority of courts have granted coverage, usually where the loss of use of hardware on account of damaged or lost data was an element of the claim for loss of electronic data. However, recent decisions suggest that Courts may be moving away from traditional distinctions between tangible and intangible property, at least with respect to electronic data.

In a controversial decision, the United States District Court for the District of Arizona, in *American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc.*, 2000 U.S.

Dist. LEXIS 7299 (D.Ariz. 2000), held that loss of data and programming information constituted physical loss or damage under a first-party property policy.

Ingram Micro, Inc. ("Ingram"), a wholesale distributor of microcomputer products, was insured by American Guarantee & Liability Insurance Company ("American Guarantee") under a property damage policy that provided coverage against certain business interruption and service interruption losses. *Id.* at *1-*2. Ingram utilized a world-wide computer network known as the Impulse System ("Impulse") to track its customers, products and daily transactions. *Id.* at *2-*3. All of Ingram's orders, whether received electronically or through telephone sales representatives, were processed through Impulse, making its entire business operation dependant upon the proper functioning of Impulse. *Id.* at *3.

On the morning of December 22, 1998, Ingram's data center suffered a power outage that shut down all electronic equipment at the center, including computers and telephones. *Id.* at *3-*4. Although power was restored within a half-hour of the failure, Ingram's three mainframe computers lost all programming information that had been stored in their random access memory. *Id.* at *4. That lost programming information had to be manually re-loaded by Ingram employees. *Id.* It was not until approximately eight hours after the shut down that Ingram was able to restore Impulse to full power. *Id.* at *5. Ingram then sought coverage under its property damage policy with American Guarantee for the substantial business and service interruptions it suffered as a result of the power outage.

American Guarantee denied coverage and filed a declaratory judgment action against Ingram, claiming that its computer system had not been "physically damaged." It argued that:

> [T]he computer system and [other hardware] were not "physically damaged" because their capability to perform their intended functions remained intact. The power outage did not adversely affect the equipment's inherent ability to accept and process data and configuration systems when they were subsequently reentered into the computer system.
>
> [*Id.* at *5-*6.]

Ingram, in response, argued that the fact that the mainframe computers and other hardware retained their ability to accept restored information and eventually operate as before did not mean that they did not undergo "physical damage." *Id.* at *6. Ingram offered a broader definition of the term "physical damage," contending that it includes loss of use and functionality. *Id.*

The Court sided with Ingram's broader definition of property damage "[a]t a time when computer technology dominates our professional as well a personal lives." *Id.* It held that "'physical damage'" is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality." *Id.* As support for its holding, the Court looked to federal and state "cyber-crime" laws that defined "damage" as impairment, alteration, degradation or destruction of a computer system or network. *Id.* at *6-*7. It found these definitions to be relevant, despite the fact that they did not appear in insurance coverage cases, on the basis that:

> Lawmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is

> damage. Restricting the Policy's language to that proposed by [American Guarantee] would be archaic.
>
> [*Id.* at *7.]

Accordingly, the Court held that Ingram Impulse system had been "physically damaged" for eight hours and that Ingram, not American Guarantee, was entitled to summary judgment on the issue of coverage. *Id.* at *8-*9.

The Court's decision in *Ingram Micro* was widely criticized, as the Court violated well-established principles governing insurance contract interpretation -- namely, that the ordinary meanings of words in a contract control. Instead of giving effect to the word "physical," as it is ordinarily used, the Court simply read it out of the contract in order to reach its desired conclusion.

Although *Ingram Micro* involved the meaning of the term "physical" under a first-party property policy, it is nevertheless relevant to coverage under a CGL policy because the meaning of "physical" and "tangible" are closely related. *Ingram Micro* is noteworthy in that if a Court can conclude that loss of data amounts to a physical loss, it can just as easily conclude that data is "tangible" property under a CGL policy.

That is precisely what happened in *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 46 P.3d 1264 (N.M. Ct. App.), *cert. den.*, 47 P.3d 447 (N.M. 2002). Computer Corner, Inc. ("Computer Corner") engaged in the sale and service of personal computers. Fireman's Fund Insurance Company ("Fireman's") issued a CGL policy to Computer Corner. *Id.* at 1265. A customer brought his computer to Computer Corner for repair, and expressly informed the Computer Corner technician that various important files were on the computer and were not backed up. *Id.* at 1265-66. Nevertheless, the technician reformatted the hard drive without first backing-up its data. *Id.* As a result, the data was

irretrievably lost. *Id.* The customer thereafter filed suit against Computer Corner seeking damages for the cost of reconstructing its files. *Id.* Firemen's agreed to defend Computer Corner under a reservation of rights, but denied any duty to indemnify it. *Id.* at 1266.

The Court in *Computer Corner* did not specifically address the issue of whether the lost data constituted "tangible" property, as the District Court sitting below had concluded that "computer data is tangible property" and this ruling was not challenged by the parties. *Id.* Although the District Court's decision is not published, the Court of Appeals quoted the lower court as stating that the computer data at issue "was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed." *Id.* As discussed in further detail below, the Court's decision addressed the applicability of several policy exclusions that the lower court had held precluded coverage. *Id.* at 1268-70. Accordingly, it reversed the ruling of the lower court and held that Firemen's had a duty to indemnify Computer Corner under its CGL policy. *Id.* at 1270.

Recently, a New York state court, in a decision that may have implications on questions of insurance coverage, abandoned the traditional tangible/intangible property distinction when it comes to electronic data. *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 285-86 (N.Y. 2007), involved the question of whether a claim for conversion of electronic data is cognizable under New York law. Louis E. Thyroff ("Thyroff"), an insurance agent for Nationwide Mutual Insurance Company ("Nationwide"), was discharged from his job and denied access to "his customer information and other personal information that was stored on the [company] computers."

Id. at 285. *See also* Nick Ackerman, *Protecting Data with an Ancient Remedy*, The National Law Journal (October 3, 2007). Thyroff sued Nationwide in federal court for, among other things, "the conversion of his business and personal information." *Thyroff*, 8 N.Y.3d at 285. The federal district court dismissed his claim on the grounds that conversion does not apply to intangible computer data. On appeal, the Second Circuit Court of Appeals determined that New York state law was not clear as to whether a claim for conversion could be based on computer data and certified to the New York Court of Appeals, the state's highest court, the question of whether a claim for conversion of electronic data is cognizable under New York law. *Id.* at 285-86.

The New York Court of Appeals answered this question in the affirmative, holding that electronic records maintained on a computer are "subject to a claim of conversion in New York." *Id.* at 293. In so doing, the Court reviewed the evolution of the tort of conversion in accordance "with emerging societal values." *Id.* at 286-88. It looked as far back as the Norman conquest of England in 1066, when a "rightful ownership of property" was usually determined by a physical altercation between victim and thief. *Id.* The medieval practices were eventually replaced by legal actions for trespass, trover and, ultimately, conversion, with New York later modifying conversion's strict requirement for tangible property to provide that "an intangible property right can be united with a tangible object for conversion purposes." *Id.* at 286-89. This modification of the law of conversion became known as the "merger doctrine," and required a connection between the intangible property and a tangible object. Thus, for example, intangible shares of stock in a company could be considered the proper subject of a claim for conversion because they were represented by tangible stock certificates.

Thyroff represents an abandoning of the merger doctrine. The Court recognized that a "document stored on a computer hard drive has the same value as a paper document kept in a file cabinet." *Id.* at 292. The Court also relied on the pervasive use of computer data as a replacement for paper documents and determined that "the tort of conversion must keep pace with the contemporary realities of widespread computer use." *Id.* at 292.

Thyroff has implications that potentially reach beyond claims for conversion and may represent how U.S. courts view electronic data in future cases. While there are still jurisdictions that cling to the merger doctrine,[4] T*hyroff* appears to be the trend. For example, in *Kremen v. Cohen*, 337 F.3d 1024, 1031 (9th Cir. 2003), the Ninth Circuit Court of Appeals held that California law does not follow the strict merger doctrine when it upheld a conversion claim for the intangible property right in an internet domain name. Courts in other conversion cases have likewise assumed that computer data is subject to a claim for conversion without reference to the tangible/intangible property distinction. *See*, *generally*, Ackerman, Nick, *Protecting Data with an Ancient Remedy*, The National Law Journal (October 3, 2007).

Given the growth of and increasing importance of electronic data as an asset in and of itself, *Thyroff* is a well-reasoned opinion that may be looked to as precedent in a challenge to an insurer's denial of coverage for a cyber-risk loss of data claim under a CGL policy.

[4] *See*, *e.g.*, *Slim CD Inc. v. Hartland Payment Sys., Inc.*, 2007 U.S. Dist. LEXIS 62536 at *12 (D.N.J. Aug. 24, 2007); *Northeast Coating Techs. Inc. v. Vacuum Metallurgical Co. Ltd.*, 684 A.2d 1322, 1324 (Maine 1996).

C. Potentially Applicable Exclusions under Coverage A

Even where loss of data may be considered damage to tangible property or loss of use of tangible property that is not physically injured, coverage may ultimately be precluded by one or more applicable policy exclusions, including, but not limited to:

Business Risk Exclusions

In *Midwest Computers*, *supra.*, 147 F.Supp.2d at 1113, the Court held that the customer's "loss of use" of its computers as a result Midwest's allegedly negligent computer services to be "property damage," but in the end declared that the "business risk" exclusion of the business owners' liability policy at issue barred coverage. *Id.* at 1116-18. That exclusion precluded coverage for property damage to "that particular part of any property that must be restored, repaired or replaced because 'your work' was incorrectly performed on it." *Id.* at 1116. Further, the Court held that the Products-Completed Operations exception to the exclusion did not apply because the underlying Complaint alleged that the loss had occurred before Midwest had completed its work. *Id.* at 1117.

On the contrary, the Court in *Computer Corner*, *supra.*, 46 P.3d at 1264, held that the business risk exclusions in the policy at issue did not preclude coverage, where the Court had already held lost computer data to be "tangible" property. One of the business risk exclusions at issue in *Computer Corner* provided that the insurance did not apply to "property damage to your product arising out of it or any part of it." *Id.* at 1268. The other business risk exclusion provided that the insurance did not apply to "property damage to your work arising out of it or any part of it and included in the products-completed operations hazard." *Id.* The Court's ultimate conclusion with respect to both

the "your property" and "your work" business risk exclusions was that the property that was lost -- the customer's computer files -- clearly existed prior to and apart from any service or parts provided by Computer Corner in repairing the computer and was thus not Computer Corner's "product" or "work." *Id.* Moreover, it also found nothing in the applicable exclusions or definitions that would have suggested to a reasonable insured in Computer Corner's position that "property damage to your product" or "property damage to your work" includes damage to a customer's pre-existing electronic data. *Id.* Accordingly, the Court held that the business risk exclusions did not apply.

Impaired Property Exclusion

Another example of a policy exclusion that may act to bar coverage in a cyber-risk case is the Court's application of the "impaired property" exclusion in *America Online*, *supra.*, 347 F.3d at 98. There, the Court held that the loss of computer data and damage to software was not damage to tangible property and, because it also found that the impaired property exclusion applied, it did not specifically answer the question of whether the losses could be considered "loss of use" property damage. The relevant portions of the impaired property exclusion at issue in *America Online* provided:

> We won't cover property damage to impaired property, or to property which isn't physically damaged, that results from:
>
> . . . your faulty or dangerous products or completed work;
>
> * * *
>
> *Impaired property* means tangible property, other than your products or completed work, that can be restored by nothing more than:
>
> . . . an adjustment, repair, replacement, or removal of your products or completed work which forms a part of it . . .

[*Id.*]

AOL argued that the impaired property exclusion could not be applied because the underlying consumer complaints "allege[d] physical damage to and loss of use of computers that could not be fixed simply by repairing, removing, or replacing AOL Version 5.0, thus taking the claims outside the definition of impaired property." *Id.* According to the Court, however, that argument failed to address what it termed the "relevant portion" of the impaired property exclusion which, in edited form, provided that: "We won't cover property damage [including loss of use of tangible property] . . . to property which isn't physically damaged, that results from . . . your faulty . . . products." *Id.* The Court believed that the "straightforward meaning" of the impaired property exclusion barred coverage for loss of use of tangible property of others that is not physically damaged by the insured's defective product and placed a limitation on the coverage of consequential damages, restricting coverage to loss of use other persons' properties that are physically damaged. *Id.* The Court further explained that without the limitation of coverage to property that is physically damaged, the insurer's risk would have been much greater and it would have been asked to defend a wide range of claims that did not involve physical damage to tangible property. *Id.* According to the Court, the limitation imposed by the impaired property exclusion was designed specifically to deny coverage for this broader risk. *Id.* And because there was no specific allegation that the physical or tangible components of any computer were damaged (only that software caused damage to other software), the Court concluded that the impaired property exclusion applied. *Id.* at 99-100.

On the other hand, the Court in *Computer Corner*, *supra.*, 46 P.3d at 1264, concluded that a similar "impaired property" exclusion did not apply to preclude coverage. The particular exclusion at issue in *Computer Corner* provided that the insurance did not apply to:

> Property damage to impaired property or property damage that has not been physically injured arising out of:
>
> (1) A defect, deficiency, inadequacy or dangerous condition in your product or your work; or
>
> (2) A delay or failure by you or anyone acting on your behalf to perform a contract or agreement in accordance with its terms.
>
> This exclusion does not apply to the loss of use of other property arising out of sudden and accidental physical injury to your product or your work after it has been put to its intended use.

[*Id.* at 1268-69.]

In short, the Court found the impaired property exclusion to be "complicated" by the incorporation of multiple terms ("property damage," "impaired property," "your product," "your work") defined elsewhere in the policy. *Id.* at 1269. It ultimately concluded that the exclusion was "unintelligible from the standpoint of a hypothetical reasonable insured operating a computer repair service." *Id.* at 1270. It therefore held the exclusion to be too vague and indefinite to be enforceable. *Id.*

Intentional Acts Exclusion

CGL policies typically contain an "intentional acts exclusion" that bars coverage for bodily injury or property damage "expected or intended from the standpoint of the insured." The applicability of an intentional acts exclusion was also among the issues examined by the Court in *Computer Corner*, *supra.*, 46 P.3d at 1264, where the insured's

computer technician reformatted a customer's hard drive without first backing-up the data. To make matters worse, the customer had also informed another of the insured's technicians that the hard-drive's data was important and had not been previously backed-up. In the end, the Court refused to apply the intentional acts exclusion, finding that the failure of one technician to report to another technician the fact that the customer expressly instructed that the files be backed-up was "the result of mis-communication, mistake or carelessness, rather than a conscious decision to cause harm to the [the insured's] property." *Id.* at 1267. Moreover, the Court found that there was no evidence that the technician who reformatted the hard drive understood that it contained the only copy of certain files and that by reformatting it he would be contributing to the permanent loss of data. *Id.* at 1269. Accordingly, the Court held that the loss of data was neither "expected nor intended" from the perspective of the insured and did not act to exclude coverage. *Id.*

Electronic Data Exclusion

The current ISO CGL form policy provides that the insurance provided under Coverage A does not apply to:

> Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.
>
> As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.
>
> [CGL Policy Form CG 00 01 12 04, ISO Properties, Inc., 2003.]

This amendment to the CGL policy takes aim at those judicial decisions that have found damage to data to be damage to tangible property and should make clear to policyholders that on a going-forward basis insurers do not intend to provide cover for losses of electronically stored data under the traditional CGL policy.

D. Personal and Advertising Injury Coverage for Cyber-Risk Claims

We also examine the potential for coverage of certain cyber-risk offenses under Coverage B, as insureds may also seek coverage under traditional CGL policies for cyber-risk claims involving defamation, invasion of privacy and intellectual property exposures, such as copyright or trademark infringement, to name a few. These will most typically arise in connection with internet websites, chatrooms and bulletin boards, including websites on which a business sells or advertises its products or services.

The term "personal and advertising injury" is typically defined to mean:

> [I]njury, including consequential bodily injury, arising out of one or more of the following offenses:
>
> * * *
>
> d. Oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services;
>
> e. Oral or written publication, in any manner, of material that violates a person's right of privacy;
>
> f. The use of another's advertising idea in your "advertisement"; or
>
> g. Infringing upon another's copyright, trade dress or slogan in your "advertisement".

[CGL Policy Form CG 00 01 12 04, ISO Properties, Inc., 2003.]

The term "advertisement" is typically defined to mean:

> [A] notice that is broadcast or published to the general public or specific market segments about your goods, products or services for the purpose of attracting customers or supporters.

[*Id.*]

Further, in light of the internet and e-commerce boom of the last decade, this definition has been modified to include that, for purposes of the definition of "advertisement":

> a. Notices that are published include material placed on the Internet or on similar electronic means of communication; and
>
> b. Regarding web-sites, only that part of a web-site that is about your goods, products or services for the purposes of attracting customers or supporters is considered an advertisement.

[*Id.*]

This language addresses the realization of the ISO drafters that internet advertising and marketing is now an important way that merchants disseminate information about their goods and services, but the language in subsection (b) appears to narrow the coverage businesses receive with respect to information on their website. *See* Robert H. Jerry, *Cybercoverage for Cyber-Risks, An Overview of Insurers' Responses to the Perils of E-Commerce*, 8 Conn. Ins. L. J. 7 (2001/2002). For example, information about a competitor's products or other unrelated products produced by other manufacturers, links to other websites and banner advertising by other businesses that appear on the insured's website all seem to fall outside of this definition of "advertisement." *Id.*

Accordingly, in order for a copyright or trademark infringement claim arising out of internet activities to be considered a "personal or advertising injury," it must arise out of the insured's advertising activities, as defined in the policy.

Likewise, for a cyber-related defamation or invasion of privacy claim to be covered as a "personal or advertising injury," the defamatory material must have been "published." In other words, a publication or utterance of the defamatory or private material is required before coverage can be found.

As for potentially-applicable exclusions, the CGL policy has long excluded coverage for insureds who are in the business of advertising, broadcasting, publishing or telecasting. *Id.* Recent revisions to the ISO CGL form have placed certain Internet-based businesses squarely within this exclusion, as follows:

> This insurance does not apply to:
>
> j. Insureds In Media And Internet Type Businesses
>
> "Personal and advertising injury" committed by an insured whose business is:
>
> * * *
>
> (2) Designing or determining content of websites for others; or
>
> (3) An Internet search, access, content or service provider.
>
> * * *
>
> For the purposes of this exclusion, the placing of frames, borders or links, or advertising, for you or others anywhere on the Internet, is not by itself, considered the business of advertising, broadcasting, publishing or telecasting.

[*Id.*]

Coverage is also now typically excluded, under the Electronic Chatrooms Or Bulletin Boards exclusion, for:

> "Personal and advertising injury" arising out of an electronic chatroom or bulletin board the insured hosts, owns, or over which the insured exercises control.
>
> [*Id.*]

Thus, for example, if an insured defames a business competitor on an industry-specific chatroom, a claim arising out of that event should be excluded from coverage pursuant to this exclusion.

Finally, we also note that the so-called "intellectual property exclusion" may act as another bar to coverage under Coverage B. That exclusion provides that the insurance does not apply to:

> "Personal and advertising injury" arising out of the infringement of copyright, patent, trademark, trade secret or other intellectual property rights.
>
> However, this exclusion does not apply to infringement, in your "advertisement," of copyright, trade dress or slogan.
>
> [*Id.*]

This broadly-phrased exclusion does not effectively leave much intellectual property coverage available to insureds. *See* Robert H. Jerry, *Cybercoverage for Cyber-Risks, An Overview of Insurers' Responses to the Perils of E-Commerce*, 8 Conn. Ins. L. J. 7 (2001/2002). It specifically excludes patent, trademark and trade secret infringement claims from coverage as "personal and advertising injury" and also excludes "other intellectual property rights." *Id.* In fact, the exclusion is so broad that it requires an exception to the exclusion to grant back the limited intellectual property coverage

afforded under Coverage B to "copyright, trade dress or slogan" in the insured's "advertisement." *Id.*

E. Potential Coverage under Directors' and Officers' and Errors and Omissions Policies

We briefly discuss two additional types of insurance coverage that may be implicated in a cyber-risk claim: Directors' and Officers' ("D&O") insurance and Errors and Omissions ("E&O") insurance. D&O insurance indemnifies individual directors and officers sued in connection with the discharge of their corporate duties. *Id.* E&O policies offer defense against and indemnification for claims arising from "negligence, omissions, mistakes, and errors by the insured in the course of providing professional services." *Id.*

Typically, D&O policies are comprised of two types of coverage: (1) coverage for defense costs and other related expenses and (2) indemnification of covered individuals for third-party liabilities. *Id.* Designed to cover acts such as negligence and errors in judgment, D&O policies may, for example, provide protection against shareholder derivative actions predicated on allegations of breach of fiduciary duty based on the purported failure to implement measures to prevent such cyber-risks as computer hacker attacks. *Id.*

E&O policies, traditionally tailored and marketed to professionals such as lawyers and physicians, have now also been specifically geared toward computer consultants, software and hardware providers and e-commerce and technology experts. *Id.* We discuss in Section III below other new forms of technology oriented insurance created to specifically provide coverage for the new forms of cyber-risks not covered under traditional CGL and other types of policies.

As discussed above, the standard form CGL policy has been amended to ensure that there is no ambiguity on the issue of whether insurers now consider lost electronic data to be property damage and whether such policies provide cover for such damage. However, as a result of the growth of e-commerce and the storage of electronic data (and the new types of claims they have wrought), insurers have begun to address the need in the insurance marketplace for cyber-risk policies that are specifically designed for cyber-related losses and liability. *Insuring Cyberspace: Why Traditional Insurance Policies are not Enough: The Nature of Potential E-Commerce Losses & Liabilities*, 3 Vand. J. Ent. L. & Prac. 84, 89 (Winter 2001). Insurance companies now offer a wide-range of cyber-risk insurance to cover losses due to cyber activities. *Id.* For example, some now offer coverage for security breaches by providing coverage for computer equipment, electronic data and storage-related risks. *Id.* The new cyber-risk policies have removed the issue of whether lost electronic data is "tangible" property by explicitly providing coverage for computer equipment, hard drives, electronic data processing, software exposure and system break downs. *Id.*

III. THE DEVELOPMENT OF CYBER-RISK INSURANCE AND CYBER-RISK MANAGEMENT

A. *Cyber-risk insurance*

"Cyber-risk insurance" is really an umbrella term that can encompass many different types of coverages, ranging from data theft and computer malfunction to external hacking, internal sabotage and theft, web-content liability and copyright infringement, to name a few. The cyber-risk insurance market was virtually non-existent ten years ago. By 2005, the cyber-risk insurance market was estimated to amount to between $250 million to $300 million in written premium. Toby L. Merrill, *Cyber*

liability market is older, wiser, smarter and still growing, available online at http://www.insuranceejournal.com/magazines/west/2007/01/29/features/76734.htm. By 2006, it had burgeoned into a $500 million market that continues to expand. *Id.*

Network Liability and Privacy Liability policies are two types of cyber-risk policies that can be viewed as "gap filler" policies intended to fill gaps in an overall insurance program for non-physical/non-tangible loss and liabilities. A Network Liability policy would include coverage for restoration costs, namely, the cost to replace, restore or recreate the insured's lost data or customized program lost as a result of a hacker or system failure. Public relations expenses might also be covered. This would encompass the costs of retaining a public relations consultant to help restore or protect the insured's reputation in response to adverse media coverage as a result of a cyber-attack or system failure resulting in lost or stolen data. Coverage might be also had for investigative expenses necessary to respond to a cyber loss so that damage may be minimized or mitigated, and future damage prevented. Investigative expenses might also include the cost of gathering evidence demonstrating wrongdoing. A Network Liability policy might also include cover for extortion threats, in the form of reimbursement of costs incurred in responding to a threat to introduce an unauthorized code into the insured's computer system or to divulge private data without authorization.

A Privacy Liability policy, which insures against liability arising from the unauthorized disclosure or loss of private information, might provide enhanced coverage for an insured's failure to protect confidential information. Such a policy might also provide coverage for credit monitoring and credit remediation for the individuals whose confidential information had been compromised; vicarious liability of the insured when

control of confidential information is outsourced to an outside vendor; public relations expenses; regulatory defense costs; government imposed fines and penalties; and the cost of notifying individuals that their personal data had been lost or stolen.

Some other types of typical cyber-risk insurance coverage products on the market today include: General Internet Crime Liability, which addresses first and third party risks associated with e-commerce, the internet, networks and informational assets; Property Liability, which protects against damage to hard assets caused via the internet, machinery taken down or equipment programmed to operate erratically (but typically does not acknowledge "data" as property); and Media Liability Coverage, which protects against claims arising out of the gathering and communication of information, providing coverage against defamation and invasion of privacy claims as well as copyright and trademark infringement. Denis Drouin, *Cyber Risk Insurance: A Discourse and Preparatory Guide*, GIAC Security Essentials Certification, Practical Assignment Version 1.4a, option 1 (February 9, 2004). A cyber-risk policy might also provide Business Income Loss coverage, which would encompass earnings loss and extra expenses loss as a result of non-physical events such as a hacker attack or a computer virus. Coverage for Business Income Loss might also include loss of revenues from websites or as a result of supply chain failures caused by viruses, hackers or employees maliciously causing a system to crash. *Id.*

Chubb, for example, is one insurer that now offers a variety of cyber-risk insurance products, including a policy marketed as "CyberSecurity by Chubb for Financial Institutions." *See* http://www.chubb.com/business/csi/chubb822.html. According to Chubb, that policy is intended specifically for financial institutions and is

designed to address their most vulnerable e-commerce exposures in one straightforward policy. The policy consists of six insuring clauses, described by Chubb as follows:

- **E-Theft:** Designed to protect against losses resulting from: (1) the transfer, payment or delivery of funds or other property due to a cyber attack; (2) the misappropriation, copying or duplication of confidential customer information or records by hacker or employees who breach network security; and (3) the physical loss or damage of stolen electronic media.

- **Denial or Impairment of E-Service:** Designed to protect the financial institution when its system is subject to cyber-attack or fraudulently accessed, *regardless of whether there has been direct physical loss or damage to tangible property*. This includes system slowdowns or shutdowns caused by cyber attacks, such as worming or spamming.

- **E-Communication:** Applies when an electronic communication is sent from one financial institution to another to initiate, authorize or acknowledge a monetary transaction, and the communication was either not sent by the insured institution or was fraudulently modified during the electronic transmission.

- **E-Vandalism:** Helps the financial institution pay for the direct cost of restoring the integrity of its site in the aftermath of hackers' vandalism of any data, instructions or communications within the system.

- **E-Threat:** Protects against threats made against the institution's system that could result in taking the system off-line or a breach in network security (*e.g.*, the release of confidential customer information). Reimburses the institution for expenses incurred to mitigate loss in the event of an alleged threat (provided the threat is technologically credible), rather than wait for the perpetrator to act on such a threat and risk any downtime. Also pays for fees and expenses of any public relations consultant if the firm has been the target of such a threat.

- **E-Signature:** Protects the institution from direct loss resulting from accepting a customer's electronic signature on loan agreements secured by real property, such as a

> mortgage, and then discovering that the signature is fraudulent.
>
> [*Id.*]

The CyberSecurity by Chubb for Financial Institutions policy is but one example of the many types of new insurance products offering coverage for cyber-risks, which, like all insurance products, can be tailored for specific industries and threats.

B. *Risk management guidelines*

Ideally, all businesses would conduct a comprehensive privacy and security audit and promptly implement all recommendations in a timely manner to avoid falling victim to one of the many "cyber-risks" that can victimize a business in today's electronic world. If a business does not have the resources to conduct its own audit, it should hire an outside company to perform a security assessment. Likewise, as part of its underwriting of a cyber-risk policy, an insurer should require that a privacy and security audit of the applicant be performed.

It is beyond the scope of this discussion to offer a comprehensive risk management guideline for managing cyber-risks. However, it is needless to say that any security audit or assessment and any risk management procedures that are put in place carefully examine both a company's network security and the physical security of its computer hardware. There are a myriad of questions that can be asked in regard to both of these areas. As to network security, some questions that arise are: whether the business has "firewalls" in place to prevent unauthorized access to internally protected networks from external sources; whether authentication vehicles are used to allow connections from remote users into internal networks; how often are firewalls and anti-virus safeguards updated; and whether the business has a dedicated response team and

continuity plan in the event of a security breach. As to physical security, some pertinent questions include: whether a full inventory of all computer-related equipment has been conducted; whether critical computer servers are maintained in a secure fashion; who has access to servers and what access controls are in place; and how sensitive materials and data are safeguarded and disposed of. *See*, *generally*, Denis Drouin, *Cyber Risk Insurance: A Discourse and Preparatory Guide*, GIAC Security Essentials Certification, Practical Assignment Version 1.4a, option 1 (February 9, 2004).

Other questions and specific areas of inquiry would depend on the type of business and the size of the business. For example, if a business conducts credit card transactions over the internet the manner in which sensitive consumer data is collected and stored would have to be thoroughly examined. Also, if a business maintains a website, pertinent questions include whether it owns the intellectual property rights to the content on the website and whether it has any established procedures in place for removing infringing or offensive material from its website. How a particular business's revenues would be affected if a security breach occurred is also a question that might be asked from a risk management perspective. *Id.*

Underwriters will, of course, have their own set of questions and issues to address in evaluating a new risk. AON has produced a document setting forth some of the factors examined by underwriters in the context of cyber-risk insurance, specifically, Network Liability coverage. These include:

- **Financial Stability and Lack of Losses:** Some industries are more prone to cyber-risk incidents than others. An insurer must price risk accordingly.

  Key Documentation: financial statements and loss runs.

- **Sales Practices and Contract Procedures:** With respect to those businesses engaged in e-commerce, an underwriter will want to examine sales practices to verify mutual expectations of the applicant business and its customers. Limitation of liability clauses, exculpation of warranty provisions and consistent contract review procedures are critical.

  Key Documentation: standard contracts and guidelines to amend standard clauses.

- **Dispute Procedures:** How does the business avoid litigation?

  Key Documentation: complaint and dispute guidelines.

- **Formal Management Responsibility and Standards:** Companies must successfully demonstrate that the responsibility to maintain a secure network is a responsibility entrusted to a senior individual within the organization, such as a Chief Security Officer, Chief Technology Officer or Chief Operating Officer (or a systems administrator for a smaller company). Network security policies and procedures should be published and communicated to all staff. Network assessment and testing should be conducted according to industry standards.

  Key Documentation: written network security policies and procedures, security audit schedules and security audit reports.

- **Physical Network Security Safeguard Controls:** The business needs to demonstrate that its physical environment is "robust" enough to keep cyber-criminals at bay. Along with basic devices such as magnetic access cards for employees and closed circuit television, data centers and server rooms should be accessible only by the IT staff. Staff should know who to call in the event of suspicious activity.

  Key Documentation: physical security policies and guidelines, lists of perimeter and internal security elements in place.

- **Logical Network Security Controls:** At a minimum, network security controls should include filters and

firewalls to keep intruders from accessing the network from the Internet or other private networks; antivirus software to keep viruses, worms and other malicious code at bay; and intrusion detection software to identify potential network trespassers. In the event that medical, financial or other non-public personally-identifiable information (*e.g.*, social security numbers) is transmitted over the Internet or stored as electronic data, sufficient encryption standards should be enforced.

Key Documentation: network architecture diagrams, firewall and intrusion detection software make and model information, antivirus vendor information, and a copy of procedures and policies in place to ensure that new equipment is properly configured before it is connected to the network.

- **Change Management Controls:** Policies and procedures must be in place to ensure that network access rights for ex-employees (and sub-contractors) who have been terminated or who have resigned are revoked, and that facility access cards are revoked during exit interviews.

  Key Documentation: written employee resignation and termination guidelines in network security planning document.

- **Internet Content Controls:** Businesses must be able to document written controls over the posting of information on websites. These include, but are not limited to, legal reviews to ensure that any third party content posted has gone through a formal clearing process and proper management of chat rooms, discussion boards and other interactive areas of company sites.

  Key Documentation: written rules, including legal reviews, regarding the posting of content on company sites.

- **Disaster Recovery and Business Continuity Planning:** This is a critical component of any Network Liability risk submission, particularly where contractually guaranteed network availability is offered to customers or network interruption coverage is required by the applicant. Companies with large networks should be prepared to demonstrate that formal disaster recovery and business continuity plans are in place not only to protect critical

> data, but also to ensure that network availability is maintained in the event of a natural disaster or hacker attack. Elements include, but are not limited to, data backup and recovery testing and redundant applications and connections.
>
> *Key Documentation:* Disaster recovery and business continuity planning reports and outlines.
>
> [AON, *Network Risk Insurance: A Layman's Overview* (October 2004).]

Finally, we note that it is also critical that all businesses ensure that they are aware of and in compliance with all applicable data notification laws, some of which are described above.

All of this brings us back to TJX. Investigators in the TJX case believe that the data breach began when hackers pointed a telescope-shaped antenna at a Marshall's store in St. Paul, Minnesota, and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers and the store's computers. That helped them hack into TJX's central database to repeatedly purloin customer information and credit card numbers. A post-breach audit has revealed that TJX was slower than many merchants to make a change to a more complex and wireless encryption system called Wi-Fi Protected Access, or WPA. The audit also found that TJX failed to install firewalls and data encryption on many of its computers using the wireless network, and did not properly install another layer of network security software it thought it had purchased. *See* Joseph Pereira, *Breaking the Code: How Credit Card Data Went Out Wireless Door*, The Wall Street Journal (May 4, 2007).

Proper and thorough underwriting and the implementation of a "cyber-risk" risk management program can help prevent businesses from becoming the next TJX and, at the same time, will help to cut insurers' losses on cyber-risk claims.

IV. CONCLUSION

Advanced and accessible computer technologies have provided businesses both large and small with new opportunities in the world of e-commerce. At the same time, those new opportunities have come with risks heretofore unseen by businesses and insurers alike. The cyber-risks represented by lost or stolen data and the other perils of the cyber-age do not neatly fit under the coverage of traditional insurance policies such as CGL policies, with their requirement of "tangible" property loss and other policy language affording coverage for the "brick and mortar" business losses of years past. Moreover, potential coverage exclusions abound under both Coverage A and Coverage B. At the same time as it has revised the standard ISO form CGL policy to further limit coverage for cyber-risks, the insurance industry has introduced new cyber-risk-specific products that move beyond the traditional areas of coverage and recognize that, to today's businesses, data is just as "tangible" as any other valuable property. Both insurers and insureds need to be aware of the new risks and must plan accordingly through implementation of cyber-risk specific underwriting and risk management guidelines and the purchase of cyber-risk insurance.