Risky Business with Cyber Insurance – Sunglasses Not Optional

American Bar Association Section of Litigation
Insurance Coverage Litigation Committee
March 1-4, 2017

Lori L. Siwik
Founder and Managing Partner
SandRun Risk
STRATEGIC | COLLABORATIVE | INNOVATIVE

Jason Warmbir
Vice President
FINEX Cyber Liability Practice
Willis Towers Watson

Dorothea W. Regal
Partner
Hoguet Newman Regal & Kenney, LLP

Ray Wong
Partner
DuaneMorris®

Kathryn Kasper
Director
HDJN

Introduction

Data breaches have resulted in hundreds of millions of data records being illegally accessed. Home Depot, Target, Michael's, TJ Maxx, Snapchat, Facebook, Twitter, Sony, Kmart, Apple's iCloud, First Commonwealth Bank, and P.F. Chang's are just a few of the companies that have reported a major data breach. The Russian hacking of the Democratic National Committee during the 2016 Presidential campaign may have impacted the election. Similarly, DDos (Denial of Service) attacks have targeted banks and other financial service providers.

According to the Verizon 2016 Data Breach Investigation Report, 89% of breaches had a financial or espionage motive. The attackers hacked, distributed malware, phished and instituted social engineering schemes to get access to the data. Employee negligence also played a role in data breaches with lost and stolen devices, as well as through the use of portable devices such as cell phones, laptops, iPads, flash drives, and other devices – all of which pose a security risk to companies and their computer networks.

Every company, large or small, is susceptible to a data breach. With more and more companies using technology to manage their daily business activities, it is becoming easier for criminals and non-criminals to get access to sensitive information like social security numbers, bank account information, credit card numbers and intellectual property information. Data breaches can cost a company millions of dollars in defense and settlement costs arising from the breach, in business interruption expenses, and in damages to remedy the breach itself. Losses arising from data breaches average $158 per lost record with an average total cost of $4 million per company.[1]

What are the Data Breach Laws?[2]

Data breach notification laws have been enacted in every state, but the requirements vary from state to state. These data breach notification laws are triggered when there has been a breach of personal information, which is not uniformly defined in the statutes. What to include in the notification can have negative consequences to the company reporting the breach. For instance, in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), Neiman Marcus followed state law and reported that 9200 credit cards had experienced fraud and that customer credit reports should be reviewed. The Seventh Circuit relied on the notice statements when ruling that the plaintiffs had met the requirements for a class action. Similarly, in *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), P.F. Chang's publicly announced its data breach before it knew the complete scope of the breach without indicating that not all its locations were affected and may have implied that all were by its action of temporarily installing a manual card-processing system at all its locations. After announcing the breach, it learned that only 33 restaurants had been affected by the breach. In the Seventh Circuit appeal, P.F. Chang's argued that the named plaintiffs in the class action suit had no standing to bring the class action because they were not customers at any of the 33 affected restaurants. The Seventh Circuit rejected this argument, relying on the early notice that P.F. Chang's had provided to all of its customers.

The FTC, under Section 5 of the Federal Trade Commission Act, has authority to protect consumers from unfair or deceptive data security practices and does so by instituting

[1] Ponemon Inst. 2016 *Cost of a Data Breach Study*: available at *http://www-03.ibm.com/security/data-breach*
[2] Recently, Mayer Brown published a guide, "*Cybersecurity Regulation in the United States: Governing Framewords and Emerging Trends."* The guide is an excellent resource.

enforcement actions.[3] The FTC holds a breached entity accountable for meeting a data security level that is "reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[4]

The Securities and Exchange Commission's Division of Corporate Finance guidance on cybersecurity disclosures provides, per the federal securities laws, that companies "should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents" and that "appropriate disclosures may include," a "[d]escription of relevant insurance coverage. *See* www.sec.gov/divisions/corpfina/guidance.

Is There Insurance Available for Data Breaches?

Companies may receive lawsuits seeking damages as a result of a data breach. Claims of invasion of privacy, lost or stolen data, loss of use of computers, misappropriation of confidential business information, etc. can cost companies thousands of dollars to defend. Governmental and regulatory actions related to data breaches are also common.

When faced with a data breach or an electronic data loss, many companies may look to their commercial general liability ("CGL") policies and first-party property policies for coverage. A dispute often arises between the insurance carrier and the policyholder regarding the availability of coverage.[5]

Sometimes the battle is over whether there is a privacy violation or a publication such that there would be coverage under CGL policies.[6] *See Zurich Am. Ins. Co., v. Sony Corp. of Am., 2014 N.Y. Misc. LEXIS 5141 (2014); Hartford Cas. Ins. Co. v. Corcino & Assocs., 2013 U.S. LEXIS 152836 at *12 (C.D. Cal. Oct. 7, 2013)* (the court rejected the insurance carrier's argument that the personal injury coverage excluded claims for disclosure of personal data of hospital patients, and observed that "medical records have been considered private and confidential for well over 100 years at common law"); *Recall Total Info. Mgmt. v. Fed. Ins. Co., 83 A.3d 664 (Conn. App. 2014), aff'd, 115 A.3d 458 (Conn. 2015); Travelers Indem. Co. of Am.*

---

[3] In *FTC v. Wyndham Worldwide Corp., 10 F. Supp.3d 602 (3rd Cir. 2014),* the Third Circuit Court of Appeals held that the FTC has authority to bring enforcement actions against companies relating to their data security practices.

[4] "*Privacy Law: Protecting the Good, the Bad and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them", Yasmine Agelidis, 31 Berkeley Tech. L. J. 1057 (2016), citing "Data Security, Fed. Trade Comm'n,* https://www.ftc.gov/datasecurity

[5] An excellent article that discusses insurance coverage for cyber attacks is *"Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of the Internet"* by Roberta D. Anderson, 49 Tort & Ins. L.J. 529 (Winter, 2014). *See also "Claims Made and Insurance Coverage Available for Losses Arising Out of or Related to Electronic Data",* by Jeffrey S. Price and Justin D. Wear, 51Tort & Ins. L.J. 51 (Fall, 2015) and "*Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation and Tomorrow's Challenges",* by Gregory D. Podolak, 33 Quinnipiac L.Rev. 369 (2015).

[6] The 2007 and later ISO insurance forms contain an exclusion for privacy-related laws.

v. Portal Healthcare Solutions, LLC, 35 F. Supp.3d 765 (E.D. Va. 2014); Pietras v. Sentry Ins. Co., 2007 U.S. Dist. LEXIS 16015 (N.D. Ill. Mar. 6, 2007); Valley Forge Ins.Co. v. Swiderski Elecs., Inc., 860 N.E.2d 307 (Ill. 2006); Zurich Am. Ins. Co. v. Fieldstone Mortgage Co., 2007 U.S. Dist. LEXIS 81570 (D. Md. Oct. 26, 2007); Park Univ. Enters., Inc. v. Am. Cas. Co., 442 F.3d 1239 (10th Cir. 2006); Columbia Cas. Co v. HIAR Holding, LLC, 411 S.W.3d 258 (Mo. 2013).

Often the battle is over whether there has been "property damage". In many insurance policies "Property Damage" is defined as "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."[7] Insurance carriers argue that electronic data is excluded from the definition of tangible property. *See Arch Ins. Co. v. Michaels Stores, Inc., No 12-00786 (N.D. Ill. Feb. 3, 2012).* Many courts find that data does not amount to "tangible property" because computer information lacks physical substance. *See Ward Gen. Servs. Inc. v. Employers Fire Ins. Co., 114 Cal. App. 4th 548, 556-57 (Cal. App. 4 Dist. 2003)* (where a computer crash, due at least in large part to human operator error, resulted in data loss, the court held that there was no physical loss or damage. The court held that data loss was simply a "loss of organized information . . . (such as client names and addresses). . . ." concluding that such information "cannot be said to have a material existence, be formed of tangible matter, or be perceptible to the sense of touch"). *See also America Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89,93-98 (4th Cir. 2003)* (the court concluded that "physical magnetic material on the hard drive is tangible", but concluded that software and data was not tangible); *Liberty Corp. Capital Ltd. v. Security Safe Outlet, Inc., 937 F. Supp.2d 891 (E.D. Ky. Mar. 27, 2013); Cincinnati Ins. Co. v. Prof'l Data Servs., Inc. 2003 U.S. Dist. LEXIS 15859 (D. Kan. July 18, 2003); AFLAC, Inc. v. Chubb & Sons, Inc.*, 581 S.E.2d 317, 319 (Ga. Ct. App. 2003). *But see Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185, 2000 U.S. Dist. LEXIS 7299, at 6 (D. Ariz. April 18, 2000)* (holding that there was physical damage when information stored on random access memory was destroyed); *Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. Minn. 2010)* (Insurer had duty to defend lawsuit alleging that a virus caused computer to be unusable, even though the insurance policy excluded "software, data, or other information that is in electronic form" from the definition of "tangible property"); *NMS Servs., Inc. v. The Hartford*, 62 Fed. Appx. 511, 514 (4th Cir. 2003) (*concurring opinion of Judge Widener); Centennial Ins. Co. v. Applied Health Care Sys., Inc., 710 F.2d 1288 (7th Cir. 1983)* (because it was possible that the losses arose from damage to the customer's tangible property, the duty to defend was triggered); *See Southeast Mental Health Ctr., Inc., v. Pacific Ins. Co., 439 F.Supp.2d 831, 837-39 (W.D. Tenn. 2006); Lambrecht & Assocs., Inc. v. State Farm Lloyds, 119 S.W. 3d 16, 25 (Tex. App. 2003)*; *Retail Sys., Inc. v. CNA*

[7] The current standard ISO form and other ISO forms since December 1, 2001 specifically exclude "electronic data" from the "property damage" definition. Sometimes endorsements add the coverage back to the policy. It is important to review the insurance policy carefully.

Ins. Co., 469 N.W.2d 735 (Minn. Ct. App. 1991); Computer Corner, Inc. v. Fireman's Fund Ins. Co., No. CV97-10380, slip op. at 3-4 (2d Dist. Ct. N.M. May 24, 2000), rev'd in part on other grounds, *46 P.3d 1264 (N.M. Ct. App. 2002).*

In first-party property policies, there must be "physical loss or damage" to the covered property for coverage to be triggered. Many first-party property policies contain a broad definition of "Covered Property" that includes all "personal property owned by" the insured. However, software and data may not constitute "personal property" and as such, may not be covered under the policy. Several cases have addressed data losses under first-party property policies. In *Ward General Insurance Services, Inc. v. Employers Fire Insurance Co., 114 Cal. App.4th 548 (2003)*, the insured suffered a computer crash which resulted in a significant loss of electronically stored data. The insurer denied coverage. The court found that the loss did not result in "direct physical loss of or damage to" property and that the data stored on a tangible medium was not tangible. Other courts have found coverage under first-party property policies. *See NMS Servs., Inc. v. The Hartford, 62 Fed. App'x 511 (4th Cir. 2003)* (the court found property damage to hacked computers per a business interruption endorsement); *Lambrecht & Assocs., Inc. v. State Farm Lloyds, 119 S.W.3d 16 (Tex. 2003)* (the court found property damage to hacked computers per a business income endorsement); *American Guar. & Liab. Co. v. Ingram Micro, Inc., No. 99-185, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. April 18, 2000)*(the court found coverage and held that "physical damage" is not restricted to the physical destruction of the computer, but also includes loss of access, loss of use and loss of functionality).

To address court decisions finding coverage under the CGL policies for data breaches, the insurance industry, through the Insurance Services Office ("ISO"), has taken action to remove cyber coverage from CGL policies. In 2013, ISO introduced an *optional* endorsement that deleted the invasion of privacy related offense (oral or written publication, in any manner, of material that violates a person's right of privacy) from the definition of personal and advertising injury applicable under Coverage B of the ISO coverage form.[8] Thereafter, ISO introduced several other endorsements that further exclude coverage for data breaches. These endorsements have been approved by insurance regulators in 45 states and became effective May 1, 2014. Each of the ISO endorsements broadly excludes data-related losses as well as those arising from the access or disclosure of confidential or personal information of a person or company. The endorsements exclude damages claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred. In addition to the exclusions, several insurance carriers have revised the definition of "property damage" in the CGL policies to state:

[8] July 18, 2014 Insurance Journal – ISO Comments on the CGL Endorsements for Data Breach Liability Exclusions.

> For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

Companies that suffer a data breach incur significant costs including but not limited to, forensic investigation costs, breach notification costs, credit monitoring costs, crisis management costs, lost business, and legal/litigation costs. To protect themselves, companies can purchase a specialty insurance policy referred to as "Cyber" insurance. Cyber insurance policies can provide coverage for first-party (cyber crime) coverage as well as third-party (cyber liability) coverage. They can provide coverage for direct loss and legal liability with resulting consequential loss caused by cyber security breaches. Cyber insurance policies are usually claims made and can be very expensive, although the costs have come down as more carriers have entered the market. Depending on the policy, there is an ability to insure notification costs, credit monitoring and other direct expenses covered if there is a data breach EVEN if there is never a liability claim. Regulatory fines and penalties are endorsable. Some insurance carriers provide crisis management, a call center, and other services to the policyholder when cyber insurance is purchased. It is important that companies review the policy wording carefully to make sure that it meets their business needs. Some policies are better written than others.

A cyber insurance policy should provide coverage for the following first-party costs[9]:

- Legal and forensic services to determine whether a breach occurred and to assist with regulatory compliance if a breach is verified
- Notification of affected customers and employees
- Electronic information restoration
- Customer credit monitoring and identity protection services
- Crisis management and public relations to educate the company's customers about the breach;
- Business interruption expenses, such as additional staff, rented or leased equipment, third-party services, and additional labor arising from a coverage claim;
- Public relations firm fees to restore reputation and mitigate damages

[9] *See "Department: Technology: Risky Business: Why Lawyers Need to Understand Cyber Insurance for Their Clients", Shawn Tuma and Katti Smith, 78 Tex. B.J. 854 (December 2015); and "Department: Law Practice Solutions: Everything You Need to Know about Cyber Liability Insurance But Never Knew to Ask", JoAnn Hathaway, 95 MI B.J. 42 (December 2016).*

- Regulatory fines
- Cyber extortion reimbursement for perils including credible threats to introduce malicious code, pharm and phish customer systems, or corrupt, damage or destroy their computer system.
- Systems failure and administrative error

Similarly, a cyber policy should provide coverage for the following third-party costs[10]:

- Judgments, settlements or civil awards
- Electronic media liability, including infringement of copyright, domain name, trade name, service mark or slogan
- Potential employee privacy liability as well as network security and privacy liability

Even companies that purchase cyber liability policies may end up in a coverage dispute with their insurance carriers. *See Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., No. 2:14-CV-170, 2015 U.S. Dist. LEXIS 62185 (D. Utah 2015)* (complaint had to contain allegations of negligence to trigger duty to defend)*; Doctors Direct Ins., Inc. v. Bochenek; 38 N.E.3d 116 (Ill.Ct.App. 2015)* (no coverage under cyber claims endorsement for TCPA or consumer protection claims); *Columbia Cas. Co. v. Cottage Health Sys., 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. July 17, 2015); and P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. 2016)*.

In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.,*[11] the court held that P.F. Chang's cyber liability policy did not provide coverage for over $1.9 million in fees and assessments that P.F. Chang's was required to pay Bank of America Merchant Services ("BAMS"). BAMS had provided P.F. Chang's with credit card processing services. Under the Master Services Agreement ("contract") between P.F. Chang's and BAMS, P.F. Chang's was required to reimburse BAMS for fees, fines, penalties or assessments BAMS paid to MasterCard. After hackers stole the credit card data of approximately 60,000 of P.F. Chang's customers, BAMS paid over $1.9 million in assessments to MasterCard and sought reimbursement of those costs from P.F. Chang's per the contract. The cyber policy issued by Federal Insurance Company had a narrow definition of "privacy injury" and contained an exclusion for any loss or expense that P.F. Chang's assumed under a contract.

The policy at question in *P.F. Chang's* was marketed by the insurer as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated

[10] *Id.*
[11] *No. CV-15-01322-PHX-SMM, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. 2016)*

with doing business in today's technology-dependent world" covering "direct loss, legal liability, and consequential loss resulting from cyber security breaches."[12] But the policy language was more particular and, ultimately, determined by the district court to be less expansive in the coverage afforded. The insuring agreement in the policy stated that the insurer shall be liable for loss on account of claims made against the insured for covered injury, including a "Privacy Injury," defined as an "injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record ...."[13] Federal's cyber policy also contained an exclusion for any loss or expense that P.F. Chang's assumed under a contract.[14] Federal argued that there was no coverage under the insuring agreement for the $1.9 million in assessments and fees and that in any event coverage was barred under the exclusion for liabilities assumed under contract. As to the insuring agreement, Federal argued that the data breach did not constitute a "Privacy Injury" since the "Records" compromised were not the records of BAMS, the card-processing entity that had presented the $1.9 million assessment claim to P.F. Chang's.[15] P.F. Chang's argued that a "Privacy Injury" existed regardless of who suffered it.[16] The policy language would seem to support the P.F. Chang's position on this point since, even with a close parsing of the definition of "Privacy Injury," the policy does not expressly require a covered "Privacy Injury" to have been sustained by the entity asserting the claim against the insured for such injury, and the definitions of "Person" and "Claim" do not support any such restriction.[17] The court assumed, without discussion, that the injury must be an injury suffered by the entity presenting the claim, and held that there was no coverage for the assessment under the insuring agreement because "BAMS did not sustain a Privacy Injury itself, and therefore cannot maintain a valid Claim for Injury against Chang's."[18] The court further held that coverage for the assessment was barred by the policy exclusion for contractual obligations arising between the insured and a third party, BAMS.[19]

P.F. Chang's relied upon the reasonable expectation doctrine in its further argument that the court should interpret the policy language to find coverage for the card-processing assessments for the data breach, presenting evidence of the insurer's marketing representation that the policy addressed "the full breadth of risks associated with doing business in today's

---

[12] *2016 WL 3055111, at *1.*

[13] *Id. at 4.* The capitalized terms are terms defined in the policy.
[14] *Id. at 7.*
[15] *Id. at 5.*
[16] *Id.*
[17] Def. Fed. Ins. Co's Answer and Affirmative Defenses to Pl's Compl. for Breach of Contract and Declaratory J., Ex. 1 at 2, *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co, No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016).*
[18] *2016 WL 3055111 at 4.*
[19] *Id. at 7.*

technology-dependent world"[20] and that it would cover direct and "consequential loss resulting from cyber security breaches" and deposition testimony of Federal's underwriter showing that, at the time the policy was renewed, Federal knew that all of the credit card transactions done by P.F. Chang's were processed through a servicer like BAMS and knew that P.F. Chang's would have liability for the type of assessment at issue in this case in the event of a data breach regarding credit card transactions.[21] Nonetheless, the court declined to apply the reasonable expectation doctrine, stating that regardless of Federal's understanding, "[n]owhere in the record is the Court able to find supporting evidence that during the underwriting process Chang's expected that coverage would exist for Assessments following a hypothetical data breach."[22] The court considered P.F. Chang's to be a sophisticated insured and commented, "[I]f Chang's, who is a sophisticated party, wanted coverage for this Assessment, it could have bargained for that coverage."[23]

Some cyber policies now explicitly provide coverage for the type of assessment that the Arizona court found not to be covered by the cyber policy at issue in *P.F. Chang's,* referred to as Payment Card Industry (PCI) coverage. This PCI coverage explicitly covers the assessments made by credit card issuers due to a data breach. Policies providing explicit PCI coverage may contain an affirmative insuring agreement covering contractually imposed PCI-DSS fines, penalties and assessments and an exception to the standard contractual liability exclusion.[24] Nevertheless, the decision in *P.F. Chang's* provides important lessons for policyholders possessing or dealing with private or sensitive data vulnerable to security breach. For one, the court in *P.F. Chang's* found that the insured's alleged expectation regarding its policy coverage was a "*non sequitur*" from the marketing statements and other evidence the insured had presented, which conclusion was unsupported by any evidence or proof as to what its *actual expectations* were.[25] Policyholders hoping to recover for cyber breaches under the reasonable expectation doctrine must therefore be able to provide an affirmative showing of such expectations. This could be done through deposition testimony with explicit statements of the insured's representatives on expected coverage[26] or other demonstrations of anticipated risks and

---

[20] *Id. at 1.*
[21] *Id. at 9.*
[22] *Id.*
[23] *Id. at 5.*
[24] Integro Insurance Brokers, Insurance Broking & Consulting White Papers, *Learning A Lesson From P.F. Chang's*, *available at* http://integrogroup.com/news/integro-white-papers/learning-a-lesson-from-p.f.-changs

[25] *P.F. Chang's, 2016 WL 3055111, at *9.*
[26] *State Farm Fire & Cas. Co. v. Rocky Sapp*, *No. 1 CA-CV 13-0623, 2015 WL 632138, at *1-6 (Ariz. Ct. App. Feb. 12, 2015), review denied (July 30, 2015)* (Policyholder, through his testimony, demonstrated that he believed he had the requisite coverage, stating that "he would not have purchased the…policy had he known that coverage would not be extended" accordingly.)

coverage.[27] *P.F. Chang's* also highlights an important issue that may recur in determining coverage claims under cyber policies, which is whether a "privacy injury" covered by a particular policy has to be an injury sustained by the claimant. In *P.F. Chang's*, the Court rejected the insured's argument that "privacy injury" is to be construed broadly to also cover those sustained by the credit card issuer imposing the assessments for breach of its credit card information, as the claimant (BAMS) was merely acting as a pass-through intermediary.[28] Under the insured's reasoning, an intermediary such as BAMS is not the true injured party, and will likely never be. Would the court's interpretation of "privacy injury" in this context then preclude coverage for all claims presented by intermediaries?

How Can Companies Make Sure That Their Cyber Policies Provide Coverage for Data Breaches?

Companies should develop and maintain a risk management program for addressing their cybersecurity risks. Besides knowing the federal, state, and local laws and regulations, companies should thoroughly access their own cybersecurity risks through a risk assessment. The assessment should include:

- Defining the system
- Identifying and classifying critical cyber assets
- Identifying and documenting the electronic security perimeters
- Performing a vulnerability assessment
- Assessing risks to system information and assets
- Selecting security controls
- Monitoring and assessing the effectiveness of controls using pre-defined metrics
- Developing and implementing effective cybersecurity policies
- Determining the level of understanding of employees with respect to cybersecurity and whether training is needed

[27] *See, e.g.*, *Hawkins v. Globe Life Ins. Co*., 105 F. Supp. 3d 430, 442-44 (D.N.J. 2015) (Although insurer argues that its solicitation materials specifically stated coverage was not effective until approved by the company, policyholder reasonably expected coverage in the interim period at issue because insurer received the policyholder's premium check and cashed the check); *Haber v. St. Paul Guardian Ins. Co., 137 F.3d 691, 697–98 (2d Cir. 1998)* ("When an individual notifies an insurer of its desire to obtain full coverage and of the existence of a live-in housekeeper, a court may infer an intention on the part of the individual to cover the employee. This inference, coupled with the complete reading of the Endorsement in question, could certain lead an average person to reasonable expect that he has the coverage sought."); *Meadow Brook, LLP v. First Am. Title Ins. Co., 2014 MT 190, ¶ 17, 375 Mont. 509, 514, 329 P.3d 608, 612* (In addition to email correspondence between policyholder and insurer discussing a request for an endorsement, policyholder paid significant money for an endorsement to the title policy for additional coverage).

[28] *2016 WL 3055111, at *5.*

Attached is a chart setting forth a gap analysis of cyber insurance coverage, as well as the Willis Towers Watson Winter 2016 Cyber Claims Brief. Recently, the American Bar Association Cybersecurity Legal Task Force created a Cybersecurity Checklist.[29]

Conclusion

Cyber breaches can be risky for businesses. A good risk management plan, along with appropriate insurance, can help businesses successfully maneuver coverage obstacles in the event of a cyber breach. Cyber policies[30], commercial property policies and CGL policies are just a few of the sources of coverage to evaluate. Depending upon the circumstances, policyholders should also review their crime policies[31], directors & officers' liability policies and their errors and omissions or professional liability policies. Some insurance policies may not include exclusions and other language to limit coverage for cyber breaches. Should a cyber-breach occur, it is worth reviewing various policies carefully to see what coverage, if any, may be available.

---

[29] *See* http://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf

[30] Cyber extortion policies are also available on the market.

[31] *See Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012),* where the claim was submitted under a computer fraud rider to a Blanket Crime Policy and the court found that the data breach loss "resulted directly from the hacking, and an exclusion for loss of confidential information did not apply to the loss of customer information; *Medidata Solutions, Inc. v. Fed. Ins. Co., Civ. Action, 2016 U.S. Dist. LEXIS 178501 (S.D.N.Y 2016); Bitpay, Inc. v. Mass.Bay Ins. Co., Case No. 1:15-cv-03238 (N.D. Ga. Mar. 17, 2016)(Order attached); Ameriforge Group, Inc. v. Fed. Ins. Co., Case No. 4:16-cv-00377 (S.D. Tex. 2016); Principle Solutions Group, LLC v. Ironshore Indem., Inc.,Case No. 1:15-cv-04130 (N.D. Ga. Aug. 30, 2016)(Order attached); and Taylor & Lieberman v. Fed. Ins. Co., 2015 U.S. Dist. LEXIS 7935 (C.D. Cal. 2015).*