McCORMICK
BARSTOW LLP
ATTORNEYS AT LAW

James P. Wagoner
jim.wagoner@mccormickbarstow.com

*Certified Appellate Law Specialist certified by the Board of Legal Specialization of the California State Bar.
(Admitted in California)

Lejf E. Knutson
(Admitted in California)
lejf.knutson@mccormickbarstow.com

FRESNO, CA OFFICE
7647 North Fresno Street
Fresno, CA 93720
P.O. Box 28912
Fresno, CA 93729-8912
Telephone (559) 433-1300
Fax (559) 433-2300

Other offices of McCORMICK, BARSTOW, SHEPPARD WAYTE AND CARRUTH, LLP

www.mccormickbarstow.com

CINCINNATI, OH OFFICE
Scripps Center, Suite 1050
312 Walnut Street
Cincinnati, Ohio 45202
Telephone (513) 762-7520
Fax (513) 762-7521

DENVER, CO OFFICE
999 18th Street, Suite 3000
Denver, Colorado 80202
Telephone (720) 282-8126
Fax (720) 282-8127

LAS VEGAS, NV OFFICE
8337 West Sunset Road, Suite 350
Las Vegas, Nevada 89113
Telephone (702) 949-1100
Fax (702) 949-1101

MODESTO, CA OFFICE
1125 I Street, Suite 1
Modesto, California 95354
Telephone (209) 524-1100
Fax (209) 524-1188

2016 PARMA ANNUAL RISK MANAGERS CONFERENCE
FEBRUARY 25, 2016 – 9 a.m. to 10 a.m.
Renaissance Indian Wells Resort & Spa
Indian Wells, CA

"VIRTUAL LIABILITIES"

CYBER LIABILITY AND RISK MANAGEMENT FOR CYBER-RELATED LOSSES AND CLAIMS

Catherine A. Jones
Director, Risk Management Services
Kern County Superintendent of Schools Office
1300 17th Street – City Centre
Bakersfield, California 93303-1847
(661) 636-4223; FAX: (661) 636-4418
E-mail: cajones@kern.org

Dennis Timoney
ARM Chief Risk Officer
Special District Risk Management Authority
1112 I Street, Suite 300
Sacramento, California 95814
(916) 231-4141 FAX: (916) 231-4111
E-mail: DTimoney@sdrma.org

James P. Wagoner
McCormick, Barstow, Sheppard, Wayte & Carruth
7647 N. Fresno Street
Fresno, California 93720
(559) 433-1300 FAX: (559) 433-2300
E-mail: jim.wagoner@mccormickbarstow.com

Lejf E. Knutson
McCormick, Barstow, Sheppard, Wayte & Carruth
7647 N. Fresno Street
Fresno, California 93720-1501
(559) 433-1300 FAX: (559) 433-2300
E-mail: lejf.knutson@mccormickbarstow.com

I. OVERVIEW:

This session will address current and emerging issues involving risk management and liability coverage for public entities in relation to computer-based cyber-related claims, including coverage issues for such claims under standardized insurance liability policies and new ISO cyber risk policy forms.

The goal of the session is to help participants better evaluate various coverages available to public entities for computer based cyber-related claims (first and third party), as well as implement best practices for the prevention, management and defense of cyber-related claims.

In addition to discussion of the pertinent issues, the panel will discuss real world examples of useful risk management practices that have been implemented by public entities in relation to such risks.

II. BRIEF OVERVIEW OF EMERGING CYBER LIABILITY RISKS

It is a fact of life in the 21st century that both public and private entities have become highly dependent on private computer network systems which are connected with the internet in order to conduct their business and interact with the outside world. However, risk exposures related to intrusions and/or interruptions of these networks are on the rise and, in fact, are considered one of the top risks faced by many entities.

For example, in the United States alone, an analysis of a representative sample of fifty-eight (58) organizations in both the public and private sectors found that the average

annualized costs of cyber attacks in 2015 for those organizations was $15 million, a 19% increase in associated costs from 2014.[1] The average time needed to resolve a cyber attack was 46 days with an average cost of $1.9 million per day, a 22% increase in costs over 2014.[2]

Moreover, cyber attacks on large corporations can result in monumental losses involving thousands or even millions of affected end customers which are then widely reported in the news media :

- Target Incident: In January, 2014, Target (the US's third largest retailer) announced that cyber intruders had stolen personal information (names, mailing addresses, phone numbers and email addresses) of over 70 million customers and the credit card information of approximately 40 million customers. Between 1 to 3 million of those credit card numbers subsequently were sold on the black market, raising an estimated $53.7 million for the intruders.
    - Costs: The attack cost Target approximately $148 million, while financial institutions associated with the attack reportedly suffered approximately $200 million in losses. In addition, Target's profits fell 46% in the fourth quarter of 2013.[3] Also, Target reportedly spent $61 million in anti-breach technology in the months following the attack,

[1] Ponemon Institute, "2015 Cost of Cyber Crime Study: United States" (October 2015), pg.5 available at http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states (last accessed, February 2, 2016).

[2] *Id.*

[3] Newsweek, "2014: The Year In Cyberattacks" (12/31/2014), located at http://www.newsweek.com/2014-year-cyber-attacks-295876 (last accessed 2/2/16).

although $44 million of this amount was reportedly offset by cyber insurance.[4]

- Ashley Madison Incident: On July 15, 2015, a hacking group called "Impact Team" released a small amount of personal data and users of the Ashley Madison website which connected end users to engage in extramarital affairs. Later in August, 2015, the same group publically posted the personal information of 32 million users on the Internet which was widely reported in the news at the time of the release.[5]
    - Costs: In August, 2015, two Canadian firms filed a class action lawsuit against the owners of the Ashley Madison website seeking $576 million in damages on behalf of "all Canadians" affected by the security breach.[6] In the US, five (5) putative class actions have been centralized in the Eastern District of Missouri by the United States Judicial Panel on Multidistrict Litigation and await coordination of pretrial hearings.[7]
- Sony Pictures Incident: In October, 2014, cyber intruders reportedly associated with the North Korean government and identifying themselves as the "Guardians of Peace" gained unauthorized access to computer systems of Sony Pictures

[4] Insurance Journal, "Target's Cyber Insurance Softens Blow of Massive Credit Breach" (2/26/14) (http://www.insurancejournal.com/news/national/2014/02/26/321638.htm) (last accessed 2/2/16).

[5] Forbes, "Cybersecurity Lessons Learned From the Ashley Madison Hack" (10/26/15), located at http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#5674c125ed99 (last accessed 2/2/16).

[6] BBC News, "Ashley Madison faces huge class-action lawsuit" (8/23/15), located at http://www.bbc.com/news/business-34032760 (last accessed 2/2/16).

[7] See *In re Ashley Madison Customer Data Sec. Breach Litig*., No. 2669, 2015 WL 8541658 (U.S. Jud. Pan. Mult. Lit. Dec. 9, 2015). The order also notes that "[t]he Panel also has been notified of thirteen related actions pending in eight districts."

Entertainment. The incident involved both the disruptions of Sony Pictures' internal computer networks as well as public dissemination of internal Sony Pictures data and communications.[8]

- Costs: While the Sony Pictures incident did not involve the public dissemination of private customer information, the intruders erased all data stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 computer servers.[9] In February, 2015, Sony executives announced that the IT costs associated with the attack would be $35 million for the fiscal year through March, 2015.[10]

III. LIABILITY ISSUES WITH RESPECT TO PUBLIC ENTITIES AND CYBER RISKS

A. Potential Liability Under California's Information Practices Act

Section 1798.82 of the California Civil Code requires a person or entity conducting business in California that owns, licenses or maintains "personal information" and suffers a breach of that information to notify the owner of the information, any third parties for whom they maintained that information, and in some cases the California Attorney General.[11]

---

[8] The Washington Post, "The Sony Pictures hack, explained" (12/18/2014), located at https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ (last accessed 2/2/16).

[9] Fortune, "Inside The Hack Of The Century" (7/1/15), located at http://fortune.com/sony-hack-part-1 ((last accessed 2/2/16).

[10] Computerworld, "2014 cyberattack To cost Sony $35M In IT Repairs" (2/4/15), located at http://www.computerworld.com/article/2879480/2014-cyberattack-to-cost-sony-35m-in-it-repairs.html (last accessed 2/2/16).

[11] California Civil Code §1798.82 states:

The term "personal information" is defined to include "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual" although it does not include information available to the general public from federal, state or local records.[12]

(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

While California was the first state to adopt a data security breach notification law, forty-six (46) other states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have also enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information. The three states without notification laws are Alabama, New Mexico, and South Dakota.

For information regarding the laws of other jurisdictions, see National Conference of State Legislatures, State Security Breach Notification Laws at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. (last accessed on January 29, 2016). In addition, a multitude of federal laws and regulations govern the security of all types of sensitive information.

[12] Civil Code § 1798.82(h)-(i).

Breach of these statutory notice requirements can result in a private cause of action by an affected person/consumer to impose injunctive relief and recover damages as well as civil penalties for "willful, intentional, or reckless" violations of the Act.[13]

With respect to public entities, one federal district court has held that the Information Practices Act is applicable only to state agencies and not local agencies. *See Clark v. Cty. of Tulare,* 755 F.Supp.2d 1075, 1096 (E.D.Cal. 2010) ("The Information Practices Act is limited to 'state' agencies. The Information Practices Act defines the term "agency" as 'every state office, officer, department, division, bureau, board, commission, or other state agency' and does not include any 'local agency.' Cal.Civ.Code § 1798.3(b). Therefore, the County cannot be liable under this section.")

The same federal district court held that a county sheriff was not liable for failing to satisfy the reporting requirement of the Act based on the lack of evidence that the sheriff, in his official capacity, was responsible for maintaining the computerized system involved in the breach. *Id.*

B. Potential Employer Immunity For Improper Cyber-Behavior Of Employees

The Communications Decency Act ("CDA") was enacted in 1996 with the goal of controlling the exposure of minors to indecent material over the Internet. An important purpose of the CDA was to encourage internet service providers to self-regulate the dissemination of offensive material over their services. However, a second objective was

[13] Civil Code §1798.84(b)-(e).

to avoid the chilling effect upon internet free speech that would be occasioned by the imposition of tort liability upon companies that do not create potentially harmful messages, but are simply intermediaries for their delivery. *Aeran v. America Online, Inc*., 129 F.3d 327, 331 (4th Cir. 1997).

It has been held that an employer that provides its employees with Internet access through the company's internal computer system is among the class of parties potentially immune under the CDA. *See, e.g., Delfino v. Agilent Technologies, Inc.*, 145 Cal.App.4th 790, 805 (2006) (internet threats transmitted by employee from computer supplied by employer were "information provided by another information content provider" within meaning of CDA immunity provision); *Kathleen R. v. City of Livermore,* 87 Cal.App.4th 684, 692–693 (2001) (rejecting contention that library was not immune under CDA for child's downloading of sexually explicit material on city library computers because of its governmental entity status).

IV. COVERAGE ISSUES RELATING TO CYBER LIABILITY RISKS UNDER STANDARDIZED, NON-CYBER LIABILITY FORMS

A. Issues Re: "Property Damage" Coverage For Cyber Risks Under Standard Forms

"Property damage" coverage under standardized third party liability forms is written to provide coverage for injury to tangible property and "loss of use" of tangible property.[14] This emphasis on "tangible property" has caused an a split of authority on whether loss of electronic data from computer systems could constitute covered "property damage":

[14] *See, e.g.,* ISO Form GL 00000173 (defining "property damage" as both "physical injury to tangible property, including all resulting loss of use of that property' and "loss of use of tangible property that is not physically injured.").

- *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 467 (E.D.Va. 2002) aff'd, 347 F.3d 89 (4th Cir. 2003) ("Computer data, software, and systems do not have or possess physical form and are therefore not tangible property as understood by the Policy");
- *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113, 1116 (W.D.Okla. 2001) ("Although the medium that holds the information can be perceived, identified or valued, the information itself cannot be. Alone, computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property.");
- *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 132 N.M. 264, 266, 46 P.3d 1264, 1266 (2002) (noting that "the district court found that the computer data in question 'was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed.' The district court concluded 'computer data is tangible property.'");
- *Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc.*, 2000 WL 726789, at *3 (D.Ariz. 2000) ("In this case, Ingram *doe*s allege property damage-that as a result of the power outage, Ingram's computer system and world-wide computer network physically lost the programming information and custom configurations necessary for them to function. Ingram's mainframes were 'physically damaged' for one and one half hours. It wasn't until Ingram employees manually reloaded the lost programming information that the mainframes were 'repaired.' Impulse was 'physically damaged' for eight hours. Ingram employees 'repaired' Impulse by physically bypassing a malfunctioning matrix switch. Until this restorative

work was conducted, Ingram's mainframes and Impulse were inoperable.") (emphasis in original);

- *Eyeblaster, Inc. v. Fed. Ins. Co*., 613 F.3d 797, 802 (8th Cir. 2010) ("loss of use" property damage coverage applied to computer system rendered unusable by spyware).

Notwithstanding this split of authority, coverage issues regarding "property damage" liability coverage and loss of electronic data likely will not remain a live issue since standardized liability policy forms generally now include: (1) policy language indicating that "electronic data is not tangible property";[15] and (2) a specific policy exclusion precluding coverage for "[d]amages arising out of loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[16]

B. Issues Re: "Personal And Advertising Injury" Coverage Under For Cyber Risks Under Standard Forms

Previous attempts to find coverage for third party Cyber Risks under standardized "personal and advertising risk" coverages have generally focused on the enumerated offense of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[17] In this context, coverage disputes have focused on whether the breach of computer networks which results in the improper release of private information to unauthorized parties satisfies the "publication" requirements in the "right to privacy" offense.

[15] ISO Form No. CG 00011001 (added in 2001).

[16] ISO Form No. CG 00011204 (added in 2004).

[17] ISO Form No. CG 00010413 [2012].

For example, in *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC*, 35 F.Supp.3d 765 (E.D.Va. 2014), the insured faced a class action suit alleging that it had failed to safeguard confidential medical records of hospital patients, with the result that those same records had become publically accessible via the internet. *Id.*, 767-768. On summary judgment, the district court determined the insurer had a duty to defend the suit because: (1) "exposing material to the online searching of a patient's name does constitute a 'publication' of electronic material"; and (2) "the public availability of a patient's confidential medical records gave 'unreasonable publicity' to that patient's private life and 'disclose[d]" information about that patient's private life'' as required to trigger potential coverage. *Id.*, 770-772; *see also Netscape Commc'ns Corp. v. Fed. Ins. Co.*, 343 F.App'x 271, 272 (9th Cir. 2009) (allegations "that AOL had intercepted and internally disseminated private online communications" sufficient to trigger "invasion of right to privacy" personal injury coverage because of "the policy's language covering disclosure to 'any' person or organization, which we find dispositive."); *Tamm v. Hartford Fire Ins. Co*., 2003 WL 21960374, at *3 (Mass.Super. 2003) (holding that "allegations of sending [] private communications via e-mail to outside attorneys seemingly satisfies both prongs under the invasion of privacy clause of the policy.")

Conversely, in *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 147 Conn.App. 450 (2014) aff'd, 317 Conn. 46 (2015), the insureds sought reimbursement for over $6 million paid in settlement of losses caused when they lost their client's data tapes containing employee personal data during transport. *Id.*, 454-455. The trial court held the insureds'

"invasion of right to privacy" personal injury coverage under their CGL policy did not apply to the loss and the Court of Appeal agreed, finding the loss of data, standing alone, did not constitute "publication" of the private employee information. *Id.*, 462 ("On the basis of our review of the policy, we conclude that personal injury presupposes *publication* of the personal information contained on the tapes. Thus, the dispositive issue is not loss of the physical tapes themselves; rather, it is whether the information in them has been *published*. The plaintiffs contend that the mere loss of the tapes constitutes a publication, and has alleged that the information was *published* to a thief. The plaintiffs have failed to cite any evidence that the information was published and thereby failed to take their allegation beyond the realm of speculation.")

Similarly, in *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, Case No. 651982/2001 (N.Y.Sup.Ct. 2014), the coverage dispute arose out of the "hacking" of Sony's PlayStation Network in April, 2001, which resulted in the theft of personal information of over 77 million users. At the trial court level, it was found that there was a "publication" of the users' personal information in violation of their "right to privacy". At the same time, the court found no coverage was triggered because the relevant "publication" was not by the insured, but rather was the result of the criminal acts of a third party. *Id.* (holding the applicable offence definition required "an act by or some kind of act or conduct by the policyholder in order for coverage to be present").[18]

[18] The case was appealed, although the appeal was subsequently withdrawn by party stipulation. *See Zurich Am. Ins. Co. v. Sony Corp. of Am.*, 127 A.D.3d 662, 6 N.Y.S.3d 915 (N.Y. App. Div. 2015).

However, and as is the case with potential "property damage" coverage, it is likely that "personal and advertising injury" coverage for similar computer network security breaches increasingly will be eliminated by newer policy exclusions targeted to preclude coverage for such liability risks.[19]

V. ISSUES RE: COVERAGE FOR CYBER RISKS UNDER NEW "CYBER-LIABILITY" COVERAGE FORMS

A. Initial Coverage Issues

1. Distinction Between First And Third Party Insurance Coverages

Similarly to some personal lines insurance coverages (e.g. homeowner's, auto), cyber risk policies are a "hybrid" form of "first" and "third" party coverages applicable to specific risks of loss associated with disruptions of and/or third-party intrusions on computer networks.

By way of background, "first party" insurance refers to coverage for the insured's own losses (i.e. injury to the insured's property, financial losses, etc.). The general focus of first party coverage is whether the loss was proximately causes by a specific risk within the scope of coverage (i.e. by an "enumerated peril"). *See Garvey v. State Farm Fire & Cas. Co.*, 48 Cal.3d 395, 406 (1989).[20]

[19] See ISO Form No. CG 21060514 [2014] (policy endorsement form providing "Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability" exclusion precluding coverage for "[d]amages arising out of" "[a]ny 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 or any other type of nonpublic information").

[20] With respect to causation for first-party coverage losses, California applies the "efficient proximate cause" doctrine which looks to whether a specified risk was the "prime", "moving" or "predominant" cause of the loss. *Garvey, supra*, 48 Cal.3d 395, 402; *see also* Cal. Ins. Code §532.

In contrast, "third party" liability coverage refers to situations where the insured is liable to third parties for acts and omissions on the part of insured and/or the insured's agents. *Id.* at 399 n.2 ("the distinction between first-and third-party claims can be summarized as follows: if the insured is seeking coverage against *loss or damage sustained by the insured*, the claim is first party in nature. If the insured is seeking coverage against *liability of the insured to another*, the claim is third party in nature.") (italics in original). As a result, third party coverage is focused on: (1) the form of injury reportedly suffered by the third party; and (2) "traditional tort concepts of fault, proximate cause and duty" as relevant to determine the insured's potential liability for the injury. *Id.*, 407.

As a result, cyber risk policies provide insureds with a "hybrid" form of first and third party coverages which are written to provide coverage for: (1) financial losses which an insured would typically suffer as a result of unauthorized intrusion into or disruption of computer networks; and (2) financial losses which third parties would typically suffer as a result of these same intrusions or disruptions and for which the insured could be held liable.

Given the different exposures and risks various companies and other entities have in connection with the use of their respective computer networks, different entities do not

---

As a result, first-party coverage generally "is unconcerned with establishing negligence or otherwise assessing tort liability" on the part of the insured. *Garvey, supra*, 48 Cal.3d 395, 406 (citing Bragg, "Concurrent Causation and the Art of Policy Drafting: New Perils for Property Insurers", 20 Forum 385, 386 (1985)).

necessarily have the same coverage needs with respect to cyber risks. As a result, since there can be significant premium differences, public entities should consider carefully "picking and choosing" which cyber risk coverages correspond to their actual exposures and coverage needs.

2. Issues Re: Claims Made And Reported "Burning Limits" Coverage

Unlike "occurrence"-based liability coverages which are focused on when the third party suffered compensable injury (i.e. "bodily injury" / "property damage") or when the insured committed an enumerated, wrongful act (i.e. "personal injury"), cyber risk coverage forms, including the ISO form, are typically written on a "claims made and reported" basis.[21] As a result, the trigger of coverage is based on when and whether: (1) the entity received notice of a "claim" during the policy period; and (2) reported that "claim" to the insurer during the applicable policy reporting period. *See, e.g., Indus. Indem. v. Superior Court,* 224 Cal.App.3d 828, 832 (1990) (enforcing claims made and reported requirements as a condition precedent to coverage).

[21] At the same time, some specific cyber risk coverages have been written on an "occurrence" basis. For example, the "Website Media Content Liability" coverage provided along with the "Information Security & Privacy Insurance With Electronic Media Liability Coverage" issued by Beazley Syndicate AEB 2623/623 is provided on an "occurrence" basis and, as written, applies to certain specified "acts committed [by the insured] in the course of Covered Media Activities occurring during the Policy Period." (Sec.I.D).

As a result, the "Website Media Content Liability" coverage is structured similarly to "personal injury" coverages which focus on when the insured purportedly committed an enumerated, wrongful act resulting in injury to a third party. *See Stonelight Tile, Inc. v. California Ins. Guarantee Ass'n,* 150 Cal.App.4th 19, 38 (2007) (discussing "personal injury liability" coverage).

Also, and is often the case in connection with "claims made and reporting" based coverage, cyber risk policies typically have been written as "self-consuming" or "burning limits" policies where the costs incurred to defend the insured against a third-party claim apply to reduce the applicable limits of available coverage. *See Aerojet-Gen. Corp. v. Transp. Indem. Co.*, 17 Cal.4th 38, 76 n.29 (1997) (discussing "self-consuming" and "burning limits" policies).

At the same time, and which is atypical for "hybrid" insurance policies, cyber risk policies can be written so that *any* payment of "loss" – whether first or third party losses – reduces the applicable aggregate limit of coverage. Under such forms, both the submission of costs associated with the insured's own first party losses and the defense and indemnification of third party losses could combine to erode the overall, applicable policy limit as those costs are incurred and submitted to the insurer for payment.[22]

---

[22] Section II – LIMITS OF INSURANCE

1. Policy Aggregate Limit of Insurance

   The most we will pay for all "loss", and "defense expenses" if covered, under the Policy is the Policy Aggregate Limit Of Insurance show in the Declarations. The Policy Aggregate Limit of Insurance shall be reduced by the amount of any payment made under the terms of this Policy. Upon exhaustion of the Policy Aggregate Limit of Insurance by such payments, we will have no further obligations or liability of any kind under this Policy.

2. Insuring Agreement Aggregate Limit Of Insurance

   a. Subject to the Policy Aggregate Limit of Insurance, the most we will pay for all "loss" and "defense expenses" if covered, under each Insuring Agreement, is the Insuring Agreement Aggregate Limit of Insurance shown in the Declarations.

      (1) The Insuring Agreement Aggregate Limit of Insurance shall be reduced by the amount of any payment for "loss, and "defense expenses' if covered, under that Insuring Agreement; and

      (2) Upon exhaustion of the Insuring Agreement Aggregate Limit of Insurance by such payments, we will have no further obligations or liability of any kind under that Insuring Agreement.

VI. THE EIGHT (8) PRIMARY CATEGORIES OF CYBER RISK COVERAGE (ISO FORM)

A. Web Site Publishing Liability (third party)

This coverage is designed to provide third party defense and indemnity coverage for "loss" resulting from designated "wrongful acts" by the insured taking place within the applicable policy period.[23]

With respect to "Web Site Publishing Liability" coverage, the current ISO form defines "wrongful act" as:

> Any actual or alleged error, misstatement or misleading statement posted or published by an 'insured' on its web site that results in:
>
> (1) Any type of infringement of another's copyright, title, slogan, trademark, trade name, trade dress, service mark or service name;
>
> (2) Any form of defamation against a person or organization; or
>
> (3) A violation of a person's right of privacy.[24]

---

b. If coverage for "regulatory proceedings' is being provided under Paragraph b. of Insuring Agreement 2. Security Breach Liability, the Limit of Insurance shall be part of, not in addition to, the Aggregate Limit of Insurance for the Insuring Agreement.

(ISO Form EC00100114 [2013] Sec.II).

[23] Web Site Publishing Liability

We will pay for both "loss" that the "insured" becomes legally obligated to pay and "defense expenses" as a result of the "claim" first made against the "insured' during the "policy period" or during the applicable Extended Reporting Period, for a "wrongful act" or a series of "interrelated wrongful acts" taking place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the "policy period".

(ISO Form EC00100114 [2013] Sec.I.1).

[24] ISO Form EC00100114 [2013] Sec.VII.35.

As drafted, the intent is to provide limited personal and advertising injury coverage in connection with statements published on an insured's website.

While there is limited case law on the subject, it is likely that insurer-insured disputes regarding this particular coverage will focus on whether or not the initial "publication" prerequisite has been satisfied, similar to standardized "personal injury" and "advertising injury" coverages with "publication" requirements. *See, e.g., Motorists Mut. Ins. Co. v. Dandy-Jim, Inc.*, 2009-Ohio-2270, ¶27, 182 OhioApp.3d 311, 321 (faxed advertisements satisfied advertising injury "publication" requirement); *Valley Forge Ins. Co. v. Swiderski Elecs., Inc.*, 223 Ill.2d 352, 367, 860 N.E.2d 307, 317 (2006) (same); *see also Cort v. St. Paul Fire & Marine Ins. Companies, Inc.*, 311 F.3d 979, 986 (9th Cir. 2002) (discussing "publication" requirements for personal injury coverage for defamation and disparagement).

One very significant difference between "Web Site Publishing Liability" coverage in comparison to other standardized advertising/personal injury coverages is that the ISO form expressly defines "loss" to include both "punitive damages" and "penalties" in some instances.[25]

[25] "Loss" means:

a. With respect to Insuring Agreements 1. Web Site Publishing Liability, 2. Security Breach Liability and 3. Programming Errors And Omissions Liability:

(1) Compensatory damages, settlement amounts and costs awarded pursuant to judgments or settlements;

(2) Punitive and exemplary damages to the extent such damages are *insurable by law*; or

However, and the same time, many jurisdictions have expressed public policy positions to the effect that insurance coverage cannot be extended to punitive damages, certain penalties or restitutionary relief, a fact recognized by the ISO "loss" definition itself. *See, e.g.,* Cal. Ins. Code §533; *California Cas. Mgmt. Co. v. Martocchio,* 11 Cal.App.4th 1527, 1533 (1992) (explaining that Cal. Ins. Code §533 "as a matter of public policy [precludes insurance coverage] for a wrongdoer from his act of wrongdoing; or for fines or restitution imposed as a result of a criminal conviction, or for civil proceedings prosecuted by the state in the exercise of its police power and regulatory authority conferred by statute"); *Perez v. Otero*, 415 So.2d 101, 101-02 (Fla.Dist.Ct.App. 1982) ("Insurance companies are not liable for punitive damages assessed against their insured for torts committed by their insured as a matter of public policy."); *Am. Sur. Co. of New York v. Gold*, 375 F.2d 523, 527-28 (10th Cir. 1966) ("Kansas public policy forbidding contracts insuring against punitive damage awards"); *AIU Ins. Co. v. Superior Court,* 51

---

(3) Under … 2. Security Breach Liability, fines or penalties assessed against the "insured" to the extent such fines or penalties are *insurable by law*.

With regard to Paragraphs 10.a.(1) through 18.a.(3), "loss" does not include:

(a) Civil or criminal fines or penalties imposed by law, except civil fines or penalties as provided under Paragraph 18.a.(3);

(b) The multiplied portion of multiplied damages;

(c) Taxes;

(d) Royalties;

(e) The amount of any disgorged profits; or

(f) Matters that are *uninsurable pursuant to law*.

(ISO Form EC00100114 [2013] Sec.VII.18) (emphasis added).

Cal.3d 807, 836 (1990) ("as a matter of public policy, an insured's payment of certain types of restitution cannot be covered by insurance").

As a result, the scope of "loss" coverage for punitive damages and/or penalties in connection with "Web Site Publishing Liability" could become **a** source of significant "choice of law" disputes in situations where the insured and third party claimants are domiciled in separate jurisdictions with differing law on the subject of insurance coverage for punitive damages and/or penalties. *See, e.g., Stonewall Surplus Lines Ins. Co. v. Johnson Controls, Inc.,* 14 Cal.App.4th 637, 649 (1993) (choice of law analysis whether California or Wisconsin law regarding insurability of punitive damage award would apply); *Fluke Corp. v. Hartford Acc. & Indem. Co*., 102 Wash.App. 237, 255 (2000), aff'd, 145 Wash.2d 137, 34 P.3d 809 (2001) (holding Washington and not California law controlled issue of insurability for punitive damages award).[26]

B. Security Breach Liability (third party)

Similarly, "Security Breach Liability" coverage is drafted to provide coverage for "loss" resulting from designated "wrongful acts" by the insured taking place within the applicable policy period.[27] The current ISO form defines "wrongful act" as:

[26] At the same time, even in jurisdictions where punitive damages, penalties or restitutionary relief are unindemnifiable as a matter of public policy, the fact that a cyber risk policy is expressly written to provide coverage for punitive damage, penalties and/or restitutionary relief could obligate the insurer to provide a full defense against such claims. *See Downey Venture v. LMI Ins. Co.,* 66 Cal.App.4th 478, 516 (1998) (personal injury coverage for "malicious prosecution" was not "illusory" notwithstanding fact that Cal. Ins. Code §533 precluded indemnity for such claims because express promise to provide "malicious prosecution" coverage required insurer to provide a defense against such claims).

[27] Security Breach Liability

a. We will pay for both "loss" that the "insured" becomes legally obligated to pay and "defense expenses" as a result of the "claim" first made against the "insured' during the "policy period" or during the applicable Extended Reporting Period, for a "wrongful act" or a series of

> Any actual or alleged neglect, breach of duty or omission by an "insured" that results in:
>
> (1) A "security breach"; or
>
> (2) A "computer system" transmitting, by e-mail or other means, a "virus' to another person or organization.[28]

In turn, the term "security breach" is defined as:

> the acquisition of "personal information" held within the "computer system" or nonelectronic format which in the care, custody or control of the "insured" or "authorized third party" by a person:
>
> a. Who is not authorized to have access to such information; or
>
> b. Who is authorized to have access to such information but whose access results in the unauthorized disclosure of such information.[29]

As drafted, the intent is to provide limited errors and omissions coverage for liability resulting from the non-authorized disclosure or dissemination of "personal information."[30]

"interrelated wrongful acts" taking place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the "policy period".

b. We will pay for both "loss" that the "insured" becomes legally obligated to pay and "defense expenses" as a result of the "claim" in the form of a "regulatory proceeding" first made against the "insured' during the "policy period" or during the applicable Extended Reporting Period, for a "wrongful act" or a series of "interrelated wrongful acts" taking place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the "policy period".

(ISO Form EC00100114 [2013] Sec.VII.35).

[28] ISO Form EC00100114 [2013] Sec.VII.18.

[29] ISO Form EC00100114 [2013] Sec.VII.30.

[30] The term "personal information" is defined as:

The overall drafting intent appears to be to provide liability coverage for the improper dissemination of "personal information" from a "computer system". However, and significantly, the ISO "security breach" definition as written applies to dissemination of "personal information" "held within … nonelectronic format", which appears broad enough to include dissemination of information stored by traditional, non-electronic means (i.e. paper records, microfiche, etc.) As a result, the "Security Breach Liability" coverage provided by the ISO form appears broad enough to apply to liability for

---

> …any information not available to the general public for any reason through which an individual may be identified including, but not limited to, an individual's:
>
> a. Social security number, driver's license number;
>
> b. Protected health information;
>
> c. Financial account numbers;
>
> d. Security codes, passwords, PINs associated with credit, debit or charge numbers which would permit access to financial accounts; or
>
> e. Any other nonpublic information as defined in "privacy regulations."

(ISO Form EC00100114 [2013] Sec.VII.21)

The term "privacy regulations" is defined, in turn, as:

> [] any of the following statutes and regulations, and their amendments, associated with the control and use of personally identifiable financial, health or other sensitive information including, but not limited to:
>
> a. The Health Insurance Portability and Accountability Act of 1996 (HIPPA) (Public Law 104-191);
>
> b. The Health Information Technology for Economic and Clinical Health Act (HITECH) (American Recovery and Reinvestment Act of 2009);
>
> c. The Gramm-Leach-Bliley Act of 1999;
>
> d. Section 5(a) of the Federal Trade Commission Act (15 U.S.C. 45(a)), but solely for alleged unfair or deceptive acts or practices in or affecting commerce;
>
> e. The Identity Theft Red Flags Rules under the Fair and Accurate Credit Transactions Act of 2003; or
>
> f. Any other similar state, federal or foreign identity theft or privacy protection statute or regulation.

(ISO Form EC00100114 [2013] Sec.VII.24).

improper dissemination of "personal information" even in situations which do not involve the storage and retrieval of "personal information" from a "computer system."

With respect to improper dissemination of "personal information" from a "computer system", the definition of "computer system" appears to be limited to physical computing devices, software and communication networks "owned, leased or operated" by the named insured.[31] As a result, potential coverage disputes may arise in situations where the insured is potentially liable for improper dissemination of "personal information" stored on "computer systems" owned and operated by third parties, such a "cloud based" network storage systems.[32] In such situations where the third party "computer system" is not "owned" by the insured, the dispute would likely focus on the contractual arrangements between the insured and the third party "computer system" provider to determine whether these third party systems are being "leased" to or "operated" by the named insured as required to fall within the scope of coverage.

---

[31] "Computer system" means the following which are owned, leased or operated by you:

a. Computers, including Personal Digital Assistants (PDAs) and other transportable or handheld devices, electronic storage devices and related peripheral components;

b. Systems and applications software; and

c. Related communications networks;

by which "electronic data' is collected, transmitted, processed, stored or retrieved.

(ISO Form EC00100114 [2013] Sec.VII.5).

[32] See https://en.wikipedia.org/wiki/Cloud_storage (last accessed January 21, 2016) (defining "cloud storage" as "a model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.")

Outside of these potential coverage limitations, the ISO form "Security Breach Liability" coverage provides coverage for "loss" defined broadly to include penalties and punitive damages (which are not uninsurable) as well as compensatory damages.[33]

Since the coverage is written to also include "regulatory proceeding(s)"[34] against the insured, the "Security Breach Liability" liability coverage would potentially provide defense and indemnity coverage in connection with proceedings by the Federal Trade Commission, Federal Communication Commissions and/or other similar governmental regulatory agencies. As a result, the liability coverage provided is not limited to civil "suits" as is often the case with many standardized liability coverages. *See, e.g., Foster-Gardner, Inc. v. Nat'l Union Fire Ins. Co.,* 18 Cal.4th 857, 882 (1998) (policy limiting defense coverage to "suit[s]" against insured did not apply to EPA remediation order since "suit" required a civil action commenced by filing a complaint in court); *Lapham-Hickey Steel Corp. v. Prot. Mut. Ins. Co*., 166 Ill.2d 520, 530, 655 N.E.2d 842, 847 (1995) (same).

C. Programming Errors And Omissions Liability (third party)

"Programming Errors And Omissions Liability" coverage is written in terms of "wrongful acts" defined as "[a]ny actual or alleged programming error or omission that results in the disclosure of your client's 'personal information' held within the 'computer system.'" (ISO Form EC00100114 [2013] Sec.VII.35).

---

[33] See, *supra,* fn.25.

[34] "'Regulatory proceeding' means an investigation, demand or proceeding brought by, or on behalf of, the Federal Trade Commission, Federal Communications Commissions or other administrative or regulatory agency, or any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity." (ISO Form EC00100114 [2013] Sec.VII.28).

While similar in some respects to "Security Breach Liability" coverage, the scope of liability coverage is drafted to apply only to the improper dissemination of the "personal information" of a "client" of the named insured. Additionally, the "Programming Errors And Omissions Liability" coverage is written only to apply to "personal information" "held" within a "computer system" and is not drafted to include such information "held within .. nonelectronic format".

Another significant coverage limitation is that improper disclosure must be the result of an "actual or alleged programming error or omission". However, the ISO "Programming Errors And Omissions Liability" insuring agreement does not require the "programming error or omission" to have been committed by the insured or one of the insured's agents.

Taken together, as drafted the "Programming Errors And Omissions Liability" coverage is written to apply to liability situations where "personal information" of an insured's client is improperly disseminated due to a "programming error or omission" committed by any party. As a result, the "Programming Errors And Omissions Liability" coverage is distinct from "Security Breach Liability" coverage which is directed at the improper dissemination of private information caused by third party network intrusions, whether or not those intrusions involved any particular "programming errors or omissions" in the computer system.

Assuming the conditions for "Programming Errors And Omissions Liability" coverage are satisfied, the resulting coverage applies broadly to "loss" defined to include

compensatory damages as well as some instances of punitive damages and penalties (where insurable).[35]

D. Replacement Or Restoration Of Electronic Data (first party)

This first party coverage applies to "'loss' of 'electronic data' or 'computer programs' stored within the 'computer system' resulting directly from an 'e-commerce incident' sustained during the 'policy period'."[36] The definitions of "electronic data"[37] and "computer programs"[38] indicate that the provided coverage is limited to electronically stored information and/or programs and does not include "tangible" property as is typically covered under standardized CGL forms.[39]

The "loss" definition provides coverage for "[t]he cost to replace or restore 'electronic date' or computer programs' as well as the cost of data entry, reprogramming and computer consultation services."[40] At the same time, the "loss" definition does not

[35] See, *supra,* fn.25.

[36] ISO Form EC00100114 [2013] Sec.I.4.

[37] "'Electronic data' means digital information, facts, images or sounds stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software) on electronic storage devices, including, but not limited to, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other mediation which are use with electronically controlled equipment. 'Electronic date' is not tangible property. [¶] 'electronic data' does not include your 'electronic data' that is licensed, leased, rented or loaned to others." " (ISO Form EC00100114 [2013] Sec.VII.9).

[38] "'Computer program' means a set of related electronic instructions, which direct the operation and function of a computer or devices connected to it, which enables the computer or device to receive, process, store or send 'electronic data'." " (ISO Form EC00100114 [2013] Sec.VII.5).

[39] See *supra*, Sec.III.A.

[40] ISO Form EC00100114 [2013] Sec.VII.18.b.

include costs associated with "duplicate research that led to the development of your 'electronic data' or 'computer programs'."[41]

The primary coverage issue is the requirement that the "loss" be the "direct[]" "result[]" of an "e-commerce incident". "E-commerce incident" is defined as a "virus", "[m]alicious code" or "[d]enial of service attack" "introduced into or enacted upon the 'computer system' (including 'electronic data') or a network to which it is connected, that is designed to damage, destroy, delete, corrupt or prevent the use or of access to any part of the 'computer system' or otherwise disrupt its normal operation."[42]

The term "e-commerce incident" appears to suggest that coverage would be restricted to data losses associated with an insured's commercial operations (i.e. on-line sales, etc.) However, the actual definition of "e-commerce incident" is not limited to commercial systems or transactions. As a result, the scope of coverage appears to extend to all "losses" of "electronic data" and/or "computer programs" which are "caused directly" by third-party system attacks, whether or not the affected "electronic data" or "computer programs" are used for commercial transactions. As a result, public entities could still benefit from so-called "e-commerce incident" coverage, so long as the entity confirms that applicable policy language does not actually restrict coverage to data or programs used in connection with commercial transactions.

[41] *Id.*

[42] ISO Form EC00100114 [2013] Sec.VII.8.

Similar to "Security Breach Liability" coverage, first party coverage for "Replacement or Restoration of Electronic Data" as written is limited to data and/or programs "stored within the 'computer system'[.]" As a result, there may be a question whether the coverage would apply to data and/or programs stored within third-party computer systems or networks, such as "cloud"-based networks.[43]

E. Cyber-Extortion (first party)

Coverage for "Extortion Threats" provides first-party coverage for "'loss' resulting directly from an 'extortion threat' communicated to you during the 'policy period."[44] The term "extortion threat" is defined as:

> a threat or series of related threats:
>
> a. To perpetuate an "e-commerce incident";
>
> b. To disseminate, divulge or utilize;
>
> (1) Your proprietary information; or
>
> (2) Weaknesses in the source code;
>
> within the "computer system" by gaining unauthorized access to the "computer system";
>
> c. To destroy, corrupt or prevent normal access to the "computer system" by gaining unauthorized access to the "computer system";

[43] See *supra* fns.31-32 and accompanying text.

[44] ISO Form EC00100114 [2013] Sec.I.4.

d. To inflict "ransomware" on the "computer system" or a network to which it is connected; or

c. to publish your client's "personal information".[45]

The coverage provided is similar to "Replacement or Restoration of Electronic Data" coverage in that it applies to the "threat" of an "e-commerce incident" instead of an actual "e-commerce incident." However, it is significantly broader in that it also applies to: (1) "losses" association with threatened dissemination of "proprietary information", "[w]eaknesses in the source code" and client "personal information"; as well as (2) "ransomware"[46] attacks which threaten to lock insured out of their own "computer systems." At the same time, "Extortion Threats" coverage is distinct from "Replacement Or Restoration Of Electronic Data" coverage in that "Replacement Or Restoration Of Electronic Data" can provide coverage for costs associated with actual data loss, while "Extortion Threats" coverage does not.

Since "Extortion Threat" coverage is directed towards threats of data loss rather than actual data loss, the "loss" definition is restricted to "[e]xtortion expenses" and "ransom payments."[47] As a result, this first party coverage is directed towards financial costs

[45] ISO Form EC00100114 [2013] Sec.VII.12.

[46] "'Ransomware' means any software that encrypts 'electronic date' held within the 'computer system' and demands a 'ransom payment" in order to decrypt and restore such 'electronic data.'" (ISO Form EC00100114 [2013] Sec.VII.27).

[47] ISO Form EC00100114 [2013] Sec.VII.18.c.

associated with the insured's responding to threats of computer intrusion[48] including, but not limited to, "ransom" payments made by the insured to the threatening party.[49]

Significantly, the scope of "loss" resulting from an "extortion threat" can vary depending on how the particular "threat" is handled by the insured. As a result, the ISO reporting provisions for "Extortion Threats" include additional contractual requirements for the insured to follow such as: (1) reporting the "threat" to "local law enforcement officials"; (2) additional examination under oath and proof of loss requirements; (3) determining the credibility of any "extortion threat"; and (4) attempting to contact a security firm before making any "ransom payment[s]".[50] Also, coverage for certain "extortion expenses" can

[48] "Extortion expenses' means:

a. Fees and costs of:

(1) A security firm; or

(2) A person or organization;

hired with our consent to determine the validity and severity of an 'extortion threat' made against you;

b. Interest costs paid by your for any loan form a financial institution taken by your to pay a ransom demand;

c. Reward money paid by your to an "informant" which leads to the arrest and conviction of parties responsible for "loss"; and

d. Any other reasonable expenses incurred by your with our written consent, including:

(1) Fees and costs of independent negotiators; and

(2) Fees and costs of a company hired by you upon the recommendation of the security firm, to protect your "electronic data' from further threats.

(ISO Form EC00100114 [2013] Sec.VII.11).

[49] "Ransom payment" means a payment made in the form of cash. (ISO Form EC00100114 [2013] Sec.VII.26).

[50] ISO Form EC00100114 [2013] Sec.VI.14.b.

require prior consultation with third parties (i.e. security firms, independent negotiators, etc.) and pre-approval of the insurer.[51]

To further deal with the problem of potentially large losses caused by the insured's mishandling of cyber threats, some non-ISO forms may have additional provisions purportedly giving the insurer the option to eliminate cyber threat coverage if the existence of that coverage becomes known to the general public and/or threatening party.[52]

F. Business Income (first party)

Coverage for "Business Income and Extra Expenses" applies to "loss" caused by an "interruption" which is the result either of an "e-commerce incident" or an "extortion threat" occurring during the policy period.[53] The term "loss" in this context is defined **as** "[t]he actual loss of 'business income' you sustain and/or 'extra expense' you incur."[54]

---

[51] See fn.48.

[52] *See* First Party Computer Securing Coverage Endorsement (potentially included with Beazley Information Security & Privacy Insurance With Electronic Media Liability Coverage policy form), Sec. FPC-C "OBLIGATIONS IN THE EVENT OF AN EXTORTION THREAT", "A. Insured's Duty of Confidentiality [¶] (i) The Insured shall use it best efforts at all times to ensure that knowledge regarding the existence of this insurance for Cyber Extortion Loss afforded by the Policy is kept confidential. The Underwriters may terminate the insurance provided by this policy for Cyber Extortion Loss upon ten (10) days written notice to the Named Insured if the existence of insurance for Cyber Extortion Loss provided by this Policy becomes public knowledge or is revealed to a person making an Extortion Threat through no fault of the Underwriters."

[53] ISO Form EC00100114 [2013] Sec.I.6.

[54] ISO Form EC00100114 [2013] Sec.VI.18.d.

"Business income" is defined in relevant part at "net income … that would have been earned or incurred" and "[c]ontinuing normal operating expenses incurred, including payroll." (ISO Form EC00100114 [2013] Sec.VI.2).

"Extra expenses" is defined in relevant part as "necessary expenses you incur: a. During an "interruption' that you would not have incurred if there had been no 'interruption' or b. To avoid or minimize the suspension of your 'e-commerce activities." (ISO Form EC00100114 [2013] Sec.VI.13).

As a result, the contractual intent is to provide first-party coverage for lost business revenue, costs associated with normal business activities and additional, resulting expenses associated with an "e-commerce incident" or "extortion threat" during the policy period.

G. Public Relations Expenses (first party)

Coverage for "Public Relations Expenses" applies to "loss" due to "'negative publicity' resulting directly from an 'e-commerce incident' or a 'security breach'" occurring during the applicable policy period.[55]

The term "public relation expenses" is defined as "'a. Fees and costs of a public relations firm; and b. Any other reasonable expenses incurred by you with our written consent; to protect or restore your reputation solely in response to 'negative publicity'."[56] "Negative publicity" is, in turn, defined as "information which has been made public that has caused, or is reasonably likely to cause, a decline or deterioration in the reputation of the 'named insured' or of one or more or its products or services."[57]

As written, this coverage is designed to apply to reasonable costs associated with mitigating the negative reputational impact suffered by an insured as a direct result of public reporting of computer security breaches.

[55] ISO Form EC00100114 [2013] Sec.I.7.

[56] ISO Form EC00100114 [2013] Sec.VI.25.

[57] ISO Form EC00100114 [2013] Sec.VI.20.

H. Security Breach Expenses (first party)

Finally, coverage for "Security Breach Expenses" applies to "'loss' resulting directly from a 'security breach' sustained during the 'policy period.'"[58] The term "loss" in this context refers to "security breach expenses" defined in turn to include costs associated with the investigation, notification and remediation of a "security breach".[59]

As written, this coverage is designed for the specific expenses associated with identifying and remediating security intrusions into the computer system itself, including: (1) providing information to members of the public who may have been affected by the intrusion; and (2) monitoring costs to determine if the security breach has affected third parties (i.e. third-party credit monitoring services).[60]

---

[58] ISO Form EC00100114 [2013] Sec.I.8.

[59] "Security breach expenses" means:

a. Costs to establish whether a "security breach" has occurred or is occurring;

b. Cost to investigate the cause, scope and extent of a "security breach" and to identity any affected parties;

c. Costs to determine any action necessary to correct or remediate the conditions that led to or resulted from a "security breach";

d. Costs to notify all parties affected by a "security breach";

e. Overtime salaries paid to "employees" assigned to handle inquiries from the parties affected by a "security breach";

f. Fees and costs of a company hired by your for the purposes of operating a call center to handle inquiries from the parties affected by a "security breach";

g. Post-event credit monitoring costs for the parties affected by a "security breach" for up to one year from the date or notification to those affected parties of such "security breach"; and

h. Any other reasonable expenses incurred by you with our written consent.

"Security breach expenses" do not include any costs or expenses associated with upgrading, maintaining, improving, repairing or remediating any "computer system" as a result of a "security breach".

(ISO Form EC00100114 [2013] Sec.VI.30).

[60] See, *supra*, fn.59.

I. Significant Exclusions

1. Mechanical Failure/Maintenance Issues

As written, cyber risk policies are designed to provide coverage for incidents associated with acts or omissions by the insured, the insured's agents and/or actions by third-parties disrupting or improperly accessing the insured's computer systems. Conversely, these policies are not designed to provide coverage associated with normal mechanical failures, maintenance of computer networks or normal costs associated with upgrades to computer networks and systems.

To that end, the ISO form contains several exclusions and other coverage limitations designed to exclude coverage for such normal operating costs and expenses, including:

(1) the "unexplained or indeterminable failure" exclusion;[61]

(2) the "insufficient capacity" exclusion;[62]

(3) the "internet failure" exclusion;[63]

(4) the "power failure" exclusion;[64]

---

[61] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of any unexplained or indeterminable failure, malfunction or slowdown of the 'computer system', including 'electronic data' and the inability to access or properly manipulate the 'electronic data'." (ISO Form EC00100114 [2013] Sec.V.5).

[62] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of any 'interruption' in normal computer function or network service or function due to insufficient capacity to process transactions or due to an overload of activity on the 'computer system' or network. However, this exclusion shall not apply if such 'interruption' is caused by an 'e-commerce incident.'" (ISO Form EC00100114 [2013] Sec.V.6).

[63] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of a complete or substantial failure, disablement or shutdown of the Internet, regardless of the cause." (ISO Form EC00100114 [2013] Sec.V.7).

[64] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of any failure of , reduction in or surge of power." (ISO Form EC00100114 [2013] Sec.V.8).

(5) the "satellite failure" exclusion;[65]

(6) the "computer system upgrade" exclusion;[66] and

(7) the "unintentional errors in data entry" exclusion.[67]

As written, these exclusions appear designed to function similarly to "deterioration", "wear and tear" and "inherent vice" exclusions in standardized property coverages. *See, e.g., Brodkin v. State Farm Fire & Cas. Co.,* 217 Cal.App.3d 210, 217 (1989); *Murray v. State Farm Fire & Cas. Co*., 219 Cal.App.3d 58, 63 (1990)

2. Intentional Act/Knowledge Of Falsity/Fraudulent Act Exclusions

As is the case with many first and third party coverages, cyber risk policies contain exclusions precluding coverage for "intentional acts",[68] "fraud" and "publication of materials" with "knowledge of falsity" by the insured.[69]

---

[65] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of any malfunction or failure of any satellite." (ISO Form EC00100114 [2013] Sec.V.10).

[66] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of cost associated with upgrading or improving the 'computer system' regardless of the reason for the upgrade." (ISO Form EC00100114 [2013] Sec.V.21).

[67] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of any unintentional errors or omissions in the entry of 'electronic data' into the 'computer system'." (ISO Form EC00100114 [2013] Sec.V.23).

[68] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of any criminal, dishonest, malicious or fraudulent act or any willful violation of any statue or regulation committed by an 'insured' acting alone or in collusion with others. However, this exclusion shall not apply to dishonest, malicious or fraudulent acts committed by an "employee" with give rise to a 'claim' or 'loss' covered under Insuring Agreement 2. Security Breach Liability." (ISO Form EC00100114 [2013] Sec.V.19).

[69] "We will not be liable for 'loss' or 'defense expenses': … Based upon, attributable to or arising out of any oral or written publication of material, if done by an "insured" or at an "insured's" direction with knowledge of its falsity." (ISO Form EC00100114 [2013] Sec.V.11).

With respect to "intentional act" exclusions and similar coverage limitations for "willful" acts as applied to standardized coverages, a primary focus of coverage litigation has been to what extent the coverage limitations apply to "innocent" co-insureds (i.e. insureds who are vicariously liable for the intentional/willful acts of another insured, co-insureds whose conduct does not rise to the level of intentional/willful injury, etc.) *See, e.g., Century-Nat'l Ins. Co. v. Garcia,* 51 Cal.4th 564, 568 (2011) (intentional act exclusion in first party fire loss policy did not apply to innocent co-insured notwithstanding fact that co-insured intentionally and criminally caused the fire); *Minkler v. Safeco Ins. Co. of Am.*, 49 Cal.4th 315, 322 (2010) (notwithstanding fact that exclusion was written to preclude coverage for injuries intentionally caused by "an insured", exclusion did not apply to parents of minor who allegedly committed sexual molestation because "severability of interests" provision created reasonable expectation that intentional act exclusion would separately apply to each insured).

Given the potential for insureds to suffer loss and/or be liable for deliberate conduct by employees and other agents of the insured in connections with cyber risks, the ISO "intentional act" exclusion contains an express exception for "dishonest, malicious or fraudulent acts committed by an 'employee' which give rise to a 'claim' or 'loss' covered under Insuring Agreement 2. Security Breach Liability."[70] In turn, the term "employee" is defined broadly as:

> any natural person who was, now is or will be:
>
> a. Employed an a full- or part-time basis;

[70] See fn.68

b. Furnished temporarily to you to substitute for a permanent employee on leave or to meet seasonal or short-term workload conditions;

c. Leased to you by a labor leasing firm under an agreement between you and the labor leasing firm to perform duties related to the conduct of your business, but does not mean a temporary employee as defined by Paragraph 10.b;

d. An officer;

e. A director, trustee or manager (if a limited liability company);

f. A volunteer worker; or

g. A partner or member (if a limited liability company);

of the "named insured" and those of any organization qualifying a "subsidiary" under the terms of this Policy, but only which acting within the scope of their duties as determined by the "named insured" or such "subsidiary".[71]

Due to this expansive definition, it appears that the ISO form is written to provide "Security Breach Liability" notwithstanding the injurious intent by employees, officers, leased workers, managers, volunteers or partners to commit the security breach so long at the breach was not specifically "intended" by the insured's control group (i.e. the board of directors as a whole, etc.)

[71] ISO Form EC00100114 [2013] Sec.VII.10.

Another important restriction on the scope of the ISO "intentional act" exclusion is the promise to provide defense coverage against claims (other than patent or trade secret violations claims) which, as alleged, would otherwise fall within the exclusion:

> With the exception of "claims" excluded under Exclusion 13., we will defend "claims" first made against an "insured" alleging such acts or violations until final adjudication is rendered against that "insured".[72]

Along with this broad promise to provide a defense against claims which, as alleged, could fall within the "intentional act" exclusion, it includes policy language promising "that Final adjudication rendered against one 'insured" shall not be imputed to any other 'insured.'"[73] As such, for the "intentional act" exclusion to apply, it would appear to require a separate, final adjudication as to the intent of the named insured (i.e. control group).

These broad limitations on the ISO "intentional act" exclusion raise an issue as to whether a reservation of rights raising that exclusion would trigger the insured's right to independent counsel. In California as in many other jurisdictions, it has long been established that when an insurer raises an "intentional act" exclusion as a coverage defense via a reservation of rights, this creates a "conflict of interest" triggering the insured's right to independent counsel based on the view that panel defense counsel

[72] (ISO Form EC00100114 [2013] Sec.VII.19); s*ee also* ISO Form EC00100114 [2013] Sec.V.13 (exclusion applicable to "loss" or "defense expense" "[b]ased upon, attributable to or arising out of any actual or alleged patent or trade secret violation, including any actual or alleged violation of the Patent Act, the Economic Espionage Act of 1996 or the Uniform Trade Secrets Act and their amendments).

[73] ISO Form EC00100114 [2013] Sec.VII.19.

would be in a position to "shape the defense" in such a way as to favor the insurer's "intentional act" coverage defense. *See, e.g.*, Cal. Civ. Code §2860; *San Diego Navy Fed. Credit Union v. Cumis Ins. Soc'y, Inc.*, 162 Cal.App.3d 358 (1984); *Pub. Serv. Mut. Ins. Co. v. Goldfarb*, 53 N.Y.2d 392, 401, 425 N.E.2d 810 (1981).

However, the language in the ISO "intentional act" exclusion indicating "that Final adjudication rendered against one 'insured" shall not be imputed to any other 'insured'" would suggest that panel defense counsel would not be in any position to "shape the defense" to fall within the exclusion in situations where the named insured's intent is not at issue in the underlying action. If so, arguably there is no conflict of interest requiring independent defense counsel. *See Dynamic Concepts, Inc. v. Truck Ins. Exch.*, 61 Cal.App.4th 999, 1006 (1998) (explaining there is no "entitlement" to independent counsel "where the coverage issue is independent of, or extrinsic to, the issues in the underlying action").

However, to the extent both the named insured and "employees" of the insured are co-defendants with respect to cyber liability claims potentially falling within the "intentional act" exclusion, it would follow that the named insured still would have the right to independent counsel based on the potential for panel defense counsel to "shape the defense" to assign liability to the named insured (as opposed to "employees' of the insured) for conduct within the exclusion. Civ. Code §2860; *Cumis, supra,* 162 Cal.App.3d 358. Moreover, the insurer would not have the right to insist on the same defense counsel for both the named insured and "employees" of the named insured

where their interests are in conflict (i.e. the named insured has an affirmative cross-claim against an "employee" or vice versa). *See, e.g., O'Morrow v. Borad*, 27 Cal.2d 794, 800-801 (1946).[74]

In this context, it should be noted that the right to independent counsel under Civil Code §2860 only applies "the provisions of a *policy of insurance* imposed a duty to defend *upon an insurer*…." (Emphasis added). However, coverage provided by a memorandum of coverage issued by a joint powers association is technically not "insurance", although it provides many of the same risk-managing functions of an insurance policy. *See* Cal. Govt. Code §990.8(c) (providing that pooling agreements such as memoranda of coverage "shall not be considered insurance nor be subject to regulation under the Insurance Code."); *see also Orange Cnty. Dist. v. Ass'n of Cal. Water Etc. Authority*, 54 Cal.App.4th 772, 777 (1977) (explaining that where contributions or premiums are based on loss history and the member agency ultimately pays back to the JPA amounts paid out on its behalf, there is "no shifting of the risk of loss. Thus, the arrangement lacks a fundamental feature of 'insurance.'")

As a result, there is a strong argument that a public agency receiving cyber risk coverage under a memorandum of coverage would not be entitled to independent counsel even in situations where the member otherwise would be entitled to independent counsel if the coverage had been provided by an insurer under an insurance policy.

[74] Significantly in this context, the ISO form's "intra-insured" exclusion contains an express exception to restore coverage for claims brought against the named insured by an "employee" "as the result of a 'security breach.'" *See* (ISO Form EC00100114 [2013] Sec.V.22).

3. "Related" Claims Exclusions

As noted above, cyber risk policies are generally provided on a "claims made and reported" basis which allows the insurer to more carefully control losses associated with specific policy years and thereby price premiums accordingly for future years. *See, supra,* Sec.IV.A.2; *see also Root v. Am. Equity Specialty Ins. Co.*, 130 Cal.App.4th 926, 944, 946 (2005) ("The key is the pricing of premiums. The core idea behind the move to claims made insurance policies was to close *the gap* between the time when the insurer prices a risk and the time when the insurer may incur an obligation to pay on that risk. … By the end of the policy period the insurer definitely knows whether X risk generated any claims in Y period….") (emphasis in original).

Consistent with the administrative function of "claims made and reporting" policies, the ISO form contains policy language designed to preclude coverage for claims which should have been reported during the applicable reporting period. For example, the ISO form includes a "pending claims" exclusion which precludes coverage for claims reported during the applicable policy period which are "[b]ased upon, attributable to or arising out of any 'claim', 'suit' or other proceeding against an 'insured' which was pending or existed prior to the 'policy period', or arising out of the same or substantially the same facts, circumstances or allegation" as the earlier "'claim, 'suit' or other proceeding."[75]

[75] ISO Form EC00100114 [2013] Sec.V.15.

Similarly, the ISO form includes a "related wrongful acts" exclusion which precludes coverage for claims "[b]ased upon, attributable to or arising out of the same facts, 'wrongful acts' or 'interrelated wrongful acts' alleged or contained in any 'claim' which has been reported, or in any circumstances of which notice has been given, under any insurance policy of which this Policy is a renewal or replacement."[76]

The ISO form's definition of "claim" is restricted to: (1) "[a] written demand for monetary or nonmonetary damages, including injunctive relief"; (2) "[a] civil proceeding commenced by the service or a complaint or similar proceeding" and (3) with respect to "Security Breach Liability" a "'regulatory proceeding' commenced by the filing of a notice of charges, formal investigative order, services of summons or similar document…."[77]

At the same time, the reporting conditions of the ISO form require the insured to notify the insurer "[i]n the event of either an occurrence or offense that *may* result in a 'claim' against an 'insured' or a 'loss' or situation that *may* result in a 'loss' covered by this Policy…." (Emphasis added).[78] As a result, there is a potential for coverage disputes between the insured and insured whether the insured was aware of information prior to the policy period which indicated that a covered "loss" or "claims" *may* have been sufficiently probable as to trigger the insured's reporting duties.

[76] ISO Form EC00100114 [2013] Sec.V.18.

[77] ISO Form EC00100114 [2013] Sec.VII.3.

[78] ISO Form EC00100114 [2013] Sec.VI.14.

However, unlike other "claims made and reporting" policies, the ISO form appears to assign the claim to the policy period when the formal demand is made on the insured as opposed to the policy period where the potential claim was first reported to the insurer.[79] As a result, it appears that the "potential claim" reporting requirements under the ISO form are designed primarily to provide opportunities for the insurer to be proactive and potentially reduce financial exposure for potential "losses" or "claims" as opposed to providing the insurer with the administrative convenience of assigning potential "losses" or "claims" to the policy period when they are first reported.

VII. AN "OUNCE OF PREVENTION" – MANAGING CYBER RISKS

A. Pre-Claim Issues

Generally speaking, the best defense for entities with respect to cyber risks is to follow industry "best practices" for the maintenance of confidential information on computer networks and maintaining computer network security overall. These practices include:

[79] *Compare* ISO Form EC00100114 [2013] Sec.VI.14 ("A 'claim' brought by a person or organization seeking damages will be deemed to have been made when the 'claim is received by an 'insured'") *with Helfand v. Nat'l Union Fire Ins. Co*., 10 Cal.App.4th 869, 889 (1992) (insurance reporting provision stating that "[i]f during the policy period ...: [¶] (i) the Company ... or the Insureds shall receive written or oral notice from any third party that it is the intention of such third party to hold the Insureds responsible for the results of any specified Wrongful Act by the Insureds while acting in the capacities aforementioned; or [¶] (ii) The Company ... or the Insureds shall become aware of any occurrence which may subsequently give rise to a claim being made against the Insureds in respect of any such Wrongful Act; and [¶] shall in either case, during such period give written notice to the Insurer of the receipt of such written or oral notice under (i) above or such occurrence under (ii) above, then any claim which may subsequently be made against the Insureds arising out of such Wrongful Act shall for the purpose of this policy be treated as a claim *made during the currency hereof*.") (emphasis added).

1) **Knowing Your Data –** Identifying what information is stored on computer systems and where the data originates. Sensitive information can include credit card or bank account numbers of customers, usernames and passwords, employee health records, information received from vendors, or other data.

2) **Defending Your Data** – As entities grow, data is often moved or archived, both on and off site. To effectively protect this data, there should be periodic reviews where and how that data is stored, including onsite backups and cloud computing. Additional best practices should include: (1) destroying records of information no longer needed; (2) encryption of data stored on company systems; (3) encryption of data being transmitted between your computers and any network access points; and (4) data backup protocalls, including testing backups to make sure they can be utilized in the event of a system failure.

3) **Defend Yourself** – Employees are often the largest source of security vulnerability for any entity. As a result, entities should provide employees access only to those systems and information they need to do their jobs. Also, entities should educate their employees and implement guidelines for technology security. These security protocalls can include password standards and guidelines on acceptable internet use. Also, entities should utilize multiple and overlapping protections to guard against failures in any specific technology or protection method, including: (1) regularly updated firewalls, antivirus, and web security solutions; and (2) ensuring that employees accessing the network remotely install and maintain firewalls on their home systems.

4) **Operate Securely** – All operating systems and software should be updated regularly. Any devices that handle sensitive information like payroll or point of sale (POS) functions should be separate from devices that do routine services (i.e. email). Any banking services should require multi-factor authentication and any fund transfers should be verified by more than one authorized employee. Employees should not use public or unsecure wireless connections to conduct any company business, such as checking email, unless they are using a secure connection (e.g. corporate VPN access and/or an SSL protected web email server). Passwords should be changed frequently, and standards for strong passwords for all employees should be enforced.

5) **Make a Plan** – entities should create a plan for each type of incident they may face which could increase the risk of a network intrusion: i.e. a lost laptop, smart phone or thumb drive with unencrypted data; an external breach, or malware.

B. Post-Claim Issues

In addition to developing a plan to response to routine incidents which could lead to security breaches (i.e. lost cellphones and laptops), it is advisable for entities to develop a general plan to respond to computer network intrusions and/or unauthorized dissemination of information from computer systems. Issues to consider in developing such a plan should include:

1) **Resecuring the Network/Confidential Information –** Given the pervasive reliance on computer networks and other systems, there are few (if any) entities that could continue to perform their essential functions without continue access to the system. At the same time, security breaches can create ongoing liability

exposure to the extent breaches create or involve ongoing security risks that can be exploited by outside third parties. As a result, it is advisable to have a plan designed to identify and resolve network security issues on an emergency basis including, when necessary, hiring outside personnel to resecure the network and/or restore its functionality. In addition to helping an entity return to normal operations, such activities may be useful from a third party liability perspective insofar as they demonstrate "reasonable", non-negligent conduct by the entity in responding to the incident. Moreover, the costs of these services may be covered by first party coverages for "Security Breach", "Replacement Or Restoration Of Electronic Data" and/or Cyber Threat" under some cyber risk policies.

2) **Notification Protocalls –** Breach of a computer system involving confidential information of clients and/or other third parties can put an entity in a conflicted situation of needing to protect the interests of those affected third parties as opposed to the entity's natural desire to protect its own reputational interests. This same potential conflict can be exacerbated in situations involving threats rather than actual security breaches or system weakness which have not yet been resolved.

Nonetheless, as laws such as California's Information Practices Act and recent case law make clear, entities have outstanding legal duties to provide reasonable notice to affected third parties and take reasonable measures to protect those same parties from the financial and reputational exposure caused by the breach. As a result, an entity's response to any actual or threatened network intrusion or improper dissemination of data should include a careful assessment of: (1)

whether and how the potentially affected third parties, law enforcement and/or insurers should be notified of the situation; and (2) when is the earliest opportunity such notice can be provided without increasing the risk of further data losses or network intrusions, such as may be the case with unresolved network security issues and/or cyber threats.

Providing notice in a reasonable way is also important from a third-party liability perspective insofar as it both satisfies statutory notice requirements and demonstrates reasonable, non-negligent conduct on the part of the entity. Moreover, providing notice to proper parties on a timely basis may be required to satisfy the prerequisites for many first party coverages provided by cyber risk policies.

3) **Coordination of Response** – The fact that a cyber incident can implicate the direct financial interests of the entity (first party losses) as well as create liability exposure to affected third parties (third party losses), indicates that an entity responding to a cyber incident should be mindful of the overall impact such an incident may have. It may often be advisable for an entity to "front load" its efforts in responding to the initial network breach (i.e. hiring system and security experts, providing data protection services to affected third parties) based on the understanding that these efforts may reduce the entities overall, third party exposure.

Moreover, to the extent the entity notifies and involves its cyber risk carrier earlier rather than later in the process, this could have the added benefits of: (1) satisfying notice requirements for triggering cyber risk coverages; (2) making

available pre-approved experts to help the entity address and resolve network security and customer notice issues, as well as public relation experts in appropriate situations; and (3) potentially securing insurer "buy in" to working with the entity on formulating an overall response strategy to the incident as a way to minimize then entity's overall exposure.