2018 Cyber & Tech Liability – Risk Transfer Update – Part 2

For:

PARMA
February 15, 2018

By:

Robert J. Marshburn, CRM, CIC, ARM, CRIS, CISC, CCIP

R. J. Marshburn & Associates
Laguna Beach, California
Bob@CertifiedRiskManagers.com

2018 Cyber & Tech Liability Risk Transfer Update

An Examination of Cyber & Tech Liability Risks facing Public Agencies and the Elements of Indemnity & Insurance for Transferring and Reducing those Risks through Contracts

To obtain maximum liability protection for PARMA Public Agencies, we will discuss:

1. Some of the Exposures involved in Cyber related Risks
2. The Difference between Cyber Risk and Tech Liability
3. Why the CGL liability policy does not cover Cyber & Tech liability
4. How the absence of a "Standard" coverage form makes matters more difficult
5. Solutions: How to Transfer Risk using effective Contract Insurance requirements
6. Sample Contract language Insurance requirements
7. Coverage Verification for your Contract Cyber & Tech Liability Requirements

Updated Contract language is necessary due to (1) changes in the exposures to Cyber Risk and (2) new and differing insurance coverage forms.

An Overview of Cyber Risk

1. Explosion of computer technology, the Internet, and cloud based solutions.
2. Many risks of loss and potential liability arising from such use and from services provided to the Public Agency from third parties.
3. Services include: portals that allow access to obtain, use or store data; colocation (shared hosting centers); managed dedicated servers; cloud hosting services; software or hardware; programming and other IT services and products.
4. Risks include loss of stored data, theft of data, disruption of network capabilities, and disclosure of private information.
5. Serious attention needs to be paid to the indemnity wording along with the insurance requirements.
6. Techniques and insurance products are emerging to respond to these risks.

Cyber Risk versus Tech Liability (aka IT Liability)

These risks and the related management techniques can be broken down into 3 primary areas. The first two are considered to be **Cyber Risk**:

1. First party risks, related to damages directly to the Public Agency's systems or data
2. Third party risks related to liability to others for breaches of security that may lead to loss of privacy or potential for identity theft.

Cyber Risk is often called Cyber Liability due to #2 above. However, #1 is a property, not liability, risk – it is an intangible property risk with potential for loss. However, the liability risk, #2 above, is liability to others. Both are included under Cyber Risk.

Public Agencies must consult with their Legal, Risk Management, and Insurance advisors to determine the extent of their own program and coverage for these risks.

On the liability side, one of the largest exposures that an entity faces is the requirement to notify and provide credit monitoring services to any party that may have had their personal, private information stolen or otherwise misused. These costs can be substantial.

3. The 3rd primary area of risk to the Public Agency is the **Tech Liability** for any of the above from a Vendor/Consultant hired by the Public Agency

The Vendor/Consultant may be responsible for theft or breaches of security but the Public Agency will no doubt be sued for such.

None of the normal policies required in other types of contracts to transfer risk to the Vendor/Consultant will respond for these types of situations, including the costs of data breach response and regulatory fines and penalties. Customized policies are required to cover these exposures.

This transfer of risk back to the Vendor/Consultant is what we will discuss in this workshop.

Transfer of Cyber Related Risks Using Contracts

1. **When you Contract with a Vendor/Consultant, you become liable for their work**

    a. Public Agencies have their own Cyber Risk liability plus responsibility and liability for the actions of others they hire (Vendors, Consultants and Subs)

2. **Party best able to control the risk should be responsible—the Consultant/Vendor**

    a. Proper use of Contract Agreements can transfer financial risk from the Public Agency to the responsible party—the Vendor or his Subs doing the work and causing the risk

3. **Two principal ways to transfer Tech liability Risk & protect Public Agencies**

    1. **Indemnity**—Vendor/Consultant agrees to assume the liability of the Public Agency. This may be insured by Contractual liability coverage (the definition of "insured contract") in Vendor's Professional Liability Insurance policy, but often is not.

    2. **Insurance**—Covering the Professional Liability of the Vendor. Rarely will the Public Agency be named as an Additional Insured on the Consultant's policy.

4. **Type of liability to be covered by Tech Liability Insurance**

    a. General liability policies exclude professional exposures such as design, engineering, or consulting errors and omissions

b. Loss or destruction of data is NOT tangible property damage and is not covered under CGL Property Damage liability

c. Professional Liability—Different from General (tort) Liability in that it includes Financial Harm even if no Bodily Injury or Property Damage happens; it covers financial loss from an error or omission.

d. From here on we will deal with Professional Liability for Tech Liability**...**

5. Elements of Contract Indemnification & Insurance Requirements—

a. Hold Harmless, Defend, Indemnify, & Waive subrogation rights.

   i. Effect of waiver of subrogation—no right of recovery

b. The Indemnity obligation must cover you both during the Contract **and** after the Contract is completed for liabilities that can occur later. Example: Private information is accessed because of the Vendor's failure to protect it.

   i. Contract should include requirement it is the Consultant's responsibility that defense and indemnity obligations shall survive the termination of the agreement

c. Contract should make clear that the defense and indemnification obligations are in addition to, and are not limited by, the insurance obligations in the agreement.

d. Include a confidentiality agreement with language that vendor/consultant acknowledges:
    i. Will receive or have access to private information; that it is not owned by the vendor/consultant; that they will not sell or otherwise misuse that private information and will have safeguards in place to protect that information
e. Make provision that all data will be available to the Public Agency at time of termination. Add a special termination clause that allows the entity to recover its data for a special fee, without regard to any other dispute that may be pending with the vendor.
f. Require that the vendor notify the entity of a breach even if no data was lost.
g. Require that data be backed up in a secure fashion and that entity have access to backups.
h. Require minimum response and recovery time.
i. Require an independent audit of operations.
j. Require your standard insurance requirements in addition to the Tech Liability specific Insurance requirements.
k. For vendors providing hardware, pre-packaged software or portal access, add a requirement for IT or Professional Tech Liability or Cyber Liability insurance that includes:
    i. Security and privacy liability, including privacy breach response costs, regulatory fines and penalties
    ii. Media liability, including infringement of copyright, trademark and trade dress
    iii. Cyber extortion
    iv. Privacy
l. Work closely with your legal, technical, and insurance advisors in drafting hold harmless language and insurance requirements to ensure the broadest possible indemnity, not limited to bodily injury or property damage but also specifically include wording that encompasses cyber-related risks that include theft, loss or misuse of data, release of private information and responsibility for costs, fines and penalties that the entity might incur.
m. Questions should be asked about the Consultant's data security procedures, including whether or not they have been audited to SSAE 16 standards regarding their controls over information technology and related processes.

6. INSURANCE COVERAGE FOR INDEMNITY OBLIGATIONS

a. Standard Insurance Services Office (ISO) Commercial General Liability (CGL) Policies contain coverage **for the Commercial Consultants** for liability assumed (Indemnification of Public Agency by Consultant) in an "Insured contract."

b. Professional Liability policies for Tech Liability services rarely have this coverage. This means that the coverage for these issues will primarily be found in the Professional Liability Insurance coverage itself for any breach of the Contract indemnity obligations.

7. Pass through provision – require that any Subs hired by the Consultant require the same coverage for the Public Agency

8. Completed Operations exposure (liability after work completed):

a. Require Vendor/Consultant to maintain insurance for a minimum of 3-5 years (or more) following completion of the project.

9. Amount of risk not necessarily consistent with size of job

a. The Scope of Work determines the coverage & limits required! Discuss early on with Risk Management, not at the end when there is pressure to get the work done!

   i. If Purchase orders are used for small jobs require a summary "Indemnity & Insurance Requirements" on the Purchase Order (or Proposal, Memorandum of Understanding, Letter of Intent, etc. – whatever you use) and have them sign and date it with a statement that

they have read, understand, and agree to comply with the Indemnity and Insurance requirements supplied with the Purchase Order. This may "trigger" the "written Contract or Agreement" requirement for coverage in many policies.

ii. **For RFPs:** It is strongly recommended when distributing an RFP (proposal) or RFQ (qualification) to include a document containing a Summary of your "Indemnity and Insurance Requirements" that includes language to provide a copy of the requirements to their insurance broker or insurer to confirm compliance. **Sample in Reference Section.**

iii. At the bottom of the form have them sign, date, and return with language that they have read, understand, and agree to comply with the Indemnity and Insurance requirements supplied with their proposal.

iv. This Provides quick & early problem screening & possible policy trigger if no Contract!

10. Many Insurance policies DO NOT provide coverage unless specifically required by a Written Contract or Agreement!

a. Contracts should require that (1) the full coverage and (2) the full limits available to the named insured shall also be available and applicable to the Public Agency**. T**he required coverage and limits shall be (1) the minimum coverage and limits specified in your Agreement; or (2) the broader coverage and maximum limits of the coverage available to the named Insured; whichever is greater.

The best way to cover Cyber Risk and Tech Liability Contract obligations is with quality Vendor/Consultant Insurance coverage

1. There is **no such thing as a "Standard" Policy** coverage form for Tech Liability!
2. Each policy must be evaluated based upon its coverage for the scope of work
3. Examine the "scope of coverage" in the Tech Liability policy, usually contained in the initial "insuring agreement."
4. Examine the exclusions contained in the policy
5. It is common for consultants and companies working in technology to not have appropriate insurance since many of their clients do not ask for evidence that this insurance is carried.
6. Insurance is the primary source of risk transfer not only for the Public Agency, but also for the vendor/consultant's own protection.
7. If the Consultant will not or cannot provide the necessary coverage, it may be possible for the entity to purchase a policy that can respond for the entity (not the Consultant) and provide sufficient risk transfer for the entity.
8. Your entity may also want to review their own Cyber Liability coverage and verify that they would be protected for claims and suits arising out of the acts of the Consultant and will defray data breach fines, penalties and credit monitoring expenses. Discuss this with your insurance broker or risk management consultant.
9. **It is unlikely that the entity will be added as an additional insured to either an IT Professional Liability or Cyber Liability policy.**
10. It is critical not only that the insurance coverage be obtained by the consultant/vendor, but that substantial limits are provided.
11. Work closely with your insurance broker or risk management consultant to verify that your Entity is requesting the correct coverage for each situation, and that you are receiving the coverage requested.
12. It is a good practice to require that the Policy itself be provided to you, rather than just receiving information on a Certificate of Liability insurance.
13. Finally, these policies are almost always written as Claims Made and Reported policies and should contain an automatic extended reporting period of 90 days or

more beyond the expiration date of the policy. You can also require in your Contract that the Professional Liability be renewed for a certain period of time, usually 3 to 5 years, after project completion.

14. **CAUTION**: Most Tech liability policies exclude coverage for damage to or loss of data, i.e., intangible property. (It is now generally well accepted that the CGL policy coverage for PD liability applies only to tangible property, so there is no coverage there.)

    a. We would seem to be able to expect that a Tech liability policy would, by the nature of what is covered, apply to intangible property. However, as noted above, most do not. This exclusion in a Tech liability policy for intangible property is roughly the equivalent of the same Type of exclusion in the CGL policy for tangible property under the care, custody, or control exclusion.

    b. However, this coverage for intangible property can be found under most Cyber policies (not Tech liability policies), since they are considered to be a Type of property policy that covers intangible property. As such, the Cyber policy covering the vendor can be endorsed to cover the intangible property of others, i.e., the Public Agency, as part of the Vendor's coverage.

    c. For this reason, we refer to both Cyber and Tech liability in the Insurance requirements. It is possible that a Tech liability policy can be endorsed to cover the intangible property of the Public **Agency, but this is rare.**

15. **BEWARE: Be careful of the wording in any Service Provider Agreements**. Most Tech agreements will have a "General Indemnity or Hold Harmless Clause" that will state that indemnification for losses by the technology professional, service provider, or vendor is limited to bodily injury and property damage to tangible personal property and that data is not considered to be tangible personal property. In other words, if the technology professional, service provider or vendor were to accidentally erase a client's data, there would be no liability for their error, if such an indemnity agreement were in place. This type of hold harmless clause is not acceptable to the Public Agency hiring the technology professional, service provider, or vendor and is should be removed before allowing the vendor to start work. However, we have seen some Public Agencies not reviewing their contacts and they have unknowingly accepted this clause without negotiation.

16. CAUTION: As noted above, many Tech Liability policies consider client data to be property in the "care, custody, or control" of the Consultant and exclude it!
17. See the following Sample Contract language to see how this can be handled...

****

In addition to the Standard coverages you require of any Vendor for General liability, Auto, and Workers' Compensation coverage - you will want to add Professional Liability such as the following:

Sample Contract language for Tech Liability Insurance requirements:

1. **Technology Professional Liability Errors and Omissions Insurance** appropriate to the Vendor's profession and work hereunder, with limits not less than $2,000,000 per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Vendor in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, copyright, trademark, invasion of privacy violations, information theft, release of private information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

    a. The Policy shall include, or be endorsed to include, ***property damage liability coverage*** for damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the Agency in the care, custody, or control of the Vendor. If not covered under the Vendor's liability policy, such "property" coverage of the Agency may be endorsed onto the Vendor's Cyber Liability Policy as covered property as follows:

    b. **Cyber Liability coverage** in an amount sufficient to cover the full replacement value of damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the Agency that will be in the care, custody, or control of Vendor.

    c. The Insurance obligations under this agreement shall be the greater of 1—all the Insurance coverage and limits carried by or available to the Vendor; or 2—the minimum Insurance requirements shown in this agreement. Any insurance proceeds in excess of the specified limits and coverage required, which are applicable to a given loss, shall be available to Agency. No representation is made that the minimum Insurance requirements of this agreement are sufficient to cover the indemnity or other obligations of the Vendor under this agreement.

VERIFICATION of Coverage Compliance© is THE MOST IMPORTANT PART OF THE ENTIRE PROCESS! Make it **standard practice** (authorized & required by your Contract) that you require a Copy of the Professional Liability Policy—

****At a minimum require a copy of the Declarations & Policy Endorsements page for the Professional Liability policy.**

(This is **necessary** to help **identify** "Restricted Coverage" policies and endorsements and verify if limitations or exclusions have been added to the policy – the policy endorsements will be listed here.)

****

IF YOU DO NOT KNOW WHAT A TECH PROFESSIONAL LIABILITY POLICY PROVIDES—GET HELP!

- **Early communication with Risk Management by the Public Agency is most important to help avoid risks and have more time to help negotiate contracts.**

THE BEST CONTRACT FOR INDEMNITY AND INSURANCE REQUIREMENTS IS USELESS UNLESS VERIFIED FOR COVERAGE COMPLIANCE!

APPLICATION OF KNOWLEDGE LEARNED

1) Match the scope of work to the coverage provided in the Professional Liability policy
2) Discuss using the recommended Insurance Contract language with your advisors
3) Use a "Summary of Indemnity and Insurance requirements" with signature for RFPs, RFQs, Purchase Orders, MOUs, LOIs, etc to prevent problems, solve earlier, trigger coverage, and make the process simpler & quicker! Sample in Reference Section.
4) Focus on high risk operations for higher limits.
5) Verification of requirements – Since all are different, Require the Policy for Review and Evaluate Yellow (Need more info—could be a problem) and red flags (Prohibited exclusions or language). It saves time, expedites any delays and questions to an earlier, manageable time process.
6) Pay special attention to the Policy and Schedule of endorsements for—
   a) How your Data is treated – Is it excluded as property in the care, custody, or control of the Consultant
   b) Policy exclusions, limitations, and reductions in coverage
7) Involve Risk Management early in the process for Contract, Indemnity, and Insurance questions
8) NEVER use a Vendor's Contract, Service Agreement, or other signed documents that may limit your protection and coverage!

BIOGRAPHICAL PROFILE—Robert J. Marshburn, CRM, CIC, ARM, CRIS, CISC, CCIP

In independent industry evaluations, Mr. Marshburn is consistently rated as one of the nation's top Risk Management Consultants and Educators. He is the founder and principal of R. J. Marshburn & Associates, CertifiedRiskManagers.com, an independent risk management consulting and educational firm. He has been in risk management 40 years.

Mr. Marshburn holds the professional designations of Certified Risk Manager (CRM), Associate in Risk Management (ARM), Certified Insurance Counselor (CIC), Construction Risk & Insurance Specialist (CRIS), Certified Insurance Specialist in Construction (CISC), and Certified Construction Insurance Program (CCIP).

Mr. Marshburn works as an outsourced risk manager, as an independent consultant to clients, and in association with other professionals with their clients. He is an appealing, frequent speaker before various groups on risk management and insurance topics.

Mr. Marshburn was an original designated Public Agency of the National Faculty of the Certified Risk Managers teaching courses for qualification for the CRM professional designation and served as a consultant developing the CRM program on the Curricula Advisory Committee. He authored Graduate courses and teaches workshops in Indemnification & Additional Insureds, Contractual Liability & Insurance Coverage, Construction Defect issues, Wrap-Up Policies, and Ethics.

He is the co-creator and author of the Certified Insurance Specialist in Construction (CISC) professional designation that was later merged into the Construction Risk & Insurance Specialist (CRIS) program from the International Risk Management Institute which he also teaches. In addition, he serves as the Senior Educational Consultant and Instructor to the Insurance Community University and is a co-creator of the University's Certified Construction Insurance Program (CCIP).

Mr. Marshburn is a nationally recognized expert in the field of Contractual risk transfer, including indemnity and insurance requirements for risk management. He currently serves as the contributing editor of the California Public Agency Insurance Contract Manual.

He is the founder and creator of the *Coverage Compliance Verification*© Program and specializes in the challenges posed in Construction Risk, including Construction Contracts, Contractual Liability Analysis & Design, Insurance Policy Coverages and Endorsements, Wrap Policies (OCIPs, CCIPs, etc), Construction Defect Liability, and Coverage Disputes.

Mr. Marshburn has been retained as a consultant, educator, and expert witness for some of the nation's premier builders, Consultants, risk managers, Public Agencies, carriers, developers, brokers, consultants, attorneys, industry & trade associations, and educational organizations.

Reference Section

Large Self Insured Retentions (SIRs) on the Vendor/Consultant's policy

1. The Consultant **must** pay the SIR first, or there is no coverage for defense or damages for the Public Agency as well!

    a. **Be very careful** of granting such high limit SIRs which must be paid by the named Insured Consultant.

    b. With respect to a Consultant that has a very high SIR – Do your due diligence. Require financials, collateral, Letter of Credit, security, etc sufficient to pay the SIR. Require a Contract provision that the Consultant pay the SIR

    c. Have the Insurance Company amend the policy to provide that the Public Agency, not just the named Insured, can satisfy the SIR (in order to trigger coverage).

    d. Include Contract requirements that—

        i. Self-insured retentions (SIR) must be disclosed to Risk Management for approval and shall not reduce the limits of liability.

        ii. Policies containing any self-insured retention (SIR) provision provide, or be endorsed to provide, that the SIR may be satisfied by either the named Insured or the Public Agency.

        iii. Public Agency reserves the right to obtain a copy of the Insurance policy and endorsements.

NOTE RE: Wrap Up Policies (OCIPs, CCIPS, etc)

Wrap Up policies (OCIPs, CCIPS, etc) – can be very good; or very, very bad

Coverage Considerations for a **Wrap** Policy **are completely different!**

All the normal rules above will not apply!

Please get help if you are involved in a Wrap-up project!

Much of my expert witness time the last several years has been where Wrap policies were involved!

Sample Notice to Bidders regarding Indemnity and Insurance Requirements (may also be use with Purchase Orders)

SUMMARY OF INDEMNITY AND INSURANCE REQUIREMENTS

1. These are the Indemnity and Insurance Requirements for Consultants providing services or supplies to Public Agency (Entity). By agreeing to perform the work or submitting a proposal, you verify that you comply with and agree to be bound by these requirements. If any additional Contract documents are executed, the actual Indemnity language and Insurance Requirements may include additional provisions as deemed appropriate by Entity.

2. You should check with your Insurance advisors to verify compliance and determine if additional coverage or limits may be needed to adequately insure your obligations under this agreement. These are the minimum required and do not in any way represent or imply that such coverage is sufficient to adequately cover the Consultant's liability under this agreement. The full coverage and limits afforded under Consultant's policies of Insurance shall be available to Entity and these Insurance Requirements shall not in any way act to reduce coverage that is broader or includes higher limits than those required. The Insurance obligations under this agreement shall be: 1—all the Insurance coverage and limits carried by or available to the Consultant; or 2—the minimum Insurance requirements shown in this agreement, whichever is greater. Any insurance proceeds in excess of the specified minimum limits and coverage required, which are applicable to a given loss, shall be available to Entity.

3. Consultant shall furnish the Entity with original Certificates of Insurance including all required amendatory endorsements (or copies of the applicable policy language effecting coverage required by this clause) and a copy of the Declarations and Endorsement Page of the CGL policy listing all policy endorsements to Entity before work begins. Entity reserves the right to require full-certified copies of all Insurance coverage and endorsements.

I. INDEMNIFICATION:

COPY YOUR INDEMNITY REQUIREMENTS HERE.

II. INSURANCE

COPY YOUR INSURANCE REQUIREMENTS HERE.

I have read and understand the above requirements and agree to be bound by them for any work performed for the Entity.

Authorized Signature: _____ Date: _____