**2019 PARMA ANNUAL RISK MANAGERS CONFERENCE**

**FEBRUARY 12, 2019 – 8:30 a.m. to 10:00 a.m.**

**Disneyland Hotel**

**Anaheim, CA**

THE ABCS OF CYBER – ASSESSING VULNERABILITIES, BALANCED RESPONSES, AND COVERAGE PITFALLS

|  |
| --- |
| **Moderator**  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 |
| **Panelists**  Graham Van Leuven  Clyde & Co.  101 Second Street, 24th Floor  San Francisco, CA 94105  (415) 365-9800 FAX: (415) 365-9801  Graham.VanLeuven@clydeco.us |
| Lejf E. Knutson  McCormick, Barstow, Sheppard, Wayte & Carruth  7647 N. Fresno Street  Fresno, California 93720  (559) 433-1300 FAX: (559) 433-2300  E-mail: lejf.knutson@mccormickbarstow.com |
|  |

1. Overview

This session will build on public entities' growing knowledge and introduce new concepts and issues for consideration. It explains the general coverages for cyber risks and helps to identify potential gaps in coverage. The goal of this session is to help participants understand and evaluate the first and third party coverages available and develop best practices for prevention, management, and defense of cyber related claims.

1. Assessing Cyber Vulnerabilities
   1. Types of Risks
      1. Data Breach

As a generic catch-all, a data breach could result from or be paired with any of the below risks. It could be the result of wrongful disclosure, unauthorized disclosure, or failure of computer security to prevent outside access.

* + 1. Phishing / Spear Phishing

Targeted attack to gain user credentials or other access to internal network or specific machines. For example, an email to an employee saying that a password needs to be reset and providing link to enter current credentials to validate before they are reset.

* + 1. Fraudulent Fund Transfers

Fraudulent emails instructing changes in payment details in efforts to misdirect outgoing wire transfers or other payments.

* + 1. Email Compromise

Third party access to/control over a user's email system. Often using rules for Office 365 to cover the attacker's tracks or to reroute emails which would reveal the ruse. This can frequently be coupled with fraudulent fund transfers.

* + 1. Ransomware

Encryption of system data and demand for ransom payment in Bitcoin or other cryptocurrency to restore access. Frequently based on a short timeline demand for payment.

* + 1. Employee Misconduct

Current employee use of organization resources for misconduct or former/departing employees abusing network by using un-withdrawn credentials.

* + 1. DDOS Attacks

Distributed denial of service attacks where an entity's network is overloaded by outside requests, thereby preventing other users from accessing network or internal use of the network based on insufficient resources.

* + 1. Lost Devices

Lost laptops, cell phones, or other electronic devices which contain confidential information or tokens for access to organization network.

1. Liability Issues With Respect To Public Entities And Cyber Risks
   1. 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.[[1]](#footnote-2)

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.[[2]](#footnote-3)

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.[[3]](#footnote-4)

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.*

* 1. 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 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).

1. Coverage Pitfalls
   1. Development of Cyber Coverages

Cyber coverage evolved from the financial lines side of the insurance market, generally under E&O policies, until it developed into its own specialized coverage.

Simultaneously, insurers on the casualty side of the insurance market, including insurers issuing GL policies, have tried to eliminate cyber coverages from their forms. There are still remnant "silent cyber" coverages, which insurers are trying to eliminate as they arise.

For example, in 2001, ISO introduced policy language in the “property damage” definition indicating that “electronic data is not tangible property”. (ISO Form No. CG 00011001). Also, in 2014, ISO introduced endorsements excluding 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” with a limited exception for bodily injury. (ISO Form No. CG 00011204).

* 1. Coverage Issues Relating To Cyber Liability Risks Under Standardized, Non-Cyber Liability Forms
     1. 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.[[4]](#footnote-5) 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”:

* *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).
  + 1. 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.”[[5]](#footnote-6) 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.

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 [] privatecommunications 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”).[[6]](#footnote-7)

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.[[7]](#footnote-8)

* 1. Common Current Cyber Coverages
     1. Privacy Notification Obligations

With Alabama's passage of a Data Breach Notification Act of 2018, all 50 states now have laws requiring notification to individuals whose personal information is exposed as the result of a data breach. Compliance with each state law is the function of the state where the *affected* individual resides. Thus, an organization thought to wholly operate within the confines of a single state may be subject to notification requirements of other states. As examples, notification may be required based on:

* **Risk of harm analysis (e.g., Massachusetts)**: Notification required where breach creates a substantial risk of identity theft of fraud against a resident or when the data owner knows or has reason to know that an unauthorized person acquired the resident's personal information for an unauthorized purpose
* **Trigger by access (e.g., California)**: Notification for any breach of the security of the system containing PII following discovery or notification of the breach

Notification may also be required based on Federal Law. For example, HIPAA for Protected Health Information.

* + 1. Regulatory Expenses

Office of Civil Rights and State Attorneys General investigations. Generally unpredictable penalties and settlements with regulators based on the specific details of any harm which occurs.

Often investigations may be temporarily abandoned or dormant, but then reactivate based on later breach, combining multiple data breaches into a single penalty.

Often difficult to coordinate investigations between different regulatory bodies.

* + 1. Payment Card Industry Fines

Defense of investigations and appeals of fines by Payment Card Companies in connection with the failure to comply with PCI Data Security Standards.

* + 1. Ransomware Payments

Payments to resolve extortion payments made to prevent or resolve a threat to network or data. This coverage frequently requires prior consent by an insurer.

* + 1. Data Restoration Costs

Costs to restore or replace data to the contents in place prior to the incident. This frequently raises coverage issues for the difference between replacing content and improvement of newly developed content. Also necessary to evaluate is whether remediation or future loss prevention may be covered under insurance.

* + 1. Wire Transfer/Payment Fraud

Indemnification for outgoing wire transfers based on fraudulent instructions or spoofed emails that mimic client information and misdirect payments. Coverages often require out of band confirmation prior to payment.

* 1. Common Coverage Issues
* Retroactive Date/Claims Made and Reported Timing Issues
* Notice to Insurer
* Pre-Tender Costs
* Insurer Consent for Incurred Costs
* Reasonableness of Costs Incurred
* Incident Response v. Reputation Protection or Remediation
* Accurate Scope of Loss
* Other Insurance

1. Balanced Responses
   1. Pre-Claim Issues

Generally speaking, the best defense for entities with respect to cyber risks is to follow “best practices” such as:

* + 1. Knowing Your Data

Identify 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.

* + 1. 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 organization’s computers and any network access points; and (4) data backup protocols, including testing backups to make sure they can be utilized in the event of a system failure.

* + 1. Protecting Yourself

Employees are often the largest source of security vulnerability for any organization. As a result, organizations should provide employees access only to those systems and information which are needed to do their jobs. Also, organizations should educate their employees and implement guidelines for technology security. These security protocols can include password standards and guidelines on acceptable internet use. Also, organizations 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.

* + 1. Updating Systems

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.

* + 1. Making 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.

If there is an incident, who is tasked with guiding the response? Are there preferred vendors that can be retained and put in place quickly? What is the typical/expected response time for everyone involved in the response?

* 1. Properly Addressing/Handling Claims As They Happen
     1. Typical Breach Timeline
        1. Discovery

First recognition of an incident and notification within organization. Best practice is to immediately notify insurers and begin internal determination of investigation steps or available resources for investigation.

* + - 1. Investigation

If a data breach is likely, privacy counsel should be retained early. Experienced privacy counsel can help manage the investigation and will retain the necessary forensic investigators, thereby maintaining privilege for forensic investigation. Additionally privacy counsel should be vetted for experience with regulatory compliance in the event government regulators are involved down the road.

Statements of work from any relevant vendors should be requested ASAP for review and to raise any potential coverage issues early.

* + - 1. Coverage Analysis

Coverage should be evaluated under both cyber and non-cyber coverages as appropriate as soon as facts are available from investigation. Also, tender to the appropriate carriers should be made as early as practical pursuant to the notice provisions of the relevant policies.

Coverage should address any potential retroactive coverage issues. What if malware was in place before any policies took effect?

To what extent is notification covered? Notified individuals? Other organizational clients? If notification is not necessary for all impacted entities will notification services be provided anyway? At whose expense?

* + - 1. Notification Obligations

Get call center, credit monitoring, and any public relations/crisis management vendors in place for fast response. Any issues with the number of notified individuals should be planned for to ensure efficient responses once notification begins.

* + - 1. Cost Resolution

Review invoices from vendors, track amounts based on initial estimates and resolve any retention/excess of limits issues with insurance.

* 1. Post Claim Evaluation

Revisit risk assessments and determine improvements. Were pre-claim plans were executed as drawn up? Where improvements possible? What happens the next time there's an issue?

1. Questions?

000003-000005 5675685.1

1. California Civil Code §1798.82 states:

   (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, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

   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 February 3, 2019). In addition, a multitude of federal laws and regulations govern the security of all types of sensitive information. [↑](#footnote-ref-2)
2. Civil Code § 1798.82(h)-(i). [↑](#footnote-ref-3)
3. Civil Code §1798.84(b)-(e). [↑](#footnote-ref-4)
4. *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.”). [↑](#footnote-ref-5)
5. ISO Form No. CG 00010413 [2012]. [↑](#footnote-ref-6)
6. 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). [↑](#footnote-ref-7)
7. 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”). [↑](#footnote-ref-8)