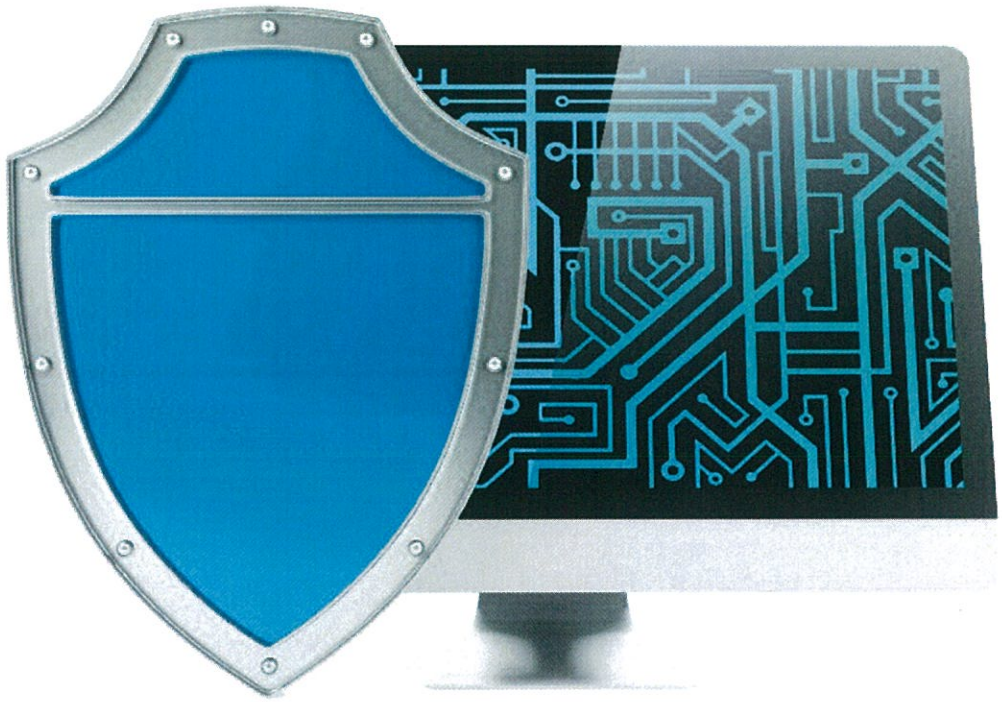

Cyber Insurance Risks for Insurance Brokers and Lessons Learned from Flood Exposures

by Jeffrey T. LaRosa and John P. Campbell

Hot topics in insurance broker malpractice claims typically follow the trend of hot topics in insurance coverage claims. In other words, insurance broker malpractice claim trends are often an offshoot of insurance coverage trends. One insurance broker malpractice trend that has received significant attention in recent years is a broker's duties concerning flood insurance. Another insurance broker topic that is likely to receive attention over the course of the next few years is cyber insurance. This article addresses broker malpractice claims that are likely to rise from the lack of cyber insurance coverage, and some comparisons to flood insurance claims.

Broker Malpractice, Generally

In New Jersey, it is well established that liability for breach of an insurance agent's duty to his or her client can occur if: 1) the agent neglects to procure the insurance, 2) the policy is void, 3) the policy is materially deficient, or 4) the policy does not provide the coverage the agent undertook to supply.[1] Every claim against an agent first starts with their client's loss or exposure. The loss typically becomes a claim to the broker's client's insurance company, but the claim is then denied. Then, the insurance agents are sued by their clients, usually at the same time the client sues the insurer. Infrequently, the client sues only the broker and not the carrier.

In the context of flood and cyber insurance, as with any broker claim, a client may allege that the agent committed malpractice because he or she obtained a materially deficient policy that did not cover the flood or cyber loss. The client may further allege that his or her agent was hired to obtain the client insurance to protect it against all potential losses. Some clients may allege specific requests, conversations, or communications regarding flood or cyber coverage. Other clients will allege more generally that they believed the general liability policy obtained by the agent was going to protect

the insured against a flood or cyber loss. Either way, the general claim is that the policy obtained is materially deficient because it did not cover the client for a flood or cyber claim.

Given the unresolved nature of cyber insurance, discussed more specifically below, it is also likely that some cyber malpractice claims will be brought against agents with the allegation that the cyber policy obtained does not provide the coverage the agent undertook to supply. In these instances, agents are likely dealing with clients who specifically sought and obtained some cyber insurance, but the particular loss at issue is not covered. These types of claims may arise against agents as the carriers continue to write non-uniform policies and take different positions on coverage.

Cyber Risk Insurance, Generally

In July 2003, California enacted a law regulating the privacy of personal information that also required notification when a data breach occurs.[2] Essentially, the law requires California businesses to disclose any breach of security regarding computerized personal information to any resident whose data was believed to have been disclosed.[3] The California law was the first of many U.S. security breach notification laws. New Jersey passed the Identity Theft Prevention Act in 2005, which requires New Jersey businesses to disclose breaches affecting New Jersey customers.

Following the creation of many security breach notification laws, cyber insurance policies were offered to address data breach expenses and increased liabilities. Cyber insurance provides coverage for such expenses as computer forensics, privacy or security breach notification and response, crisis management, and data loss or destruction. A typical cyber policy includes insuring agreements relating to more than one of these coverages, and may include other insuring agreements not principally directed at risks to personal identifying information. Commercial general liability (CGL) insurance policies cannot be relied upon for coverage relative to data breach losses. Therefore, like flood insurance before it, cyber insurance fills a coverage gap that may arise under CGL policies.

The Losses, Generally

New Jersey has had more than its fair share of flood losses in recent years, and a flood insurance loss is usually self-evident. Water comes. Property is destroyed. The damages occur most frequently in specified areas (flood zones) and, when damage occurs, it usually affects a number of properties at once. After the loss, the value of the lost property is assessed. The parties disagree about the total value, but a range is determined.

Data breach losses are increasing with regularity. They are less tangible and may not be discovered for quite some time after the breach. Moreover, the losses are impacting businesses across numerous industries, including healthcare, retail, entertainment, technology and law.

The losses may be caused by data breaches from inside or outside a business. For example, an internal breach might occur if an employee inadvertently discloses sensitive information with personal identifiers in an email to many people. An internal breach may also occur if an employee posts sensitive information on a social media platform or other outside website. A data breach initiated from outside a business might occur from the theft of computer hardware. A data breach might even occur if something falls off a truck.[4] Importantly, a data breach is not solely caused by a clandestine hack from China.

Once a data breach occurs, the costs will accumulate quickly. The businesses that suffer the data breach will be responsible for costs associated with their response, investigation and notification process. The extent of any business's notification process will vary, but it will be an expensive endeavor no matter what. For example, in New Jersey businesses are first required to notify the Division of State Police, in the Department of Law and Public Safety, for investigation or handling. Thereafter, once permitted by law enforcement agencies, customers must be notified "in the most expedient time possible and without unreasonable delay."[5] The notification must be made through written notice, through electronic notice or by substitute notice if the cost of providing notice would exceed $250,000.[6] Substitute notice consists of sending an email to customers, posting notice on the company's website and providing notification to the major news media.[7]

Businesses are required to promptly notify customers if their information has been compromised. They also need to quickly report the news to minimize disruption and loss of business, and to avoid or mitigate legal liability. Businesses might also be responsible for costs associated with any litigation that stems from the breach. Litigation may include claims alleging statutory violations governing consumer protection, as well as privacy and breach notification statutes. Litigation may also include consumer claims of negligence, fraud or breach of contract.

Businesses might also be responsible for costs associated with any regulatory prosecution and/or penalties. The defense of federal and/or state regulatory actions would be quite expensive. A business might also be subject to fines and penalties.

The Ponemon Institute LLC and IBM conducted a series of studies over the last several years to determine data breach costs. According to the 2015 study, the average cost for each lost or stolen record containing sensitive and confidential information is $217.[8] The

total average cost paid by organizations that participated in the study was $6.5 million.

Recent Cyber Coverage Decisions

With such significant costs at stake, the issue quickly turned to whether or not data breach costs would be covered by typical insurance policies. Most businesses have CGL policies, so the question became whether these cyber expenses would be covered by the CGL policy. The results (and the rationales behind those results) are somewhat mixed, but the developing trend seems to be that CGL policies do not cover cyber losses.

On Oct. 7, 2013, the U.S. District Court for the Central District of California held that the advertising injury coverage in a Hartford Insurance CGL policy provided coverage for a privacy breach.[9] Hartford insured Corcino & Associates, a technology consultant, under a CGL policy. Corcino and a hospital co-defendant were sued in class action lawsuits after the records of almost 20,000 patients were posted on a public website. The hospital provided the medical record data to its technology consultant, which in turn gave it to a job applicant to work with in order to evaluate his employment potential. The applicant then posted the data on a website used as a tutorial marketplace for programmers seeking assistance with data conversions. The data was discovered by one of the plaintiffs a year after it was posted. The plaintiffs filed suit, asserted various common law and statutory violations of privacy claims.

Hartford then brought a declaratory judgment action against Corcino alleging the statutory relief exclusion in the personal and advertising injury provision barred coverage for the class action claims. The policy provided that personal and advertising injury "[a]rising out of the violation of a person's right to privacy created by any state or federal act" is excluded from coverage. However, the court found coverage under the CGL policy for this data breach because "the right to medical privacy at issue in the Underlying Litigation was not created under either of the two statutes under which the plaintiffs seek relief." Instead, the court found that the statutes the plaintiffs relied upon in the class action lawsuits codified existing rights and, therefore, "the relief sought under these statutes can reasonably be interpreted to fall outside of Hartford's Policy exclusion."

However, a few months later, in Jan. 2014, the Appellate Court of Connecticut found that Federal Insurance Company and Scottsdale Insurance Company were not required to defend or indemnify insureds in a claim following the loss of computer tapes that exposed personal information of some 500,000 current and former IBM Corp. employees.[10] That decision was then upheld by the Supreme Court of Connecticut.[11] The facts of the *Recall Total* case establish that a data breach can occur in the most mundane ways.

IBM contracted with Recall Total Information Management, a data management firm, to transport and store computer tapes containing personal information of its employees. Recall Total then contracted with Executive Logistics to transport the tapes. Executive Logistics maintained a CGL and umbrella policy naming Recall Total as an additional insured. During transport of the IBM computer tapes a cart containing 130 tapes fell out of Executive Logistics' van. The tapes were never recovered and it was assumed they were retrieved along the road. The tapes contained the personal identification information of approximately 500,000 IBM employees, but there was no evidence that anyone ever accessed the sensitive information or that their loss damaged any IBM employee. Nevertheless, IBM spent more than $6 million to mitigate the damage and sought reimbursement from Recall Total and Executive Logistics.

Recall Total and Executive Logistics filed suit against Federal Insurance and Scottsdale Insurance, alleging a breach of the insurance contracts. Specifically, the insureds alleged that the loss of the computer tapes constituted a "personal injury," defined by the policies as an injury caused by an offense of electronic, oral, written or other publication of material that violates a person's right of privacy.

The defendants moved for summary judgment, which was granted by the trial court, which found the plaintiffs' losses were not within the scope of the personal injury clauses of the policies. The appellate court then affirmed the trial court's summary judgment, finding that despite the theft or loss of the information, the computer tapes did not constitute a personal injury as defined by the policies because there had not been a "publication" of the information resulting in a privacy violation. The Connecticut Supreme Court then affirmed the appellate court's decision.

In *Zurich American Insurance Co. v. Sony Corp. of America*, a New York trial court ruled along the same lines as the Connecticut courts.[12] Sony made a claim for litigation that arose from a well-publicized 2011 hacking event under a provision that covered liability for "oral or written publication in any manner of [the] material that violates a person's right of privacy." In Feb. 2014, a New York trial court issued a bench ruling that a hacking was a "publication" under Zurich's CGL policy. Nevertheless, the court denied coverage because the publication was not made by the insured itself. An appeal was filed, but later withdrawn.[13]

However, as recently as April 2016,[14] the Fourth Circuit upheld a District Court for the Eastern District of Virginia ruling that a CGL policy covers a data

breach.[15] In *Travelers Indemnity Co. of America v. Portal Healthcare Solutions LLC*, Travelers sought declaratory judgment that it was not obligated to defend its insured, Portal Healthcare, in a civil suit brought by patients whose private medical records were exposed on an unsecured server accessible through a Google search. First, the district court ruled that Travelers was obligated to defend Portal under its coverage Part B personal and advertising injury.[16] Then, the Fourth Circuit upheld the district court's decision in an unpublished opinion, finding coverage applied to the conduct alleged by the plaintiffs because exposing confidential medical records to online searching is "publication" giving "unreasonable publicity" to or "disclosing" information about a person's private life. Therefore, the court found Travelers had a duty to defend Portal against the underlying class action.

Key Events Identify a Gap Between Liability Exposure and Coverage Under a CGL Policy

Both flood insurance and cyber insurance have been spotlighted by key events. In the case of flood insurance, Hurricanes Katrina and Sandy shed light on the topic of flood insurance and the many problems associated with that coverage, which in turn has spawned a host of broker malpractice claims. In the case of cyber insurance, the topic has been highlighted by the publicity related to a number of high-profile security breaches, such as those at Target,[17] Sony, Wyndham Worldwide[18] and, more recently, Mossack Fonseca (the Panama Papers).[19]

And the need for flood insurance and cyber insurance is a consequence of those risks being denied coverage under traditional CGL policies. With respect to claims for damage resulting from flooding, the issue has always been whether the damage was the result of 'wind' damage, which is likely covered by the CGL policy, or 'water' damage, which is specifically excluded by a CGL policy. As indicated above, with respect to cyber insurance, early efforts to obtain coverage for cyber losses under a CGL policy have been met with, at best, mixed success, and the more high-profile cases, such as SONY, have denied coverage for cyber liability losses under CGL policies. And in any event, CGL carriers are making changes to their policies to clarify that cyber risks are not covered.

Curiously, the 'gap' in the market for flood insurance and cyber risk insurance has been filled in dramatically different ways. Regarding flood insurance, the federal government stepped in, creating the National Flood Insurance Program (NFIP), because it concluded that flood insurance would not survive in the private insurance market given the relatively low rates that could be charged and the potential for high exposures caused by significant, widespread weather events. Thus, while many flood insurance policies are written through private carriers, it is the federal government that ultimately pays the claim.

Conversely, private insurers are flocking to the cyber risk arena, which is causing its own litany of problems, most notably the fact that there is no uniformity to the policies, the exclusions, the limits or sub-limits.

With respect to broker malpractice claims relating to flood insurance, they primarily centered upon the broker's failure to offer any flood insurance to the insured. For the most part, the standardization of the NFIP policy precluded claims that the broker failed to adequately explain the policy or failed to secure the proper endorsements, etc. The NFIP further capped the policy limits at $250,000 building/$100,000 contents for residential and $500,000 building/$500,000 contents for non-residential or commercial. There is a private insurance market for properties with values beyond that permitted by the NFIP policies, and that market provided the potential for business interruption, contingent business interruption and off-site power failures, but relatively few broker malpractice claims were filed that addressed this niche market.

With respect to cyber insurance, it can safely be assumed that the range of broker malpractice claims will address a much wider spectrum of issues than did broker malpractice claims arising out of flood insurance. The first issue will be whether the broker properly understands cyber insurance. Unlike flood insurance, about which one can get a working knowledge after a review of any of the numerous NFIP publications available online, cyber insurance is an exceedingly complex and changing arena. Many of the smaller brokers may not fully understand the topic, which may lead them to simply ignore it. The statistics regarding the percentage of companies that have cyber risk insurance is startlingly low, and brokers' failure to address the topic is considered one of the primary causes.

Not only must the broker understand the topic, the broker must also be able to sift through the different offerings by the different carriers, which is no small feat. There is no standardization for cyber insurance at this time, and there is no indication that it will occur in the foreseeable future; thus, there is likely no Insurance Services Office (ISO) policy on the horizon for cyber insurance. By some estimates, there are around 50 cyber risk insurance policies that provide cyber risk insurance.[20] It is not reasonable to expect brokers to be knowledgeable about the nuances of every policy, particularly since the policies are ever changing. Instead, brokers are likely to be held responsible for understanding the basic cyber insurance issues and could potentially be held liable for failing to do so.

Presumably, the broker will be

required to ensure that he or she has done the following:

1. discussed the concept of cyber insurance with the insured;
2. offered cyber insurance that covers first-party claims, which would include expenses related to a data breach such as forensic investigations, lost profits, public relations costs and any costs notifying individuals whose private information has been accessed;
3. offered cyber insurance that covers third-party claims that would cover both private lawsuits against the insured and regulatory claims against the insured, include legal defense costs;
4. offered a policy that does not have sub-limits or exclusions that significantly limit the coverage or, if it does, that the insured is made aware of this fact;
5. offered a policy with appropriate limits. However, one would expect that the insured, not the broker, is best equipped to determine the potential severity of any cyber breach of the insured's information. As a result, one would expect the broker's obligation would be limited to informing the insured of the availability of coverage and that decisions regarding the amount of coverage are the responsibility of the insured.
6. upon the renewal of the policy, the broker made sure the renewal policy does not have any significant or material changes from the prior policy or, if it does, the broker notifies the insured of those changes.

Given that it is an emerging area, there are very few insurance broker malpractice cases that have been filed relating to cyber insurance. One interesting case[21] is winding its way through the courts in Louisiana. In that case, a hotel suffered a cyber attack involving credit and debit cards. The hotel sued its cyber insurance carrier and also sued its insurance agent, arguing that if the insurer's position is correct, the broker failed to procure appropriate coverage. Ironically, the hotel only obtained cyber insurance after having suffered a cyber attack the preceding year. The insurance policy in effect for this second loss had a $3 million policy limit, but only a $200,000 sublimit for monetary fines imposed by credit card companies for non-compliance with data security standards. This sublimit was modified from the preceding year. The complaint alleged that the agent was charged with knowledge of the types of insurance policies available, their terms and their coverage parameters. In an apparent nod to the complexity of the issues, the complaint further alleged that if the broker did not understand the policy, the broker had an obligation to discover what the policy included and excluded.

The broker filed a third-party suit against the wholesale broker through whom it had placed coverage. In the third-party complaint, the broker acknowledged that it had "no expertise" in procuring cyber insurance policies and, therefore, relied upon the wholesale broker who held itself out as having expertise in cyber insurance. The third-party complaint went so far as to quote from the wholesale broker's website to establish that it held itself out as an expert in the field. The broker criticized the wholesale broker for not informing it of the $200,000 sublimit.

The *Hotel Monteleone* case addresses a number of the topics listed above. First, the plaintiff questions whether the broker to whom they went properly understood this complex area. Second, it addresses the fact that there was, at least in the plaintiff's perspective, an important sublimit that was not explained by the broker. Third, as a result of the third-party complaint, it explains that, even when a broker involves a wholesale broker to procure coverage, that does not necessarily insulate the retail broker from being included in a suit. And regarding the wholesale broker, the broker may be inviting a higher standard of care either: 1) by holding itself out as an expert; or 2) by making promises or assurances on its website about its expertise in the area.

Conclusion

Cyber risk issues are a relatively new phenomenon, but they are here to stay. Accordingly, the need for cyber insurance is also here to stay, and will likely grow substantially. Moreover, it is an issue very much in flux due to the lack of homogeneity in cyber insurance policies and the relative infancy of cyber insurance coverage case law. These factors create a perfect storm that will likely lead to claims of coverage gaps, misplaced coverage and improper coverage. The end result will likely be that insurance brokers find themselves the subject of malpractice claims arising out of cyber risk issues just as they did for flood insurance issues, though the claims against them will likely be markedly different in nature.

Jeffrey T. LaRosa *is a partner and the co-chair of Schenck, Price, Smith & King's professional liability practice group. He also practices in the areas of insurance coverage, commercial litigation and construction law.* ***John P. Campbell*** *is counsel at Schenck, Price, Smith & King and a member of the firm's professional liability practice group. He also practices in the areas of commercial litigation, product liability, construction defects, and general negligence.*

ENDNOTES

1. *See Avery v. Armitage Agency*, 242 N.J. Super. 293, 300 (App. Div. 1990) *quoting Rider v. Lynch*, 42 N.J. 465, 476 (1964).
2. California S.B. 1386.
3. California S.B. 1386.

4. *Recall Total Info. Mgmt. Inc. v. Fed. Ins. Co.*, 147 Conn. App. 450 (Conn. App. Ct. 2014).
5. N.J.S.A. 56:8-163(a).
6. N.J.S.A. 56:8-163(d).
7. N.J.S.A. 56:8(d)(3).
8. Ponemon Institute, 2015 Cost of Data Breach Study: United States, Benchmark Research sponsored by IBM Independently conducted by Ponemon Institute LLC, May 2015. *See* www.ibm.com/security/data-breach.
9. *Hartford Casualty Insurance Company v. Corcino & Associates et al.*, CV 13-3728, United States District Court Central District (Oct. 7, 2013).
10. *Recall Total Info. Mgmt.*, 147 Conn. App. 450.
11. *Id.*
12. *Zurich Am. Ins. v. Sony Corp. of Am.*, 2014 N.Y. Misc. LEXIS 5141, 28-29 (N.Y. Sup. Ct. Feb. 21, 2014)
13. *Zurich Am. Ins. Co. v Sony Corp. of Am.*, 127 A.D.3d 662 (N.Y. App. Div. 1st Dep't 2015).
14. The article submission deadline was April 13, 2016. It is anticipated that additional decisions will be reached between the submission deadline and publication date. However, it is also anticipated that these decisions will not firmly resolve any of the cyber insurance coverage issues that will impact brokers in the realm of professional liability.
15. *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions*, 2016 U.S. App. LEXIS 6554 (4th Cir. 2016).
16. *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions*, LLC, 35 F. Supp. 3d 765, 767 (E.D. Va. 2014).
17. Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop, *New York Times*, Aug. 5, 2014, by Rachel Abrams. *See* http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html.
18. Wyndham Settles FTC Data Breach Charges, *Wall Street Journal*, Dec. 9, 2015, by Brent Kendall. *See* http://www.wsj.com/articles/wyndham-settles-ftc-data-breach-charges-1449680917
19. From Encrypted Drives to Amazon's Cloud, The Amazing Flight of the Panama Papers, *Forbes*, April 5, 2016 by Thomas Fox-Brewster. *See* http://www.forbes.com/sites/thomasbrewster/ 2016/04/05/panama-papers-amazon-encryption-epic-leak/#44be44c71df5.
20. Risk and Insurance, Analyzing Cyber Risk Insurance, Risk and Insurance, March 13, 2015, by Steve Raptis. *See* http://www.riskandinsurance.com/analyzing-cyber-risk-coverage/; Reuters, How to find the best cyber security insurance for your firm, June 26, 2015 by Matt Rybaltowski. *See* http://www.reuters.com/article/advisers-insurance-cybersecurity-idUSL1N0ZC0IV20150626.
21. *New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London, et al.*, Civil District Court for the Parish of Orleans, Louisiana (Docket No. 15-11711), filed Dec. 10, 2015.

This article was originally published in the June 2016 issue of New Jersey Lawyer magazine, a publication of the New Jersey State Bar Association, and is reprinted here with permission.