NAIC
National Association of Insurance Commissioners

JOURNAL OF INSURANCE REGULATION

Cassandra Cole and Kathleen McCullough
Co-Editors

Vol. 33, No. 6

Cyber Liability: It's Just a Click Away

Anthony R. Zelle
Suzanne M. Whitehead

JIR-ZA-33-06

NAIC
National Association of Insurance Commissioners

The NAIC is the authoritative source for insurance industry information. Our expert solutions support the efforts of regulators, insurers and researchers by providing detailed and comprehensive insurance information. The NAIC offers a wide range of publications in the following categories:

Accounting & Reporting
Information about statutory accounting principles and the procedures necessary for filing financial annual statements and conducting risk-based capital calculations.

Consumer Information
Important answers to common questions about auto, home, health and life insurance — as well as buyer's guides on annuities, long-term care insurance and Medicare supplement plans.

Financial Regulation
Useful handbooks, compliance guides and reports on financial analysis, company licensing, state audit requirements and receiverships.

Legal
Comprehensive collection of NAIC model laws, regulations and guidelines; state laws on insurance topics; and other regulatory guidance on antifraud and consumer privacy.

Market Regulation
Regulatory and industry guidance on market-related issues, including antifraud, product filing requirements, producer licensing and market analysis.

NAIC Activities
NAIC member directories, in-depth reporting of state regulatory activities and official historical records of NAIC national meetings and other activities.

Special Studies
Studies, reports, handbooks and regulatory research conducted by NAIC members on a variety of insurance-related topics.

Statistical Reports
Valuable and in-demand insurance industry-wide statistical data for various lines of business, including auto, home, health and life insurance.

Supplementary Products
Guidance manuals, handbooks, surveys and research on a wide variety of issues.

Securities Valuation Office
Information regarding portfolio values and procedures for complying with NAIC reporting requirements.

White Papers
Relevant studies, guidance and NAIC policy positions on a variety of insurance topics.

For more information about NAIC publications, view our online catalog at:

http://store.naic.org

Printed in the United States of America

NAIC Executive Office
444 North Capitol Street, NW
Suite 700
Washington, DC 20001
202.471.3990

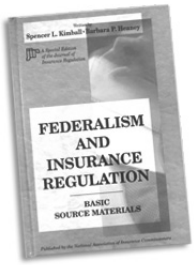
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, MO 64106
816.842.3600

NAIC Capital Markets
& Investment Analysis Office
One New York Plaza, Suite 4210
New York, NY 10004
212.398.9000

NAIC
National Association of Insurance Commissioners

Companion Products

The following companion products provide additional information on the same or similar subject matter. Many customers who purchase the ***Journal of Insurance Regulation*** also purchase one or more of the following products:



Federalism and Insurance Regulation

This publication presents a factual historical account of the development of the framework for insurance regulation in the United States. It does so in part by using illustrative early statutes, presenting them chronologically, and in part by using cases that illustrate the interpretation of the crucial later statutes. Copyright 1995.

Regulation and the Casualty Actuary

This anthology reprints 20 important papers from past issues of the Journal of Insurance Regulation that are most relevant for practicing actuaries and state insurance regulators. It covers a wide range of issues, such as ratemaking, auto insurance pricing, residual markets, reserving and solvency monitoring. This invaluable reference explains these complex topics in straightforward, non-technical language. Copyright 1996.

How to Order

816.783.8300 | prodserv@naic.org | http://store.naic.org

International orders must be prepaid, including shipping charges. Please contact an NAIC Customer Service Representative, Monday - Friday, 8:30 am - 5 pm CT.

Editorial Review Board

Purpose

The *Journal of Insurance Regulation* is sponsored by the National Association of Insurance Commissioners. The objectives of the NAIC in sponsoring the *Journal of Insurance Regulation* are:

1. To provide a forum for opinion and discussion on major insurance regulatory issues;
2. To provide wide distribution of rigorous, high-quality research regarding insurance regulatory issues;
3. To make state insurance departments more aware of insurance regulatory research efforts;
4. To increase the rigor, quality and quantity of the research efforts on insurance regulatory issues; and
5. To be an important force for the overall improvement of insurance regulation.

To meet these objectives, the NAIC will provide an open forum for the discussion of a broad spectrum of ideas. However, the ideas expressed in the *Journal* are not endorsed by the NAIC, the *Journal's* editorial staff, or the *Journal's* board.

Cyber Liability: It's Just a Click Away

Anthony R. Zelle*
Suzanne M. Whitehead**

Abstract

In 2014, the number of records containing sensitive personal information involved in reported data breaches in the United States over the past decade will surpass 1 billion. Additionally, the cost of data breaches is expected to approach $500 billion in 2014. Inevitably, litigation comes on the heels of data breaches. Over the past decade, courts have considered the issue of whether data breaches and other cyber-based losses are covered under general liability policies. This article discusses the evolution of cyber-risk disputes involving traditional policies and explores possible future coverage issues under cyber liability policies.

* Anthony R. Zelle is the founding partner of Zelle, McDonough & Cohen, LLP. His expertise is insurance law and risk management. He counsels insurers and policyholders and, since he began practicing in 1986, he has litigated, arbitrated and ultimately resolved disputes involving all types of liability, property, life, health and disability insurance products. He is a member of the board of directors of the Defense Research Institute and previously served as the chair of the Insurance Law Committee. He compiled and edited the *Compendium of the Law of Insurance Bad Faith and Extra-Contractual Liability*, which is the primary desk reference for both practitioners and insurers in the field.

** Suzanne M. Whitehead is a senior associate at Zelle, McDonough & Cohen, LLP, where she counsels clients and litigates matters involving insurance coverage disputes arising under general liability and professional liability policies. She is a member of the Defense Research Institute Young Lawyers Steering Committee. Suzanne was the associate editor-in-chief for the Defense Research Institute's *Professional Liability Insurance Coverage: A Compendium of State Law*.

Introduction

Companies rely on cyber technology to administer many facets of their business, including transacting business with outside customers or clients; capturing, storing and analyzing pertinent data; and managing the financial aspects of the company. All of this crucial and sensitive information could be compromised in several ways, leading to serious consequences for the average business. A hacker gaining access to a business's records could potentially steal confidential personal information. A computer virus could systematically cripple crucial operating systems, effectively shutting down the company for days, weeks or longer. An employee could access financial accounts, alter records and misappropriate significant sums of money. Or, a home computer with "cloud computing" linked to the user's employer could be stolen, thereby providing potential access to sensitive business information.

In 2014, the number of records containing sensitive personal information involved in reported data breaches in the United States over the past decade will surpass 1 billion (*SC Magazine*, 2014). At the rate data breaches have increased over the past decade, that number will exceed 1 trillion in the next decade. The cost of data breaches is expected to exceed $491 billion in 2014 (Robinson, 2014). The more notable data breaches over the past few years include Target, involving 70 million records; Neiman Marcus, involving 40 million records; LivingSocial, involving 50 million records; Apple, involving 12 million records; and a seven-year hacking scam perpetrated by five Russians and a Ukrainian that involved 160 million records held by 7-Eleven, JCPenney, Dow Jones, NASDAQ and JetBlue among others.[1] The good news: According to a 2013 report prepared by the Ponemon Institute (Ponemon, 2012), which conducts independent research on privacy, data protection and information security policy, the average loss cost per record for data breaches in the United States is decreasing and was $188.00 in 2012.[2] However, the average loss per incident is increasing and was $9.4 million in 2012.

Beyond the data breach liability, massive infrastructure property damage and personal injury, as a result of computer-coded human implants, for example, pose significant risk. The insurance market has responded, and many carriers, large and small, have taken the opportunity presented by developments in the cyber world to develop coverage forms that will protect businesses against the risk of cyber crime

1. For more specifics on these and other widespread data breach losses and a fascinating graphic depiction of the data, see, "World's Biggest Data Breaches," *www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/* (last visited June 5, 2014).

2. For these and other costs associated with data breach losses, there is abundant information developed through benchmark research sponsored by Symantec and independently conducted by Ponemon Institute LLC, available at *www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf*.

and mischief. Beazley PLC began offering cyber-risk coverage four years ago and already has thousands of clients that generate more than $100 million a year in premiums (Willhite, 2013). These policies offer protection against some of the measurable costs that follow a breach. Those include the forensics required to analyze a breach, regulatory requirements to alert customers when their data have been exposed and credit monitoring for affected customers. Covered by less accurately measurable risk is the cost of litigating class-action lawsuits that may arise in the wake of a breach.

For regulators, the ebb of consumer general liability (CGL) protection and flow of cyber coverage presents both a challenge and an opportunity. Generally, cyber coverage falls into two categories: 1) forms that offer coverage for first-party risks, such as cybercrime, viruses and system malfunctions; and 2) forms that insure against third-party risks, such as data breach claims and claims for the infection of outside systems. Although these cyber policy provisions afford coverage for cyber risks, coverage disputes should be anticipated as the cyber infrastructure and processes change and grow. By way of example, new risks flow from the potential for loss due to cloud-based computing, the present understanding of what constitutes a "computer virus" may evolve, and criminal or unauthorized data mining may change the meaning of "identity information."

Security Breach Laws

Current state legislation has focused on notification, with 47 states having legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information (National Conference of State Legislators, 2014). Alabama, New Mexico and South Dakota are the only states that do not have security breach legislation (National Conference of State Legislators, 2014). State notification statutes generally require businesses "to publicly acknowledge data breaches" and alert "affected parties to take appropriate precautions" (Schneider, 2009). California was the first state to enact a notification statute, the Security Breach Information Act (Schneider, 2009). The Security Breach Information Act requires businesses to "disclose any [known] breach … of the security of the system … to any resident of California whose unencrypted personal information was … acquired by an unauthorized person" (Cal. Civ. Code § 1798.82).

Many states followed the California statute as a model for their own notification legislation and included an exception to the notification requirement "when the lost data was encrypted (as opposed to plain-text) or to assist law enforcement" (Fisher, 2013). Additionally, many states follow California's statute in declaring that waiver of notification is "contrary to public policy and therefore void and unenforceable" (Fisher, 2013). However, the means and methods of

notification vary among the states, as does the required content of the notice and the penalties for noncompliance.[3]

For example, in New York, "notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired" (N.Y. Gen. Bus. Law § 899-aa). Illinois specifically requires that the following language is included in a notice of breach: "(i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach" (815 ILCS 530/10). Massachusetts requires notice to "include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use" (Mass. Gen. Laws c. 93H, § 3). The Iowa notification statute requires that notice include, at a minimum, all of the following: "(a) A description of the breach of security; (b) The approximate date of the breach of security; (c) The type of personal information obtained as a result of the breach of security; (d) Contact information for consumer reporting agencies; and (e) Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general" (Iowa Code Ann. § 715C.2).

Many states allow written notice, electronic notice or substitute notice, such as notification to major statewide media, if the cost of notice will exceed $250,000 or the affected class of persons is greater than 500,000 (*see e.g.* Illinois, 815 ILCS 530/10; Indiana, Ind. Code Ann. § 24-4.9-3-4; Massachusetts, Mass. Gen. Laws c. 93H, § 3; North Carolina, N.C. Gen. Stat. Ann. § 75-65; Texas, Tex. Bus. & Com. Code Ann. § 521.053; Washington, Wash. Rev. Code Ann. § 19.255.010).

Penalties for noncompliance vary by state. For example, in Texas, a person who violates the notification statute is liable to the state "for a civil penalty of at least $2,000 but not more than $50,000 for each violation," and a violation is considered a deceptive trade practice actionable under the Deceptive Trade Practices-Consumer Protection Act (Tex. Bus. & Com. Code Ann. §§ 521.151, 521.152). If a person or business violates the New York notice statute, the court may impose a civil penalty of the greater of $5,000 or up to $10 per instance of

3. For a comparison of state notification statutes, see Mintz Levin, "State Data Security Breach Notification Laws," July 1, 2014, *www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf*.

failed notification, not to exceed $150,000 (N.Y. Gen. Bus. Law § 899-aa). In Idaho, an "agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system" (Idaho Code Ann. § 28-51-107). In Indiana, the attorney general may bring an action to obtain any or all of the following: "(1) An injunction to enjoin future violations of IC 24-4.9-3; (2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act; (3) The attorney general's reasonable costs in: (a) the investigation of the deceptive act; and (b) maintaining the action" (Ind. Code Ann. § 24-4.9-4-2).

During 2014, nearly half of the states have proposed security breach legislation that would generally amend existing laws. While some of this legislation has failed, in June, Florida passed what has been called "the nation's broadest and most encompassing breach law" in existence. The state's existing security breach law was repealed and replaced with the Florida Information Protection Act of 2014, which requires not only notification of data breaches, but also that companies protect personal information held in electronic form (Greenwald, 2014).

It should be noted that while there is no federal legislation[4] that regulates data security and notification, there are industry-specific statutes, such as the federal Health Insurance Portability and Accountability Act (HIPAA) in health care and the federal Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6810, in the financial services industry (Fisher, 2013). Likewise, while cybercrime is bred in a world without borders, there has been little in the way of development of international law and global regulation.

Cybercrime Activity, Costs and the Courts

Since September 2013, there have been rising numbers of ransomeware attacks using CryptoLocker and other trojans that prevent access to a business's or an individual's stored data. The news today is replete with accounts of modern businesses suffering from compromised technology. Target, the third-largest U.S. retailer, is currently handling the fallout and investigation of a data breach that made headlines in December 2013. Hackers stole about 40 million credit and debit card records, as well as personal information, such as addresses and phone numbers, belonging to about 70 million customers (Hosenball, 2014). Estimates of the costs associated with this breach exceed $1 billion (Webb, 2014).

Neiman Marcus is also investigating a data breach discovered in December 2013. That breach involved 1.1 million credit and debit cards. According to Neiman Marcus, malware was "clandestinely" put into its system and stole

4. The House of Representatives passed the National Cybersecurity and Critical Infrastructure Protection Act of 2013 in July. However, this bill has not been made law.

payment data off cards customers used from July 16, 2013–Oct. 30, 2013 (Harris, Perlroth and Popper, 2014). In January 2007, TJX, the operator of T.J. Maxx and Marshalls stores, announced that cyber hackers accessed certain systems that process and store customer transaction data, thereby potentially compromising the credit card, debit card and bank account information of millions of shoppers at these stores (Evers, 2007). In fact, T.J. Maxx offered that 45.6 million credit and debit card numbers were stolen over a period of 18 months, thereby bestowing upon this incident the dubious title of worst loss of personal data to date (Vijayan, 2007). In 2008, Hannaford Supermarkets reported an interception of 4.2 million credit card and debit card numbers due to a breach of its technology (Consumeraffairs.com, 2008). According to the Identity Theft Resource Center, a nonprofit resource and information provider that tracks, lists and publicizes data breaches, there were at least 330 security breaches resulting in the exposure of more than 8.7 million confidential records in the first five months of 2014 (Identity Theft Resource Center, 2014).

The cost to a company following a data breach can be staggering. For example, within three months after discovering the compromise of its data systems, TJX had already spent $5 million on notifying potentially affected consumers, on hiring outside companies to assist in assessing the extent of stolen information, in handling the associated media frenzy, in defending itself against several lawsuits filed against it in the wake of the announcement, and in fixing and improving its computer systems' security (Vijayan, 2007). Those repercussive costs reached $256 million after nine months (Kerber, 2007). Not only did TJX have to incur millions to conduct internal investigations and repairs, but also it spent significant sums to settle with consumers by offering free credit-monitoring services for three years for those affected customers whose driver's license numbers were compromised, cash reimbursements, shopping vouchers, and a three-day customer appreciation event at which affected consumers received 15% discounts on all goods (Vijayan, 2008). TJX's costs are representative of the type a company may expect following a data breach, although its costs were so massive thanks, in part, to the breadth of the breached information.

Another significant data breach occurred at ChoicePoint, self-described as the "nation's leading provider of identification and credential verification services," in February 2005 (Gatzlaff and McCullough, 2010). Cyber thieves obtained personal information of 140,000 people. In 2006, ChoicePoint agreed to pay a $10 million fine, which was the largest ever levied by the Federal Trade Commission (FTC) (Gatzlaff and McCullough, 2010).

Only about one-third of companies currently have cyber insurance policies; though last year, cyber insurance policies sold to retailers, hospitals, banks and other businesses jumped 20%, according to Marsh LLC (Fernandes, 2014). A recent survey by global consulting firm Towers Watson notes "the sizable number of companies that do not have a liability policy in place," which "speaks to the need for more education and a better understanding of the long-lasting financial and reputational costs that companies face if they don't develop comprehensive risk strategies to thwart cyber-attacks" (Anderson, 2014). Further, an independent

research survey that Zurich sponsored concluded that "few organizations—less than 20 percent, according to survey respondents—have purchased security and privacy insurance specifically designed to cover exposures associated with information security and privacy-related issues" (Anderson, 2014).

Many companies say they plan to purchase cyber policies in the future, but nearly as many say they do not plan to purchase cyber policies due to costs and the policies' exclusions, restrictions and uninsurable risks (Ponemon Institute, 2013). Other reasons for the slow adoption of cyber-risk insurance include: 1) the belief that investment in prevention is better than insurance; 2) limited markets; 3) broker disconnects; and 4) lack of information to make informed decisions (Glascott and Aisen, 2013). Bonner (2012) observed, "The economy, uncertainty about how the policies work, lack of awareness about the exposure and an assumption … that existing general liability or errors and omissions policies will provide coverage" are impediments to the growth of the cyber liability insurance market. This lack of widespread adoption may be a significant problem because the insurance industry depends on spreading risk among a large number of policyholders (Bonner, 2012). Because the majority of companies do not have, and have not had, cyber liability insurance, they have turned to other insurance policies for coverage when a data breach occurs.

The standard CGL policy that the Insurance Services Organization (ISO) drafted provides coverage for damages because of: 1) bodily injury or property damage caused by an "occurrence;" and 2) "personal and advertising injury," which is defined as "injury" arising out of certain enumerated offenses, including the violation of privacy rights. In some cases, 10 or 15 years ago, insureds had mixed success in finding coverage for cyber liability under CGL policies. However, ISO has continued to amend the CGL policy form in an attempt to limit or eliminate coverage for cyber liability claims.

Disputes regarding whether data loss could constitute "property damage" arose under the pre-2001 CGL form, which defined property damage as follows:

> 12. "Property damage" means:
>
> a. Physical injury to tangible property, including all resulting loss of use of that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or
>
> b. Loss of use of tangible property that is not physically injured. All such loss shall be deemed to occur at the time of the "occurrence" that caused it.

ISO Form No. CG 00 01 11 88. Although many courts held that electronic data was not "tangible property," some courts disagreed.[5]

In a seminal case, *America Online, Inc. v. St. Paul Mercury Insurance Co.*, 347 F.3d 89 (4th Cir. 2003), the Fourth Circuit held that computer data, software and systems were not "tangible" property under commercial general liability policy provisions covering liability for property damage. Further, the court held that an impaired property exclusion, which denied coverage for loss of use of tangible property that was not physically damaged, excluded coverage for damage to the claimants' software, including operating systems, because there was no demonstration or claim that the physical or tangible components of any computer were damaged.

The claimants—customers of the insured, an Internet service provider—had alleged that the insured's proprietary software package caused physical damage to their computers, computer data and software systems. St. Paul Mercury Insurance Company, the primary insurer, denied coverage because the claimed damages were not "property damage" as defined by the policy and were otherwise restricted by the "impaired property" exclusion. The policy provided that St. Paul would "pay amounts the insured is legally required to pay as damages for covered … property damage." Property damage was defined as "physical damage to "tangible" property of others … or loss of use of tangible property of others that isn't physically damaged." The "impaired property" exclusion provided that St. Paul was not obligated to cover "property damage to impaired property, or to property which isn't physically damaged" resulting from either "faulty or dangerous products or completed work" or "a delay or failure in fulfilling the terms of a contract or agreement."

The insured contended that the claims against it were physical damage to tangible property, as covered by St. Paul's policy, making three arguments in support of this contention. First, it argued that because the claimants alleged damage to "computers," they have alleged "physical damage to tangible property." Second, it argued that because software involves the arrangement of atoms on computer disks, software has a physical property, and so damage to software is "physical damage to tangible property." Third, it argued that "tangible," as defining property damage, was ambiguous and must be construed in the insured's favor. St. Paul contended that the underlying complaints alleged two types of harm: 1) interference with non-AOL software; and 2) loss of data and information; and that neither of these injuries were covered because computer software and data are simply information and ideas stored in electronic form, and damage to them is not loss of use of computer hardware or "tangible property."

The court focused on the insured's second argument, finding that the claimants were actually alleging damage to computer software, not the physical "computers," and that "tangible" would be construed in accordance with its usual

5. Compare *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003) with *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 2002-NMCA-054, 132 N.M. 264, 266, 46 P.3d 1264, 1266 (N.M. 2002).

and ordinary meaning. Thus, considering whether damage to software was physical damage to tangible property, the court questioned whether the data, information and instruction—which are codified on a hard drive, as opposed to the physical magnetic material on the hard drive—were tangible property. The court stated that if a hard drive were physically scarred so that it could no longer record data, information or instructions, then damage would be physical. But where the arrangement of the data and information stored on the hard drive becomes disordered, or the instructions conflicted, the physical capabilities of the hard drive would not be compromised. The court explained that instructions to the computer and the data and information processed by it were "abstract ideas in the minds of the programmer and the user." Loss of or damage to software would, therefore, damage "to the idea, its logic, and its consistency with other ideas and logic," and would not render the computer hardware unusable or create physical damage to tangible property.[6]

Turning to the "impaired property" exclusion, the court took up the insured's argument that even in the absence of physical damage to tangible property, it was exposed to property damage claims because "property damage" was defined by the policy to include loss of use of tangible property and that the exclusion would not apply to bar such coverage. The court found that this argument ignored the language of the exclusion, which limited coverage for loss of use of tangible property "which isn't physically damaged" by the insured's faulty product. Because there was no physical damage to the claimants' property, the court further rejected the insured's argument for covering loss of use.

In contrast to *America Online*, in *Computer Corner, Inc. v. Fireman's Fund Insurance Co.*, 2002-NMCA-054, 132 N.M. 264, 266, 46 P.3d 1264, 1266 (N.M. 2002), the New Mexico Court of Appeals held that computer data stored on a hard drive constituted "tangible property." The appeals court affirmed the trial court's decision that computer data "was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed" and that "computer data is tangible property." The court further concluded that the loss of data from reformatting a customer's computer hard drive was neither expected nor intended and, therefore, the intentional acts exclusion did not preclude coverage. Additionally, the court determined that the customer's lost files due to the reformatting of the hard drive were not "your product" or "your work" within the meaning of the CGL exclusions because the property that was lost existed prior to and apart from any service or parts provided in repairing the computer. The court also concluded that the "impaired property" exclusion was "too vague and indefinite to be enforceable."

6. *America Online*, 347 F.3d at 95-96 (citing *Lucker Mfg. v. Home Ins. Co.*, 23 F.3d 808, 819 (3d Cir. 1994) (instructions, data and information are abstract and intangible); *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (holding that, in an insurance context, computer data has no physical substance, it is not tangible property).

The ISO responded to the uncertainty among the insurance industry and the courts regarding whether electronic data was "tangible property" by amending the definition of "property damage" to explicitly state that electronic data is not tangible property. Since 2001, the CGL definition of "property damage" has included the following provision:

> For the purposes of this insurance, *electronic data is not tangible property*.
>
> As used in this definition, 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. (ISO Form No. CG 00 01 10 01 (emphasis added)).

However, this amendment did not completely eliminate coverage for claims involving computer programs and software. Although liability for damage to data itself was not covered under the 2001 CGL policy, claims seeking damages due to the loss of use of tangible property caused by damage to data could still be covered. In *Eyeblaster, Inc. v. Federal Insurance Co.*, 613 F.3d 797 (8th Cir. 2010), the Eighth Circuit held that a general liability policy provided coverage for claims of damage to a third-party computer user's computer, software and data, and that an "impaired property" exclusion did not bar coverage. The court also found coverage under a technology errors and omissions policy.

In *Eyeblaster*, the insured was a worldwide online marketing management company that provided online advertising services. The claimant sued the insured, alleging that his computer was infected with a spyware program after visiting one of the insured's websites. He alleged this caused his computer to freeze up, as well as caused software damage and data loss. The insurer denied coverage under the general liability policy on the basis that to the extent that the claim against the insured alleged property damage, it did not allege that the property damage was caused by an accident or occurrence as the policy required. With respect to the errors and omissions policy, the insurer denied coverage, asserting that the claimant had not alleged that the insured had committed a wrongful act in connection with a product failure or in performing or failing to perform its service.

As to the general liability coverage, the court found that the claimant had accused the insured of "intentionally accessing a protected computer without authorization, knowingly committing deceptive trade practice violations intending to deceive the user and intentionally installing unwanted spyware onto a user's computer." Despite the allegations of direct injury to the operation of the claimant's computer, there were not allegations of damage to the hardware itself. The court explained that the complaint would have had to state a claim for

physical injury to the hardware in order for the insured to be covered for "physical injury to tangible property." However, considering the insurer's duty under the second part of the definition of "property damage," which obligated the company to provide coverage if the insured was alleged to have caused the "loss of use of tangible property that is not physically injured," and the fact that the complaint alleged the "loss of use" of the user's computer, the court concluded that the allegations establish a claim that fell within the coverage grant afforded by the general liability policy.

Finding coverage under the general liability policy, the court then considered whether the "impaired property" exclusion applied to negate coverage. The exclusion provided that the insurance did not apply to property damage to impaired property or property that had not been physically injured if the damage arose out of any defect, deficiency, inadequacy or dangerous condition in the insured's product or work. The court held that the user's computer could not be considered "impaired property" because the insurer failed to present any evidence to prove that the computer could be restored to use by removing the insured's product or work from it. In other words, the damage caused by the spyware was done, and removing the spyware would not repair the damage.

Turning to the errors and omission policy, the court considered whether the insurer met its burden of demonstrating that the insured was alleged to have acted with the requisite intent. The policy obligated the insurer "to pay loss for financial injury caused by a wrongful act that resulted in the failure of the insured's product to perform its intended function or to serve its intended purpose." The policy specifically covered intangible property such as software, data and other electronic information. The policy defined "wrongful act" as an error, an unintentional omission or a negligent act. The court found coverage under the errors and omissions policy, stating that although the complaint alleged that the insured acted intentionally in installing damaging products on the claimant's computer, the insurer did not produce evidence that doing so was intentionally wrongful.

In 2004, the ISO made another amendment to the CGL form, an exclusion that was intended to eliminate coverage for loss of use claims related to electronic data:

> 2. Exclusions
>
> This insurance does not apply to:
>
> * * *
>
> q. Electronic Data
>
> 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 (ISO Form No. CG 00 01 12 04).

In *Recall Total Information Management, Inc. v. Federal Insurance Co.*, No. X07CV095031734S, 2012 WL 469988 (Conn. Super. Ct. Jan. 17, 2012), *aff'd* 147 Conn. App. 450 (Conn. Ct. App. Jan. 14, 2014), the court considered a loss of electronic media and distinguished between the tapes on which the information was stored and the information itself. Federal Insurance Company and Scottsdale Insurance Company issued CGL policies to Recall Total Information Management, Inc. Recall entered into a vital records storage agreement with IBM to transport and store IBM electronic media. Recall subsequently entered into a secure transport subcontract with Executive Logistic Services, LLC (Ex Log) to transport the IBM media. Under the contract, Ex Log was required to maintain general liability insurance and name Recall as an additional insured.

In February 2007, an IBM cart containing electronic media fell out of an Ex Log transport van near a highway exit ramp. The cart and approximately 130 computer data tapes containing personal information for more than 500,000 IBM employees were stolen by an unknown person. IBM wrote to Recall claiming damages as a result of the loss of the tapes. Recall entered into a settlement agreement with IBM for the full amount claimed and demanded indemnification from Ex Log. Recall and Ex Log provided notice of the claim to Federal Insurance Company and Scottsdale Insurance Company. Federal and Scottsdale denied coverage, stating that their CGL policies did not cover the loss of the IBM tapes.

In their motion for summary judgment, the insurers argued that Recall's claims were not covered under the policies because "they do not qualify as property damage as the amounts paid to IBM are not for the loss of use of tangible property." Both policies defined property damage as "damage to tangible

property." The court agreed with the insurers that "electronic data is not tangible property and that electronic data is explicitly excluded from the definition of tangible property." The policies stated: "Tangible property does not include any software, data or other information that is in electronic form." The claims arose from the preventative measures IBM took because of the theft, or loss of use, of the data on the tapes—not the tapes themselves. The court held that this was not damage to tangible property.

Recall also argued that the policies provide coverage pursuant to the personal injury section of the policy. "Personal injury" was defined as "injury, other than bodily injury, property damage or advertising injury, caused by an offense of … [e]lectronic, oral, written or other publication of material that … violates a person's right of privacy." The court determined that the term "publication" generally refers to communication to a third person, and there was no coverage under the personal injury provision because there was no evidence of communication to a third party. The court, therefore, granted the insurers' motions for summary judgment. As noted above, this decision was affirmed by the Connecticut Appellate Court on Jan. 14, 2014 (*Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 147 Conn. App. 450 (Jan. 14, 2014)). On March 5, 2014, the Supreme Court of Connecticut granted plaintiffs' petition for certification for appeal from the Appellate Court, limited to the following issue: "Did the Appellate Court properly affirm the trial court's summary judgment entered in favor of the defendants?" (*Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 311 Conn. 925 (2014)). The parties' briefing deadline was scheduled for July 23, 2014.

A data breach coverage case that further defines the third-party insurance coverage landscape involves the Sony data breach that occurred in April 2011. In this breach, hackers accessed data, which included personal identification and financial information, for more than 101 million users on Sony's online video games. Sony was hit with another breach in early October 2011 that involved the usernames and passwords of about 93,000 customers. Sony gave notice of the claims and expected claims to Zurich, which disclaimed coverage and filed a declaratory judgment action in the Supreme Court of the State of New York (*Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011 (N.Y. Sup. Ct. Sept. 27, 2011)). In its complaint for declaratory judgment, Zurich alleged that it was not obligated to defend or indemnify Sony for the claims asserted in the class action complaints, Canadian class action complaints, miscellaneous claims or potential future actions by any state attorney general. Both Zurich's primary and excess policies provided coverage for "bodily injury" and "property damage" caused by an "occurrence" under Coverage A and coverage for "personal and advertising injury" under Coverage B. Zurich's Canadian policy provided coverage for "bodily injury," "property damage," "advertising injury" and "personal injury liability."

According to Zurich, the claims asserted in the underlying class actions and other miscellaneous claims arising out of the cyber attacks and the unauthorized access to and theft of the named plaintiffs' and class members' personal identification and financial information do not assert claims for "bodily injury,"

"property damage" or "personal and advertising injury," and, therefore, no coverage existed under its primary or excess policy. As to its excess policy, Zurich contended that its obligation to provide its quota share excess coverage to Sony is conditioned on the exhaustion of all underlying insurance. In regard to the Canadian policy, Zurich alleged that it was subject to a self-insured retention and applicable definitions, exclusions and endorsements, and, therefore, it had no duty to defend or indemnify Sony.

After arguments on cross-motions for summary judgment, Judge Oing ruled from the bench on Feb. 21, 2014, that Sony failed to establish that the claims fell within the Coverage B insuring provision. Judge Oing discussed that courts addressing the "personal injury" definition generally have held that the insured must have conducted or perpetrated the wrongful act, *i.e.*, the publication. According to the court, the "in any manner" language referred to the way in which the material is publicized, not who publicized it. Moreover, the court held that when reading the policy as a whole, it did not provide coverage for acts of a third party. The court determined that the "invasion of privacy" section of the "personal injury" definition required that the insured committed the publication. Judge Oing stated that interpreting the language to expand liability to publication by third parties would expand the policy coverage beyond what the insurers had agreed. Therefore, because the publication at issue was a publication perpetrated by third-party hackers, and not by Sony, the court concluded that there was no coverage for the claims.

In 2011, the Eleventh Circuit Court of Appeals issued a decision in *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, No. 11-11781, 2011 WL 4509919 (11th Cir. Sept. 30, 2011) in connection with a claim for coverage for claims against the insured alleging violations of the federal Fair and Accurate Credit Card Transaction Act that may have a bearing on claims for cyber torts under Coverage B. In *Creative Hospitality*, these claims were based on the insured's issuance of receipts revealing more than five digits of a customer's credit card number or the card's expiration date. The Eleventh Circuit held that Coverage B of the CGL policy did not provide coverage because the issuance of a credit card receipt did not constitute a "publication" as required under the policy's coverage for personal and advertising injury. Rejecting the insured's argument that the policy language of "publication in any manner" was ambiguous, the court applied the dictionary definition of "publication" as previously used by the Florida Supreme Court in *Penzer v. Transp. Ins. Co.*, 29 So. 3d 1000, 1005 (Fla. 2010). "Publication" means "communication (as of news or information) to the public: public announcement" or "the act or process of issuing copies … for general distribution to the public." The court determined that the receipt is a "contemporaneous record of a private transaction between [insured] and the customer, and [insured] neither broadcasted nor disseminated the receipt or the credit card information to the general public." The insured provided only the receipt to the customer, who already knew the card information. Therefore, the court concluded that providing a customer with a contemporaneous record of a retail transaction does not involve dissemination of information to the general public and does not constitute publication under the

policy. Further, the court rejected the insured's argument that the phrase "in any manner" expands the definition of "publication" to include providing a written receipt. Agreeing with the district court, the Appeals Court ruled that the phrase "in any manner" simply expands the categories of publication, but it does not change the meaning of the term "publication."

Despite the ISO amendments over the past 15 years, courts continue to be asked to resolve issues involving cyber claims under CGL policies. One court recently held that coverage for "loss of use" of property that is not itself physically damaged can be implicated even if a company's liabilities are primarily focused on data or "non-tangible" property. In *Collective Brands Inc. v. National Union Fire Ins. Co. of Pittsburg, Pa.*, No. 11-4097, 2013 WL 66071 (D. Kan. Jan. 4, 2013), the court determined that claims for alleged wrongful customer communications, including calls and texts, were potentially covered under "property damage" provisions because customers could have suffered "loss of use" of their phones. The policies defined "property damage" to include both physical injury to tangible property, as well as the "loss of use of tangible property that is not physically injured." The court ultimately concluded, however, that the "violation of communication statutes" exclusion precluded coverage. In *Liberty Corp. Capital Ltd. v. Sec. Safe Outlet Inc.*, 937 F. Supp. 2d 891 (E.D. Ky. 2013), however, the court held that a customer list, whether electronic or a paper copy, did not constitute "tangible property" under the "property damage" provision in the CGL policy and, therefore, the alleged misappropriation of the list was not covered under the policy. The underlying action involved a claim against the insured by a competitor for misappropriation of trade secrets—the competitor's customer database, which included customer names and emails. The competitor's former IT employee started working for the insured and shared the competitor's customer database with the insured. The court determined that the electronic copy of the customer database had "no physical form or characteristics," and, therefore, "it simply does not fall within the definition of 'tangible property.'" Further, the court noted that the terms of the policy "clearly and unequivocally exclude 'electronic data,' including information stored, created or used on computer software, from the definition of 'tangible property.'"

In another recent case, *Hartford Casualty Insurance Co. v. Corcino & Associates*, No. CV 13-3728 (C.D. Cal. Oct. 7, 2013), the court determined a CGL policy provided coverage under Coverage B for a hospital data breach that compromised confidential medical records of approximately 20,000 patients. In two underlying class actions, the plaintiffs sought statutory damages under the California Confidentiality of Medical Information Act and the California Lanterman-Petris-Short Act. The hospital sought coverage under Coverage B of Hartford's policy, which provided coverage for "those sums that the insured becomes legally obligated to pay as damages because of … 'personal and advertising injury'" and defined "personal and advertising injury" to include "[o]ral, written or electronic publication of material that violates a person's right to privacy." Hartford filed a declaratory judgment action, seeking a declaration that the statutory relief sought by the claimants was precluded under an exclusion for

"Personal and Advertising Injury … [a]rising out of the violation of a person's right to privacy created by any state or federal act." The hospital moved to dismiss on the grounds that the exclusion did not apply because the claimants sought remedies for breaches of privacy rights that were not "created by any state or federal act," but which "exist under common law and the California state Constitution." The court agreed with the insured and concluded that the right to medical privacy was not *created* by statute; it was simply codified by statute, and is an existing constitutional and common law right.

In September 2013, the ISO filed for approval with state insurance authorities of new wording for CGL policies that would seek to exclude coverage for cyber claims such as data breaches. The CGL exclusion (effective as of May 2014) is titled "Exclusion – Access or Disclosure of Confidential or Personal Information and Data-Related Liability – with Limited Bodily Injury Exception" and precludes coverage for injury:

> "arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."

The exclusion continues and explains that it applies even if damages are claimed for notification costs; credit monitoring expenses; forensic expenses; public relations expenses; or any other loss, cost or expense incurred by the insureds or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.

As noted above, insurers have developed new coverage forms that afford data breach coverage. As a general matter, cyber coverage falls into two categories, much like the traditional property liability policies: 1) forms that offer coverage for first-party risks, such as cybercrime, viruses and system malfunctions; and 2) forms that insure against third-party risks, such as data breach claims and claims for the infection of outside systems. Depending on the coverage selected, such a policy may provide indemnity to businesses forced to investigate and respond to notifications of a data breach, to close any technology "open doors" to prevent future breaches, and to recreate lost or altered information. The coverage may further cover attendant costs, such as offering credit monitoring to affected parties whose personal information may have been stolen, or attorneys' fees incurred to defend against a regulatory action over private information violations. Claim payouts reportedly average $2.4 million per data breach (Foy, 2013). The largest component of the claim payout is cost of legal defense—$500,000 per claim on average—and the second largest component is crises services—forensics, notification, call center and legal counsel (Foy, 2013).

Currently available coverages have names such as Network Security Liability, Privacy Liability and Data Loss Liability Coverage forms. Businesses considering cyber coverage generally work closely with brokers to determine the scope of

coverage that they may already have, which may include Directors & Officers coverage (*e.g.*, for failure to make proper disclosures of security breaches) or Errors & Omissions coverage (*e.g.*, for cyber losses that may be the result of negligence of the insured in providing professional services).

As evidence of the global nature of cyber risk, Lloyd's of London insurer Kiln started offering cyber insurance in March 2011 to small- and medium-sized online retailers (Insurance Journal, *Kiln*, 2011). In the U.S., The Hartford launched data breach coverage for small businesses, offered as an endorsement to the company's business owner's policy (Insurance Journal, *The Hartford*, 2011). Data breach coverage includes:

1. First-party coverage for response expenses, including legal and forensic services, notification expenses, crisis management and good faith advertising expenses.

2. Third-party coverage for defense and liability, including defense costs, civil awards, settlements or judgments that an insured is legally obligated to pay.

3. Access to a secure breach preparedness website that offers tips and guidelines for safeguarding customer, patient and employee information; preparing a data breach incident response plan; and regulatory requirements by state.

4. Consultative services, including help with breach notifications and credit monitoring for victims of identity theft or fraud, if warranted.

Hiscox also offers a Privacy and Data Breach policy in "six compatible coverage modules" outlined here:

1. Covers both the first-party and third-party liabilities arising from a data breach event.

2. Covers defense cost and indemnity, whether it's a claim for a statutory violation, regulatory investigation, negligence or breach of contract.

3. Provides full limits for forensic costs incurred in the defense of a covered claim.

4. Provides full limits for credit or identity protection costs as part of a covered liability judgment, award or settlement, with no cap on cost per individual and no limitation on number of years provided.

5. Covers both negligence and breach of contract claims arising out of a breach of credit card details, including coverage for a breach of a merchant agreement and coverage for indemnified PCI fines.

6. Provides both complimentary pre-loss breach prevention services (Breachprotection.com) and complimentary breach responses services, including one hour with a data breach coach to assist in responding to a breach event (Hiscox eRisk Hub®) (*Privacy Data-Breach Insurance*, 2014).

Travelers offers a claims-made third-party CyberRisk liability policy with the following provision:

> THIRD PARTY LIABILITY INSURING AGREEMENTS
>
> A. NETWORK AND INFORMATION SECURITY LIABILITY
>
> The Company will pay on behalf of the Insured, Loss for any Claim, other than a Regulatory Claim, first made during the Policy Period or, if exercised, during the Extended Reporting Period or Run-Off Extended Reporting Period, for a Network and Information Security Wrongful Act.
>
> Network and Information Security Wrongful Act means any actual or alleged:
>
> 1. failure to prevent unauthorized access to, or use of, electronic or non-electronic data containing Identity Information;
>
> 2. failure to prevent the transmission of a Computer Virus through a Computer System into a computer network, any application software, or a computer operating system or related network, that is not rented, owned, leased by, licensed to, or under the direct operational control of, the Insured Organization;
>
> 3. failure to provide any authorized user of the Insured Organization's website or Computer System with access to such website or Computer System; or

> 4. failure to provide notification of any actual or potential unauthorized access to, or use of, data containing private or confidential information of others if such notification is required by any Security Breach Notification Law, by, or asserted against, an Insured Person, in his or her capacity as such, or the Insured Organization (Travelers CyberRisk Policy, 2014).
>
> Philadelphia Insurance Companies offers a similar provision:
>
> E. Network Security and Privacy Liability Coverage
>
> We shall pay on your behalf those amounts, in excess of the applicable deductible shown in the Declarations, which you are legally obligated to pay as damages and claim expenses arising from your acts, errors or omissions, or from acts, errors or omissions of others for whom you are legally responsible, including outsourcers or vendors, provided such acts, errors or omissions follow a security breach or privacy breach and occur on or after the retroactive date set forth in the Declarations and before the end of the policy period (Philadelphia Insurance Companies, 2014).

Although these cyber policy provisions afford coverage for cyber risks, insurance professionals and their counsel should be mindful of the potential for coverage disputes. Both insureds and insurers must understand the specific risk for which coverage is sought and ensure that coverage is appropriate for the insured's business. Otherwise, they may face exposure that was not anticipated at the time of underwriting the risks (Glascott and Aisen, 2013). One area in which disputes may arise involves cloud computing, as coverage may depend on whether the security breach occurs on the insured's own systems or "in the cloud" (Bublitz, 2010). In the context of wording of a policy affording coverage for a company's own acts and the acts of others for whom the company is legally responsible, if the agreement between the company and the cloud provider does not delineate that the company is legally responsible for the cloud provider's act, there may be a factual question that complicates the coverage determination.

Another coverage issue relating to cloud computing may arise in the context of the coverage for "others for whom you [the insured] are legally responsible," based on the requirement that "such acts, errors or omissions follow the security breach." In this instance, a factual dispute may lie in determining the place and time the cloud-based security breach occurred and whether the cloud provider had control over that aspect of the securitization of the data. This issue should not arise where the policy wording applies only to a failure by or asserted against an insured person or organization. However, where there is room for an argument to be made that bootstraps the conduct of the policyholder to that of the third-party cloud storage provider, that argument will assuredly be made.

Data breaches such as those involved in the Target, Sony and TJX losses may also generate coverage under cyber-risk policies in that context. When a data

breach involves obtaining usernames and passwords of customers, hackers can use username and password information to try to obtain bank information, credit card numbers and other information. Username and password information itself may not be "identity information" as that term is used in cyber-risk policies; however, it provides hackers with an avenue to obtain that information. Issues relating to this distinction may turn on whether this type of breach is a "failure to prevent unauthorized access to" electronic data containing "identity information."

Another issue that may arise involving "identity information" provisions is exemplified by *Creative Hospitality Ventures Inc. v. United States Liability Ins. Co.*, 444 F. App'x 370, (11th Cir. 2011). In *Creative Hospitality*, coverage issues arose concerning whether printing of the expiration date and last five digits of a customer's credit card constituted a data breach. Courts will need to consider whether this type of breach is sufficient to constitute a "failure to prevent unauthorized access to" electronic data containing "identity information."

The construction of the term "computer virus" may also be the subject of attacks by policyholders that seek to expand the scope of coverage beyond that intended by the policy drafters. In both *America Online, Inc. v. St. Paul Mercury Insurance Co.* and *Eyeblaster Inc. v. Federal Insurance Co.*, the courts considered whether loss of computer use after visiting an insured's website or using an insured's product constituted a covered breach. In these cases, the insured's products did not contaminate users' computers through actual computer viruses, but rather impaired computer use with pop-up ads, hijacked browsers, random error messages and software corruption. Whether such acts constitute a "failure to prevent the transmission of a computer virus" may also give rise to coverage disputes.

The advent and increasing popularity of insurance coverage for cyber risks is bound to present challenges for insurance professionals and their counsel. However, the same sound principles of good faith claim handling that are routinely adhered to throughout the insurance industry in connection with traditional risks insured under general liability and other first-party property and third-party liability policies will provide insurance professionals with ample tools to solve new disputes that may arise.

Conclusion

As the structure and processes of cyber space expands, so will the risks. As with all insurable losses, the unintended consequences drive the need for insurance coverage. With the Internet creating ever-expanding opportunity for economic growth, intellectual advancement, social interaction and entertainment, it will be incumbent on insurance regulators to learn about and understand the extremely delicate balance between what should and should not be covered. Unlike well-established insurance products, which have vast and dependable actuarial predictive models—be they life, health and disability products, or

property and casualty products—there is virtually no predictive modeling data for the virtual world. What regulators can readily understand and must thoughtfully consider is that while exposures to cyber liability increase, so do cyber security and related protective products. Of course, insurers that write cyber liability policies are no more guarantors of the policyholders' work or products than are the insurers who write general liability coverage. Thus, it is incumbent on regulators to understand both the breadth, depth and scope of coverage the carriers intend to provide, as well as the basis for the pricing.

While the development of cyber space can be viewed as the dawn of a new era, the benefit of the availability of insurance coverage for cyber risks is rooted in prehistoric times. Then, as now, the purpose of insurance was to limit risk. Pre-humans appreciated that hunting in packs reduced the risk of injury faced by a loan hunter. In the Middle Ages, artisans belonged to guilds and paid dues that would fund the rebuilding of property in the event of fire or flood and would support a widow in the event of death. Risk spreading is part of the bedrock of today's global economy, and all insurance regulators are responsible for the domains they regulate. Risk is spread from those injured to the insurers and the reinsurers, and as the market needs capital to sustain itself, it is ultimately spread through premiums back to the policyholders. Financial reverberations—from natural disasters, such as Hurricane Katrina; economic crises, such as the subprime mortgage and credit default swap fiasco; and health and environmental exposures, such as asbestos and pollution—are felt for decades.

It would be imprudent to expect that cyber space will not generate comparable exposures that transcend decades and international boundaries. The responsibility of insurance regulators working in the sphere of new insurance products developed to shift certain risks arising out of cyber liability is one on which many will depend, and its importance cannot be underestimated.

References

America Online, Inc. v. St. Paul Mercury Insurance Co., 347 F.3d 89 (4th Cir. 2003).

Anderson, R.D., 2014. "Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz," *Tort Trial & Insurance Law Journal*, 49(2): 529.

Bonner, L., 2012. "Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches," *Washington University Journal of Law & Policy*, accessed at *http://digitalcommons.law.wustl.edu/wujlp/vol40/iss1/7/*.

Bublitz, E., 2010. "Catching the Cloud: Managing Risk When Utilizing Cloud Computing," accessed June 5, 2014, at *www.propertycasualty360.com/2010/08/30/catching-the-cloud-managing-risk-when-utilizing-cloud-computing*.

California Civil Code § 1798.82. Person or business who owns or licenses computerized data including person information; breach of security of system; disclosure requirements (effective July 1, 2003; amended Jan. 1, 2014).

Computer Corner, Inc. v. Fireman's Fund Ins. Co., 2002-NMCA-054, 132 N.M. 264, 266, 46 P.3d 1264, 1266 (N.M. 2002).

ConsumerAffairs.com, 2008. "Hannaford Bros. Faces Class Action Over Data Breach: Hacker Broke Into Grocery Chain's System," accessed June 5, 2014, at *www.consumeraffairs.com/news04/2008/03/hannaford_data2.html*.

Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co., No. 11-11781, 2011 WL 4509919 (11th Cir. Sept. 30, 2011).

Evers, J., 2007. "T.J. Maxx Hack Exposes Consumer Data," *CNET*, accessed June 5, 2014, at *http://news.cnet.com/T.J.-Maxx-hack-exposes-consumer-data/2100-1029_3-6151017.html*.

Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797, 799 (8th Cir. 2010).

Fernandes, D., 2014. "More Firms Buying Insurance for Data Breaches," *The Boston Globe*, Feb. 17, 2014.

Fisher, J.A., 2013. "Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach," William & Mary Business Law Review, 4(1): 215, 224.

Foy, M.S., 2013. "The Worm That Byte Me: Emerging Issues in Insurance Coverage for Data Breaches, Invasion of Privacy Claims, and Cyber Crimes," *Defense Research Institute*, December 2013.

Gatzlaff, K.M. and K.A. McCullough, 2010. "The Effect of Data Breaches on Shareholder Wealth," *Risk Management and Insurance Review*, 13(1): 61-83.

Glascott, M.T. and A.J. Aisen, 2013. "The Emperor's New Clothes and Cyber Insurance," *FDCC Quarterly*, accessed at *www.thefederation.org/documents/22.The%20Emperors%20New%20Clothes.pdf*.

Greenwald, J., 2014. "Florida governor signs sweeping data security breach bill into law, *Business Insurance*, accessed at *www.businessinsurance.com/article/20140624/NEWS07/140629916/florida-governor-signs-sweeping-data-security-breach-bill-into-law?tags=|299|69|80|87|329|305|303*.

Harris, E., N. Perlroth and N. Popper, 2014. "Neiman Marcus Data Breach Worse Than First Said," *The New York Times*, accessed at *www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html? r=0*.

Hosenball, M., 2014. "Target Vendor Says Hackers Breached Data Link Used for Billing," *Reuters*, accessed June 5, 2014, at *www.reuters.com/article/2014/02/06/us-target-breach-vendor-idUSBREA1523E20140206*.

Identity Theft Resource Center, 2014. "2014 Data Breach Stats," accessed June 5, 2014, at *www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html*.

Information is Beautiful, 2014. "World's Biggest Data Breaches," accessed at *www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*.

Insurance Journal, 2011. "Kiln, Lockton Team Up to Offer Cyber Coverage to UK Retailers," accessed at *www.insurancejournal.com/news/international/2011/03/02/188592.htm*.

Insurance Journal, 2011. "The Hartford Launches Data Breach Coverage for Small Businesses," accessed at *www.insurancejournal.com/news/national/2011/09/19/216404.htm*.

ISO Form No. CG 00 01 10 01.

ISO Form No. CG 00 01 12 04.

Kerber, R., 2007. "Cost of Data Breach At TJX Soars To $256m: Suits, Computer Fix Add To Expenses," *The Boston Globe*, accessed *at www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m*.

Liberty Corp. Capital Ltd. v. Sec. Safe Outlet Inc., 937 F. Supp. 2d 891 (E.D. Ky. 2013).

Mintz, L., 2014. "State Data Security Breach Notification Laws," accessed at *www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf*.

National Conference of State Legislators, 2014. "Security Breach Notification Laws," accessed at *www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*.

Philadelphia Insurance Companies. "Cyber Security Liability Coverage Form," accessed June 5, 2014, at *www.phly.com/Files/CyberSecurityLiabilityPolicy_Admitted31-932.pdf*.

Ponemon Institute LLC, 2013. "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," accessed at *http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf*.

Privacy Data-Breach Insurance. Accessed June 5, 2014 at *www.hiscoxusa.com/broker/usa_privacy_data_breach.htm*.

Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 311 Conn. 925 (2014).

Recall Total Information Management, Inc. v. Federal Insurance Co., No. X07CV095031734S, 2012 WL 469988, at *1 (Conn. Super. Ct. Jan. 17, 2012), *aff'd* 147 Conn. App. 450 (Conn. Ct. App. Jan. 14, 2014).

Robinson, T., 2014. "Breaches, malware to cost $491 billion in 2014, study says," accessed June 5, 2014, at *www.scmagazine.com/breaches-malware-to-cost-491-billion-in-2014-study-says/article/339167/*.

SC Magazine, March 2014. "Threat Stats," accessed June 5, 2014, at *www.scmagazine.com/march-2014-threat-stats/slideshow/1852/#0*.

Schneider, J.W., 2009. "Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data," *Boston University Journal of Science & Technology Law*, 15: 279, 282.

Symantec, Ponemon Institute LLC, 2013. "2013 Cost of Data Breach Study: Global Analysis," *accessed at https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf*.

Travelers CyberRisk Policy. Accessed June 5, 2014, at *www.travelers.com/business-insurance/management-professional-liability/documents/CYB-3001.pdf*.

Vijayan, J., 2008. "Hannaford Hit By Class-Action Lawsuits In Wake Of Data-Breach Disclosure," *Computerworld*, accessed June 5, 2014, at *www.computerworld.com/s/article/9070281/*.

Vijayan, J., 2007. "TJX Data Breach: At 45.6M Card Numbers, It's The Biggest Ever," *Computerworld*, accessed June 5, 2014, at *www.computerworld.com/s/article/9014782/TJX_data_breach_at_45.6M_card_numbers_it_is_the_biggest_ever*.

Webb, T., 2014. "Analyst sees Target data breach costs topping $1 billion," accessed at *www.twincities.com/business/ci_25029900/analyst-sees-target-data-breach-costs-topping-1*.

Willhite, J., 2013. "On Alert Against Cybercrime," *The Wall Street Journal*, Aug. 13, 2013.

Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011 (N.Y. Sup. Ct. Sept. 27, 2011).

Journal of Insurance Regulation

Guidelines for Authors

Submissions should relate to the regulation of insurance. They may include empirical work, theory, and institutional or policy analysis. We seek papers that advance research or analytical techniques, particularly papers that make new research more understandable to regulators.

Submissions must be original work and not being considered for publication elsewhere; papers from presentations should note the meeting. Discussion, opinions, and controversial matters are welcome, provided the paper clearly documents the sources of information and distinguishes opinions or judgment from empirical or factual information. The paper should recognize contrary views, rebuttals, and opposing positions.

References to published literature should be inserted into the text using the "author, date" format. Examples are: (1) "Manders et al. (1994) have shown. . ." and (2) "Interstate compacts have been researched extensively (Manders et al., 1994)." Cited literature should be shown in a "References" section, containing an alphabetical list of authors as shown below.

Cummins, J. David and Richard A. Derrig, eds., 1989. *Financial Models of Insurance Solvency*, Norwell, Mass.: Kluwer Academic Publishers.

Manders, John M., Therese M. Vaughan and Robert H. Myers, Jr., 1994. "Insurance Regulation in the Public Interest: Where Do We Go from Here?" *Journal of Insurance Regulation*, 12: 285.

National Association of Insurance Commissioners, 1992. *An Update of the NAIC Solvency Agenda*, Jan. 7, Kansas City, Mo.: NAIC.

"Spreading Disaster Risk," 1994. *Business Insurance,* Feb. 28, p. 1.

Footnotes should be used to supply useful background or technical information that might distract or disinterest the general readership of insurance professionals. Footnotes should not simply cite published literature — use instead the "author, date" format above.

Tables and charts should be used only if needed to *directly support* the thesis of the paper. They should have descriptive titles and helpful explanatory notes included at the foot of the exhibit.

Papers, including exhibits and appendices, should be limited to 45 double-spaced pages. Manuscripts are sent to reviewers anonymously; author(s) and affiliation(s) should appear only on a separate title page. The first page should include an abstract of no more than 200 words. Manuscripts should be sent by email in a Microsoft Word file to:

Cassandra Cole and Kathleen McCullough
jireditor@gmail.com

The first named author will receive acknowledgement of receipt and the editor's decision on whether the document will be accepted for further review. If declined for review, the manuscript will be destroyed. For reviewed manuscripts, the process will generally be completed and the first named author notified in eight to 10 weeks of receipt.