Ways the Virtual World Rocks the Real World: 
Understanding the Nuances of Information Security Risk 
and the Insurance Market Response

By: Angela Elbert, Seth Lamden, Theodore Howard, 
Mary Guzman & Suzanne Whitehead

I. Background

There has been much news in recent times relating to cyber and privacy exposure. Cyber attacks increased 42% in 2012 and have only accelerated in 2013.2 Outgoing FBI director Robert Mueller recently stated: “There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.”3 In a recent New York Times article, for example, a consultant for a policy group in Washington D.C. specializing in computer security issues, was quoted as saying “We hit rock bottom on this in 2010. Then we hit rock bottom in 2011. And we are still at rock bottom. We were vulnerable before and now we’re just more vulnerable.”4 For the first time in 12 years, the results of the Law and Boardroom Study conducted by FTI Consulting, surveying nearly 2,000 General Counsels and 11,340 corporate directors at public companies, shows data-security concerns are now at the top of mind, as the most prevalent concern among both groups (48% of Board of Directors and 55% of General Counsels), topping both operational risk and reputation concerns.5 With recent books and movies like Stieg Larsson’s The Girl with the Dragon Tattoo and protagonist Lisbeth Salander’s hacking into everything under the sun, one might wonder: is it really that easy to hack into the world’s deepest secrets? Apparently so.

Incidents of cyber crime and “hactivism” (taking revenge on perceived slights) are rampant today.6 Privacy Rights Clearinghouse reported that, since 2005, more than 534 million personal records have been compromised.7 In 2011, 273 breaches were reported involving 22 million sensitive personal records.8 The World Economic Forum’s Global Risks 2012 report identified cyber attacks as the fourth most worrisome risk, behind economic fears and concerns over rising greenhouse gas emissions.9 The biggest risks are to business handling a lot of personal information from customers and/or employees. Industry groups that tend to see the largest risks are in retail, financial, health care and hospitality sectors.10

Recent hacking stories include the 2011 Sony shutdown of its PlayStation online network for an entire month, which is now reportedly the second largest data breach in U.S. history with a price tag estimated to be in excess of $200 million and rising.11 Sony has now been reportedly sued in over 60 class actions in the United States and Canada, which allege damages arising out of the theft of the plaintiffs’ Personally Identifiable Information (“PII”) and financial information, as well as Sony’s delay in providing notice and shutdown of its system. Several investigations by state Attorneys General and the Federal Trade Commission are also pending against Sony. In July 2011, Zurich American Insurance Company filed a declaratory judgment lawsuit against Sony, requesting that the court find that there is no coverage for its insured Sony for the class actions and other lawsuits relating to this shutdown under primary and excess General Liability insurance policies Zurich issued to Sony.12

Other recent notable data breaches which made the news include: Zappos/Amazon allegedly had 24 million records hacked in 2012; Global Payments, a third-party payment...
processor for credit card companies, was breached in 2012 and suffered a security breach which cost approximately $125 million; and the State of South Carolina Department of Revenue in 2012 had 3.6 million tax records, social security numbers, names, addresses, dates of birth and some bank routing numbers compromised.

In January 2007, TJX, the operator of T.J. Maxx and Marshalls stores, announced that cyber hackers accessed certain systems which 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. In fact, TJX 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 ever loss of personal data to date.

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 them 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. Those repercussive costs reached $256 million after nine months. Not only did TJX have to incur millions to conduct internal investigations and repairs, it also 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. TJX’s costs are representative of the type which a company may expect following a data breach, although TJX’s costs were so massive thanks, in part, to the breadth of the breached information.

This article will address the regulatory domestic framework that sets forth requirements for responding to data breaches as well as traditional insurance coverages that have been asked to provide coverages for the costs and liability associated with such breaches. Last, this article will address the newer dedicated product to arrive on the insurance market, cyber and privacy related stand alone insurance coverage.

II. Regulatory Framework

The problem is that each state’s laws vary as to how, whom and when to notify and most of the other statutes identified above apply to a particular industry or subset of entities and individuals and can have unexpected outcomes. For example, California retailers received quite a shock in early 2011 when the California Supreme Court, in the case of Pineda v. Williams Sonoma Stores, Inc., 51 Cal. 4th 524, 541 (2011), reversed an appellate court’s finding and held that the collection of zip code information from customers during a credit card transaction could retroactively amount to a potential violation of the Song-Beverly consumer privacy statute. This ruling opened the floodgates to the filing of more than 150 class action lawsuits by plaintiffs against more than 100 California retailers. See also Tyler v. Michaels Stores, Inc., No. SJC-11145, Slip Op. (Mass. March 11, 2013). In Tyler, after initially granting a retailer defendant’s Motion to Dismiss an action asserting that collection and recording of a customer’s zip code information in connection with a credit card transaction constituted a violation of Mass. Gen. Laws chpt. 93, § 105(a) -- see 848 F. Supp. 2d 438 (D. Mass. 2012) -- a federal district court was persuaded by the plaintiff to certify the state law issues of first impression presented in the case to the Massachusetts Supreme Judicial Court. The SJC, adopting reasoning closely analogous to that provided by the California Supreme Court in Pineda, held that a customer’s zip code constitutes personal identification information, the solicitation and electronic recording of which in connection with a retail credit card transaction violated the Massachusetts unfair and deceptive trade practices statute. In the immediate aftermath of the Tyler decision, class actions against other retailers have commenced in the Massachusetts courts, following the California template.

In addition, federal pre-emptive legislation has been kicking around Congress for quite a while. In 2009, during the release of his Cyberspace Policy Review, President Obama declared that the “cyber threat is one of the most serious economic and national securities we face as a nation.” Thereafter, much interest was focused on H.R. 2221, The Data Accountability and Trust Act (“DATA”). In December 2009, for the first time ever, a federal data breach notification bill was put up for a vote and passed the House, but then stalled in the Senate. DATA, which would have preempted state laws, provides one standard in the U.S. which would have required, in key measure that: consumers be notified within 60 days of a data breach; breaches be reported to credit bureaus if more than 5,000 accounts were compromised; two years of credit monitoring to consumers and a toll-free number to call for information about any breach. DATA defined PII as an individual’s first name or initial and last name or address, or phone number in combination with any one or more of the following data elements for that individual: social security number, driver’s license number or other state identification number, financial account number or credit/debit card number and any required security code, access code, or password that is necessary to permit access to an individual’s financial account. The bill would have made the Federal Trade Commission (“FTC”) the agency responsible for oversight and enforcement and provided it with the authority to further define procedures. It would also have required organizations that hold PII to establish their own data security policy, identify a person as an “information security officer” and outline a process for identifying vulnerabilities in their systems and methods of monitoring for breaches. One criticism voiced concerning this and many similar bills is that the FTC does not have the power to enforce regulations on entities such as and including the government, banks, the insurance industry and non-profits (e.g. colleges).
DATA did not take away the existing rights of state Attorneys General to enforce their own states’ consumer protection laws, to the extent not preempted.18

Since DATA stalled, there have been numerous additional attempts to pass federal pre-emptive legislation addressing data breach notification and cybersecurity. In 2011, over 50 cyber-related bills were introduced, including one proposed by President Obama in May 2011 with steps for improving cybersecurity. The Obama proposed legislation included harsher penalties for computer criminals – adding cyber offenses to RICO in order to harmonize computer crimes with other crimes and set mandatory minimum prison sentences for cyber intrusions and would have made the Department of Homeland Security overseer of cybersecurity. Similarly to DATA, this legislation would have applied to organizations that store PII for at least 10,000 individuals a year, requiring notification within 60 days of a breach, preempting state laws and making the FTC the gatekeeper for data notification.19

The federal legislative measure gaining the most attention recently is the Cyber Intelligence Sharing and Protection Act (“CISPA”), a proposed law which would allow for the sharing of Internet traffic information between the U.S. government and private technology, telecommunications and manufacturing companies in order to enhance the government’s capacity to ensure the security of networks against cyber attacks and more effectively investigate cyber crimes. CISPA was originally introduced in the House of Representatives in November of 2011, with 112 co-sponsors, and passed the House in April 2012, but it did not pass the U.S. Senate and faced a threatened veto by President Obama in any event.20 The legislation was reintroduced in February 2013 and again passed by the House on April 18, 2013. Senate leaders immediately indicated that CISPA would not be acted upon, and it appears to be dead for now.21

Given Congress’ failure to reach a consensus and escalating risks to critical systems, as a stop gap measure, President Obama signed an Executive Order entitled “Improving Critical Infrastructure Cybersecurity” on February 13, 2013. It requires federal agencies (such as the U.S. Department of Justice, Department of Homeland Security and National Intelligence Agency) to examine ways for the U.S. Government to share information about potential cyber threats with private sector companies. The hope is to improve cybersecurity sharing and collaboratively develop and implement risk-based voluntary standards. However, this order is not a stand-alone measure. Legislation is still needed to address gaps in the Executive Order, which is vague and requires a lot of the specifics to be figured out over time. There is a concern over the risk of legal liability and absence of anti-trust protection for companies that share information with the government and with each other. Such concerns can only be addressed by Congress, but it is unable to agree on how to protect businesses and consumers alike. This Order was months in the making following difficult negotiations with the private sector, which generally disfavors additional government regulation.

Many see the Executive Order as largely symbolic. During a speech on February 12, 2013, President Obama said America’s enemies are “seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy…. Now, Congress must act as well by passing legislation to give our government a greater capacity to secure our networks and deter attacks.” A commentator on the order, Jerry Ferguson, co-chair of BakerHostetler’s privacy and data protection practice, was reported by the
National Law Journal as saying, “You look at the actual language of this and it’s pretty vague stuff. You can see an order like this being announced and then just disappearing. It is also possible this is going to be a watershed event in that it will be a first step toward a coordinated cybersecurity strategy.”

Further guidance in this area has recently come from the SEC. In October 2011, the SEC provided its CF Disclosure Guidance for Cybersecurity Risks and Cyber Incidents. It changes the way companies will address cyber security by requiring public companies to disclose material cyber risks if they “are among the most significant factors that make an investment in the company speculative or risky.” It also requires disclosure of relevant insurance maintained by the reporting companies for such risks. The Chairman of the U.S. Senate’s Commerce Committee found this guidance to be a “sea change.” The guidance specifically requires disclosure of: aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences; description of those functions that are outsourced and disclosure of how the registrant addresses those risks; cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences; risks related to cyber incidents that may remain undetected for an extended period; and description of relevant insurance coverage. The guidance requires that the disclosure must be tailored and is to avoid boilerplate generic language. The good news/bad news is that the SEC Guidance is not binding. But the standards in the guidance are likely to be used by the SEC and shareholders of publicly traded companies as a baseline to assess overall compliance.

A report, Willis Fortune 500 Cyber Disclosure Report 2013, found that 88% of the Fortune 500 are following SEC Guidelines as of April 2013 and providing some disclosure. However, Bloomberg reported in August 2012 that a few companies got scolded by the SEC for failing to report known hacking attacks as required by the disclosure: “In future filings please expand this risk factor to disclose that you have experienced cyber-attacks and breaches”, the SEC wrote to Amazon on April 18, 2012, referring to the Zappos breach. Similar occurrences were reported about Google, Hartford and AIG.

More recently, there has been further proof that the 2011 guidance provided by the SEC on cyber security is not a one-and-done occurrence. In an April 2013 panel discussion by the SEC’s Division of Corporate Finance, the panel suggested that further comments on SEC disclosure of cyber breaches may be forthcoming later this year. The panel further commented that a public company’s Board of Directors has ultimate oversight responsibility of cyber security.

In addition to the various federal and state guidelines and the SEC, the Card Brands (collectively Visa, MasterCard, American Express, and Discover) have all implemented specific processes to which the parties to a credit card transaction must submit as part of their various operating guidelines. Specifically, Visa implemented a process in October of 2012 called the Global Compromised Account Recovery process (or GCAR), which is intended to assign financial and administrative responsibility throughout the payment chain so that costs are allocated to the merchant, card processor, and issuing banks, accordingly. The process is designed to curtail the litigation between these parties by assigning expenses for card reissuance,
breach response (notification, credit monitoring, forensics), and finally, fraud that occurs on the compromised cards.

The process Visa uses is proprietary to them, and there appears to be little one can do to overturn the decision on what Visa ultimately determines as the amount owed. This can be an issue in both standard (CGL) insurance contracts and otherwise well-meaning stand-alone cyber insurance as many of the policies have contractual liability, liquidated damages, PCI, or other “card brand claim” exclusions in them. In addition, the Card Brands have the right to insist that the Insured hire a particular vendor to its own investigation on top of the one you may already be doing, which could create challenges in getting these costs reimbursed. It is important to make sure you understand how your policy is going to respond in the event that credit card risk is a major part of your exposure and that you use qualified insurance brokerage and legal services in procuring the appropriate coverage.

III. Traditional General Liability Coverage for Cyber and Privacy Exposure

The standard commercial general liability (“CGL”) policy drafted by the Insurance Services Organization (“ISO”) 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. Historically, policyholders had some success finding coverage for cyber liability and privacy claims under their CGL policies. In response to these successes, the ISO adopted a series of amendments to the original 1973 CGL policy form in an attempt to limit or eliminate coverage for such claims.

For example, disagreements arose between insureds and their insurers with regard to whether data loss could constitute covered “property damage” 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.

Fireman’s Fund Ins. Co., 46 P.2d 1264 (N.M. App. Ct. 2002) (Computer data stored on hard drive constitutes “tangible property”). In response to uncertainty over whether data was “tangible property,” the insurance industry amended the definition of “property damage” to specify 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).

The 2001 amendment to the definition of “property damage” did not completely eliminate coverage for claims involving computer programs and software. While liability for damage to data itself may not be covered under the 2001 CGL policy, claims seeking damages due to the loss of use of tangible property (e.g. a computer or server) caused by damage to data (e.g. software) still could be covered. See, e.g. Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797 (8th Cir. 2010) (coverage for physical injury to computer hardware such as freeze-up (loss of use) caused by spyware). Even after the 2001 amendment, coverage for claims alleging loss of use of tangible property arising out of the insured’s software or data would be covered unless the “the repair, replacement, adjustment or removal” of the insured’s software, without more, would completely restore the claimant’s property, in which case the “impaired property” exclusion (Exclusion m.) would eliminate coverage.

In 2004, the insurance industry added the following exclusion to the CGL policy which was intended to eliminate coverage for data-related loss of use claims:

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.
Another issue that has been contested by insurers over the years is whether privacy-related cyber liability falls within the scope of the “Personal and Advertising Injury” coverage provided by a CGL policy. CGL policies provide coverage for damages because of “advertising injury,” which was defined in the 1985 CGL policy, in relevant part, as follows:

“Advertising injury” means injury arising out of one or more of the following offenses:

* * * * *

b. Oral or written publication of material that violates a person's right of privacy.

ISO Form No. CG 00 01 11 85.

In *Recall Total Information Management, Inc. v. Federal Insurance Co.*, No. X07CV095031734S, 2012 WL 4699888 (Conn. Super. Ct. Jan. 17, 2012), 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. Both policies were issued for the term of May 6, 2005 to January 4, 2006 and were renewed for two consecutive one-year terms until January 4, 2008. 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. *Id.*, at *1.

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 over 500,000 IBM employees was 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.” *Id.*, at *4. Both policies defined property damage as “damage to tangible property.” *Id.* 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.” *Id.*, at *5. The policies stated that “Tangible property does not include any software, data or other information that is in electronic form.” *Id.* 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. *Id.*
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.” Id. 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. Id., at *6. The court therefore granted the insurers’ motions for summary judgment.

The first big wave of coverage disputes in this area arose in the context of alleged violations of the Telephone Consumer Protection Act of 1991 (“TCPA”). The TCPA prohibits the “use [of] any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine.” 47 U.S.C. § 227(b)(1)(C). Courts are split on whether sending unsolicited advertisements by fax constitutes “[o]ral or written publication of material that violates a person's right of privacy.” Some courts have held that TCPA claims are covered because they interpret “right of privacy” to refer to the claimant’s right to seclusion, and sending an unwanted fax is a “publication” that violates the recipient’s right of seclusion. For example in Valley Forge Insurance Co. v. Swiderski Electronics, Inc., 860 N.E.2d 307 (Ill. 2006), the Illinois Supreme Court held that “[t]he receipt of an unsolicited fax advertisement implicates a person's right of privacy insofar as it violates a person's seclusion, and such a violation is one of the injuries that a TCPA fax-ad claim is intended to vindicate.” Other courts have held that TCPA claims are not covered because the “right of privacy” refers only to the content of the material subject to publication, and faxing an unwanted advertisement does not disclose “secret” or confidential personal material in violation of the claimant’s right to privacy. See Penzer v. Transportation Ins. Co., 29 So.3d 1000 (Fla. 2010). Although most courts have held that statutory TCPA damages constitute covered “damages” under a CGL policy, not all courts agree. See Standard Mut. Ins. Co. v. Lay, 2013 IL 114617 (citing cases).

The next big wave of coverage disputes arose in the context of advertising injury coverage for alleged violations of the Fair Credit Reporting Act of 1970 (“FCRA”) claims. The FCRA claims typically involve a consumer alleging that a business has obtained his or her credit information and used that information for purposes not authorized by FCRA. Several courts have found coverage for FCRA claims because they involve liability because of an “[o]ral or written publication of material that violates a person's right of privacy.” Some of these cases also seem to make the distinction between secrecy and seclusion. In Pietras v. Sentry Ins. Co., 2007 WL 715759 (N. D. Ill. Mar. 6, 2007), for example, the court held that FCRA claims fell within the “advertising injury” coverage because “even if the [insured’s] solicitations did not contain personal credit information, they still implicate the consumers’ right to privacy protected by the FCRA - the right not to receive credit solicitations sent without a permissible purpose.” In American Family Mut. Ins. Co. v. C.M.A. Mortgage, Inc., 2008 WL 906230, *1 (S.D. Ind. Mar. 31, 2008), the court also found coverage for a FCRA claim alleging that the insured accessed consumers’ credit reports as part of a “prescreening” process that generated solicitation letters to persons identified with certain credit traits.

In a 2011, the Eleventh Circuit Court of Appeals issued a decision in connection with a claim for coverage for claims against the insured alleging violations of the Fair and Accurate Credit Card Transaction Act that may have a bearing on claims for cyber-torts under Coverage
B. See, Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co., No. 11-11781, 2011 WL 4509919 (11th Cir. Sept. 30, 2011). 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 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.” Id. at *5. 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.” Id. The insured only provided 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 does not change the plain meaning of the term “publication.” Id. This decision provides insurers with authority to deny coverage, under Coverage B, for data breach claims that do not result in the dissemination of information to a third party.

Some individual insurers have developed and incorporated manuscripted “invasion of privacy” language into their policies in an effort to avoid judicial interpretations recognizing a “seclusion interest” as well as a “secrecy interest” in the standard policy language. For example, a provision used by Travelers states as follows:

Making known to any person or organization written or spoken material that violates a person’s right of privacy . . . .

b. Oral, written or electronic publication of material that appropriates a person’s likeness, unreasonably places a person in a false light or gives unreasonable publicity to a person’s private life . . . .

Travelers “Web XTend Liability” Form No. CG D2 34 01 05.

Also over the years, CGL insurers have added exclusions to the Personal and Advertising Injury Liability coverage provisions in their policies for cyber liability. Prior to 2007, the exclusions could be added to a CGL policy by endorsements such as the following:

- “Exclusion – Violation of Statutes that Govern E-Mails, Fax, Phone Calls or other Methods of Sending Material or Information” (ISO No. CG 00 67 03 05);

- “Recording and Distribution of Material or Information in Violation of Law Exclusion” (ISO Form No. CG 68 05 09); and
• “Information Distribution and Recording Violations Exclusion” (AAIS Form No. GL 1022 09 09).

In 2007, ISO added a “Distribution of Material In Violation Of Statutes” exclusion to the CGL policy, which eliminated coverage for:

"Bodily injury" or "property damage" [or “personal or advertising injury”] arising directly or indirectly out of any action or omission that violates or is alleged to violate:

(1) The Telephone Consumer Protection Act (TCPA), including any amendment of or addition to such law; or

(2) The CAN-SPAM Act of 2003, including any amendment of or addition to such law; or

(3) Any statute, ordinance or regulation, other than the TCPA or CAN-SPAM Act of 2003, that prohibits or limits the sending, transmitting, communicating or distribution of material or information.

ISO Form No. CG 00 01 12 07.

In 2009, ISO further broadened the scope of this exclusion by introducing a mandatory “Recording And Distribution Of Material Or Information In Violation Of Law” endorsement, which included TCPA and FACTA claims pursuant to the following paragraph:

(3) The Fair Credit Reporting Act (“FCRA”) and any amendment of or addition to such law, including the Fair and Accurate Credit Transaction Act (“FACTA”); . . . . .

ISO Form No. CG 00 01 12 07. This endorsement also broadened the final “catch-all” paragraph in the exclusion from “[a]ny statute, ordinance or regulation . . . that prohibits or limits the sending, transmitting, communicating or distribution of material or information” to “any federal, state or local statute, ordinance or regulation . . . that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information.” See id. This exclusion was incorporated into the April 2013 version of the ISO CGL policy. See ISO Form No. CG 00 01 04 13.

In addition to the preceding ISO exclusions, manuscripted policy provisions intended to eliminate coverage for privacy-related cyber liability under CGL policies have also cropped up. One such provision, found in a CGL policy issued by The Hartford, excludes coverage as follows:

q. Right of Privacy Created by Statute:

“Personal and advertising injury” arising out of a person’s right of privacy created by any state or federal act.
However, this exclusion does not apply to liability for damages that the insured would have in the absence of such state or federal act.

Consistent with the breadth and underlying intent of these various exclusions, carriers have sought to apply their exclusions broadly to extinguish virtually every possible type of privacy coverage relating to statutes that are not specifically included by these exclusions, such as claims relating to the Song-Beverly Act and related state court causes of action or allegations, in regard to which several insurers have sued their policyholders seeking declaratory judgments of no coverage. See Tsikoudakis, “ZIP Codes Deliver Liabilities; As Retailer Suits Mount, Will Insurers Cover?” Business Insurance, July 25, 2011; Allaband, “United States: Coverage Disputes Arise Out of Rash of Consumer Class Actions,” Mondaq Business Briefing, July 28, 2011.27

IV. Other Forms of Traditional Coverage Potentially Responsive To Cyberliability Claims

In addition to CGL coverage, policyholders have sought, and in some instances successful obtained, coverage for losses and/or liabilities attributable to cyberattacks under other forms of policies typically included in the comprehensive insurance programs of sophisticated corporate entities.

First, as regards the basic coverage afforded by first-party property insurance policies, the determination whether the loss of electronic data meets the policies’ conception of “physical injury to Covered Property” will largely depend upon resolution of the same question wrestled with by the courts in regard to third-party liability coverage, as addressed above. If electronic data is regarded as “tangible” property -- see Computer Corner and Ingram Micro, supra -- then coverage will likely be found to exist, whereas if it is not -- see America Online and Seagate Technology, supra -- then coverage may be denied. See, e.g., Ward General Ins. Servs., Inc. v. Employers Fire Ins. Co., 114 Cal. App. 4th 548, 7 Cal. Rptr. 3d 844 (2003) (where negligently-caused “crash” of insured’s computer system resulted in loss of customer database, but there was no attendant harm to or destruction of the data storage medium, no coverage was due because all potentially-responsive coverage grants or endorsements incorporated in the subject first-party property policy were triggered by “direct physical loss of or damage to Covered Property” and database, in and of itself, did not constitute such property).

However, as in the third-party context, uniformity of decisions is conspicuous by its absence and several courts, in noteworthy decisions, have held that a policyholder’s loss of electronic data, especially (but not necessarily) when paired with some physical harm to computer hardware itself, creates clear circumstances for the provision of coverage by insurers under first-party property policies and their typical endorsements, including those addressing Business Interruption expenses and so-called Extra Expense. See e.g., Lambrecht & Assoc. Inc. v. St. Paul Fire & Marine Ins. Co., 119 S.W.3d 16 (Tex. Ct. App.-Tyler May 13, 2003) (insured’s complete loss of use of its server and all computerized data stored therein, its replacement of previously-existing software, and its costs associated with the loss of business resulting from inability of employees to utilize the computer system while the server was down and the labor associated with manual re-entry into the revitalized system of all data lost due to third-party computer hacker’s infection of the insured’s system with a virus, all constituted...
“Covered Loss” attributable to “accidental [from the standpoint of the insured] direct physical loss to business personal property”); *NMS Servs., Inc. v. The Hartford*, 62 F. App’x 511, 2003 WL 1904413 (4th Cir. 2003) (reversing summary judgment in favor of insurer in the trial court, Court of Appeals held that insured’s losses attributable to destruction of insureds computer system by hacking activities of disgruntled former employee, including Business Income lost during restoration period and collateral expenses that would have been unnecessary except for the disruption, were subject to coverage under first-party property policy’s Business Interruption and Extra Expense coverage provisions).

Policyholders may have also purchased “Contingent Business Interruption” coverage, premised upon the loss of revenues associated with the disruption of the policyholder’s own business operations as a result of injury or damage to the property and business operations of third-party entities that serve as the policyholder’s key suppliers of materials or finished-product customers. Based on an extension of the same reasoning adopted by the courts in *Lambrecht & Assocs.* and *NMS Services*, supra, it may reasonably be anticipated that policyholders may secure first-party property coverage in those circumstances as well.

Sophisticated, well-advised policyholders may seek to protect their business interests by obtaining insurance beyond the coverage provided by CGL and first-party property policies, such as directors & officers liability, errors and omissions liability, fidelity and surety bonds, and commercial crime insurance policies. All such coverages could, under particular circumstances, theoretically respond to claims arising in connection with a cyberattack. See, *e.g.*, *Eyeblaster*, 613 F.3d at 801-05 (in case in which underlying claimant alleged that visit to insured’s interactive advertising website infected claimant’s computer with spyware, causing the computer to freeze up and resulting in loss of important tax return data and other performance problems, appellate court held that insurer had duty to defend insured under provisions of both a CGL policy and an Information and Technology Errors and Omissions policy obligating the insurer “to pay loss for financial injury caused by a wrongful act that results in the failure of Eyeblaster’s product to perform its intended function or to serve its intended purpose”).

In *Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh*, PA, 691 F.3d 821 (6th Cir. 2012), the Court of Appeals, in a case addressing issues of first impression, affirmed a lower court holding that the insureds were entitled to coverage, under the provisions of a computer fraud rider to a Blanket Crime Policy, for $6.8 million in stipulated losses (including prejudgment interest) attributable to a computer hacking scheme that compromised customer credit card and checking account information. The background was that over a 14-day period in early February 2005, organized hackers used a local wireless network at one of the insured’s Designer Shoe Warehouse (DSW) retail stores to obtain unauthorized access to the insureds’ main computer system and download credit card and checking account information of more than 1.4 million customers at 108 different stores. Fraudulent transactions utilizing the stolen customer information followed, in connection with which the insureds were first notified on March 2, 2005. See 691 F.3d at 824.

In the wake of discovery of the data breach, the insureds incurred substantial expenses with respect to public relations, customer communications, defense and resolution of customer claims, and attorneys’ fees relating to investigations by the Federal Trade Commission and seven state Attorneys General. The FTC inquiry was resolved administratively through consummation
of a consent decree pursuant to which the insureds agreed to establish and maintain a comprehensive internal information security program designed to safeguard the integrity and confidentiality of personal information obtained from or about customers. *Id.* Some $4 million of the insureds’ total expenses arose in connection with compromised credit card information in the form of costs associated with charge backs, card reissuance, account monitoring to identify fraudulent transactions, and fines imposed on the insureds by Visa/MasterCard. *Id.*

Upon the provision of notice to the insurer, followed by the submission of proofs of loss, coverage was denied and coverage litigation ensued. The parties agreed that the exclusive basis of potential coverage for the insureds’ losses was a provision of an endorsement addressing “Computer & Funds Transfer Fraud Coverage,” under which the insurer agreed to pay for “Loss which the Insured shall sustain resulting directly from . . . [t]he theft of any Insured property by Computer Fraud[.]” *Id.* at 826 (emphasis added). “Computer Fraud” was defined for these purposes, in pertinent part, as “the wrongful conversion of assets under the direct or indirect control of a Computer System by means of . . . [t]he fraudulent accessing of such Computer System[.]” *Id.*

In the district court and on appeal, the insurer urged the courts “to interpret the ‘resulting directly from’ language as unambiguously requiring that the theft of property by computer fraud be the ‘sole’ and ‘immediate’ cause of the insured’s loss.” *Id.* at 828. The district court, however, predicted in regard to this issue of first impression that the Ohio Supreme Court would adopt a proximate cause standard and, following that approach, the district court concluded that “‘there is a sufficient link between the computer hacker’s infiltration of [the insureds’] computer system and [the insureds’] financial loss to require coverage under Endorsement 17.’” *Id.* (citation omitted in original). The appellate court concurred, rejecting the insurer’s so-called “direct-means-direct” line of argument. *Id.* at 831 (“Despite defendant’s argument to the contrary, we find that the phase ‘resulting directly from’ does not unambiguously limit coverage to loss resulting ‘solely’ or ‘immediately’ from the theft itself.”).

Thus, *Eyeblaster* and *Retail Ventures* both demonstrate that, at a minimum, creative arguments regarding coverage for cyberattacks and resulting liabilities may, in certain circumstances, bear fruit under non-CGL forms of traditional coverages purchased by policyholders in an effort to protect their business interests. However, for more consistent protection of these sorts of claims, more policyholders have considered the purchase of standalone cyber and privacy coverage.

### V. Cyber and Privacy Related Stand Alone Coverage

In the past decade that this policy has existed, it has come a long way. An expert in the field has suggested “that this line of insurance could represent the biggest new product opportunity that we have ever seen.” In our own experience, this policy started off as very clunky coverage that involved a complex and time intensive application process, was virtually cost prohibitive to purchase, contained literally more exclusions than it did coverage and was offered by very few carriers in the marketplace. However, each of these characteristics of this coverage has significantly improved over the past several years. From our vantage point as counselors and negotiators of helping to place such coverage on behalf of our policyholder clients, what we are starting to see is a dynamic policy, with a much simpler application process,
from a growing competitive marketplace that seems to be providing real coverage for a reasonable price, with the number and reach of exclusions starting to lessen. Those changes may very well be because most carriers see cyber insurance as a huge growth trend for them in this challenging economy and are offering policyholders competitive options to try and catch a big piece of this market and be seen as a major go to player in the world of cyber insurance.

However, the 2011 Risk and Finance Manager Survey conducted by Towers Watson reported that 73% of the companies surveyed had not purchased cyber security insurance. It is expected that this percentage will go down dramatically in the coming years, because in our experience, companies both large and small are clearly starting to take notice of the daily news stories on the subject and are asking more questions about cyber policies, either as standalone coverage or as an add on to already existing Errors and Omissions coverage.

One of the biggest questions asked by policyholders considering the purchase of this coverage that we regularly receive is what does this policy cover? It is an interesting product because it can provide a hybrid of different coverages that encompass both first and third party coverages. Unlike, a CGL policy, for example, a cyber policy can provide coverage for liability but also provide coverage for traditional first-party property loss, like business interruption. The tricky part of the coverage though, is that unlike more developed coverage, like for example a Directors’ & Officers’ Liability policy, which oftentimes provides the same coverage grants of Side A (Non-Indemnified), Side B (Indemnified) and Side C (Entity) coverages, a cyber policy is not yet so standard. Many diverse coverage grants are available in the marketplace, but oftentimes, they are not yet all included in the basic cyber forms offered by the carrier – instead, they often can be added in by endorsement. So, when considering the purchase of cyber insurance it is important for the policyholder to work with a broker and an attorney who are very familiar with the cyber marketplace and what is available in it. These professionals should specifically know to ask for the coverage grants that will best protect a particular policyholder’s expected risks.

Some of the types of coverages that are available in the cyber marketplace today include:

A. Liability Coverage. In our experience, liability coverage is offered in virtually every, if not every, cyber policy in the current marketplace. The hope is that this policy will pick up where the historic CGL policies left off and provide coverage for many sorts of liability relating to data breaches and network security glitches, often including loss arising from a theft, hacking, loss, unauthorized disclosure of PII, alterations, corruption, destruction, deletion or damage to data or loss arising out of a breach in network security that allowed outsiders to access PII. By way of an example, think about the Sony class action lawsuits mentioned above that alleged theft of PII. Cyber liability coverage would be important to Sony to pay for its defense costs (and later for its indemnity costs) for each of those lawsuits. Cyber liability coverage can also include coverage for media or website related defamation and intellectual property, although the insured may need to specifically request this coverage as an add-on to the standard liability coverage.

Another type of liability exposure that can be insured through a cyber policy is coverage for a claim brought by a regulatory agency relating to an insured’s alleged failure to follow data notification or cyber security laws over the control and use of PII. This form of coverage can
include a defense and possibly payment of penalties ultimately owed relating to the insured’s liability. These are actions or investigations that are generally brought by state attorneys general or the Federal Trade Commission, but may include other entities as well.

An often overlooked coverage feature of some cyber policies has nothing to do with the breach of privacy, but is more in line with supply chain exposure. If there is a breach of security that causes a company to fail to meet its product or service delivery obligations, leaving the customer(s) with a business interruption loss (or perhaps even a downstream liability risk to the ultimate customer), the policies can be written to respond to such third party claims (for breach of contract, etc.). Many policy forms specifically define a “security breach” as something where the third parties’ computer system has to be harmed in some way, so again be aware of what your policy covers if this is a risk for you.

B. First Party Losses. While this is not always available in the standard cyber forms, there is usually an add-on to coverage that may be included for a first party property business interruption type of claim relating to your network being down. Back to the Sony example, this could be an important coverage for Sony to have because its entire on-line gaming system was down for about a month and the costs relating to that business interruption were certainly large.

First party coverage can also be included for the costs associated with hiring a data forensic and privacy breach response expert vendors who would need to be brought in following a data breach for the purpose of determining the cause, source and extent of network attack. First party coverage may further be added to pay for the cost of fixing the established problem. Again, these are all categories of expenses Sony certainly experienced following the breach of its online gaming system.

Another first party type of coverage available, has started to become a very significant inclusion for costs the insured incurs in the event of a data breach to notify those effected, answer questions they have about the breach and to offer injured persons credit monitoring services and other measures to prevent and correct identity theft. These services can be extremely costly to perform. Some insurers offer to simply reimburse such costs for their insureds up to a set sublimit, while others offer to put in place a team of vendors who perform the services for the insured in the first instance at the insurers’ expense.

In addition, insurers sometimes offer as an add-on to a cyber policy, coverage relating to cyber or network extortion. This coverage will reimburse an insured for amounts it paid to avert a credible threat to commit or continue a network attack against the insured or to disclose PII for the purpose of obtaining payment.

Last, insurers are often offering additional coverage for a set sublimit to help pay the public relations costs in dealing with restoring public confidence in the insured following a data breach or other covered event, often referred to as Crisis Event Management.

One area in which coverage disputes may arise involve cloud computing, as coverage may depend on whether the security breach occurs on the insured's own systems or “in the cloud.” See, Erich Bublitz, Catching the Cloud: Managing Risk When Utilizing Cloud Computing, P&C NATIONAL UNDERWRITER (Aug. 30, 2010); (In “evaluating network
security and privacy insurance, companies need to secure coverage broad enough to apply to personal data maintained by others on the insured’s behalf.” In the context of the language a coverage form 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 case, the factual dispute will lie in where and when the cloud 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 coverage form applies only to a failure by or asserted against an insured person or organization. However, the is little doubt that policyholder lawyers will attempt to bootstrap the conduct of the policyholder to that of the third party cloud storage provider.

***

In purchasing cyber insurance, one important point to which a policyholder should pay very close attention to is the sublimits the insurer offers for these various coverage grants. Generally speaking, most policies contain specific sublimits for each type of coverage offered and may not be able to be aggregated. The liability limits tend to allow for recovery of the full aggregate limits, but all the remaining (first party) coverages tend to have lower sublimits that are much less than the aggregate limits and often much less than the costs that will be incurred to pay for the covered service. For example, costs associated with notification and monitoring can be an extremely high service, based upon the amount of PII the insured stores that could potentially be breached. The insured should consider the costs likely to be associated with notification before it agrees to the amount of coverage that will be available in its cyber policy sublimits for this particular coverage and consider negotiating for higher sublimits or even full limits to make sure that it has adequate coverage. In addition, note that some carriers offer notification cost sublimits based on the number of persons notified (with a maximum amount of coverage available) rather than just based upon the estimated dollar amount of the costs associated with such notification.

Another consideration that a policyholder purchasing cyber coverage should closely study is the exclusions. In our experience, the trend appears to be moving toward less exclusions in a cyber policy. Having said that, there are still a number of common exclusions the policyholder is likely to encounter today. For example, the cyber policy purports to exclude coverage for claims that are generally covered by another existing policy, such as: bodily injury/property damage (covered by CGL), discrimination (covered by Employment Practices Liability Insurance), ERISA (covered by Fiduciary Insurance), Directors & Officers claims and Errors & Omissions claims (including transfer of funds, money or securities or other SEC violations). This policy also excludes the standards types of things that are also generally excluded in these other coverages (and are mostly considered uninsurable): Bad Acts (with exceptions), Prior Acts/Prior or Pending Litigation, Breach of Contract (with exceptions), Pollution/Nuclear, Anti-Trust, Patent law violations (and some other specific IP type exclusions), insured v. insured claims (with some exceptions), and war. It is important for the policyholder to
ensure that these sorts of exclusions each have appropriate carvebacks for the coverage that is supposed to be provided by this policy.

Last, there is a category of exclusions that are more specific to a cyber related claims that includes: fire, smoke, explosion, lightning, windstorm, flood, surface water; failure of utility service or infrastructure, including internet service; expiration or withdrawal of technical support by software vendor; violation of TCPA or similar federal or state law; FTC claims; RICO Claims; failure of software vendor to distribute a patch or other remedy for defect or vulnerability in the software provided, when such defect was known by vendor; and laptop exclusion. It is with this last category of exclusions with which a policyholder must be the most cautious with and do its best to negotiate the removal of such exclusions or at the very least include carvebacks to these sorts of exclusions that would include defense costs relating to any such claims. For example, a laptop exclusion would take away a significant risk for which an insured purchases cyber coverage. Every insured should outright refuse to purchase a cyber policy that contains this exclusion. An insured should also closely consider its agreements with its software vendors to make certain that the vendor maintains liability for the above uninsurable aspects. Last, insureds should pay close attention to the passage of federal pre-emptive legislation on cyber security and data notification. It is anticipated that such legislation will further allow the FTC and others to initiate claims against violators of the laws, which will include potential RICO actions. If that is the case, one would not want to have FTC and RICO exclusions in a cyber policy, particularly for defense costs relating to defending such possible actions.

Overall, given the great efforts by insurance companies to avoid cyber and privacy related coverage under other more traditional insurance policies, policyholders have every incentive to consider purchasing a standalone policy, particularly given that such policies are providing more coverage and value. Notwithstanding such improvements over the past several years, it is incumbent upon a policyholder to be vigilant and cautious in reviewing and negotiating such coverage to obtain the best possible coverage grants, limits, with minimal exclusions so as to provide it with the strongest blanket of insurance coverage in the event of a breach or claim.

1 Angela R. Elbert and Seth D. Lamden are partners in the Chicago, Illinois law firm of Neal, Gerber & Eisenberg LLP, where they counsel and represent corporate policyholders with respect to risk management matters and complex insurance coverage claims and disputes. Theodore A. Howard is a partner in the Washington, D.C. law firm of Wiley Rein LLP, where he counsels and represents property/casualty and professional liability insurers with respect to complex coverage disputes and litigation. Suzanne M. Whitehead is an associate in the Boston, Massachusetts law firm of Zelle, McDonough & Cohen LLP, where she litigates matters involving complex insurance disputes and represents insurers in coverage disputes involving general liability and professional liability policies. She acknowledges the writing of Anthony Zelle, H. Suzanne Beck and Aliya Page, who assisted in the paper. Mary Guzman is a Senior Vice President and the E&O and Information Security Practice Leader for McGriff, Seibels & Williams and has been an insurance broker for more than 20 years. She is responsible for setting the strategic direction for consulting and service offerings provided to McGriff’s clients and is charged with developing new products and writing policy language that will provide state of the art protection as these risks continue to evolve. The views articulated in this paper are those of the authors and do not necessarily represent the positions of their respective law firms or the firm’s clients.


FRAUD AND ABUSE ACT TO PROTECT CYBERSPACE AND COMBAT EMERGING THREATS


See also Retail Systems, Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 737-38 (Minn. Ct. App. 1991) (misplaced computer tape and data contained therein constituted “tangible property” subject to coverage under CGL policy); cf American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc., Civ. Action No. 99-185 TUC/ACM, 2000 WL 726789, at *2-*3 (D. Ariz. April 19, 2000) (in case in which power outage caused all of the computers in the insured’s facility to stop working, some for as long as 8 hours after power was restored, court found under “all risk” policy that “loss of access, loss of use and loss of functionality” of computers constituted “physical damage” thereto, even if their circuitry was not harmed or destroyed).

26 See also Tamm v. Hartford Fire Ins. Co., No. 02054BLS-2, 2003 WL 21960374, at *4 (Mass. Super. Ct. July 10 2003) (underlying complaint alleging that the insured, a computer software developer formerly employed by the claimant, unlawfully accessed claimant’s internal e-mail system and disseminated claimant’s confidential information through pre-lawsuit communications to claimant’s outside attorneys met elements for “Personal Injury” offense of invasion of privacy -- publication of private information; accordingly, insurer owed duty to defend even though complaint did not formerly assert a claim for invasion of privacy).

27 The limited caselaw interpreting these exclusions to date suggests that they are enforceable as written. See e.g., Creative Hospitality Ventures, Inc. v. U.S. Liability Ins. Co., 655 F.Supp.2d 1316, 1339-40 (S.D. Fla. 2009) (insurer granted summary judgment with respect to underlying claims that insured restaurants issued credit card receipts to claimant customers reflecting full credit card numbers and expiration dates in violation of FACTA based on court’s determination that coverage was barred by the plain language of the Distribution of Material in Violation of Statutes Exclusion), aff’d on other grounds, 444 F. App’x 370 (11th Cir. 2011) (unpublished); see also Oregon Mut. Ins. Co. v. Rain City Pizza, L.L.C., No. 67471-4-1, 2013 WL 150175, at *2-*3 (Wash. Ct. App. Jan. 14, 2013) (holding that Distribution of Material in Violation of Statutes Exclusion unambiguously barred coverage for underlying “blast fax” advertising claims in violation of TCPA and analogous state statute); cf. Axiom Ins. Managers, LLC v. Capitol Specialty Ins. Co., 876 F.Supp.2d. 1005, 1015 (N.D. Ill. 2012) (Distribution of Materials in Violation of Statutes Exclusion applicable to bar coverage for underlying claims alleging publication by the insured of false statements regarding claimant’s financial condition in violation of provisions of Texas Insurance Code, but not with respect to claimant’s common-law defamation claim against the insured).

