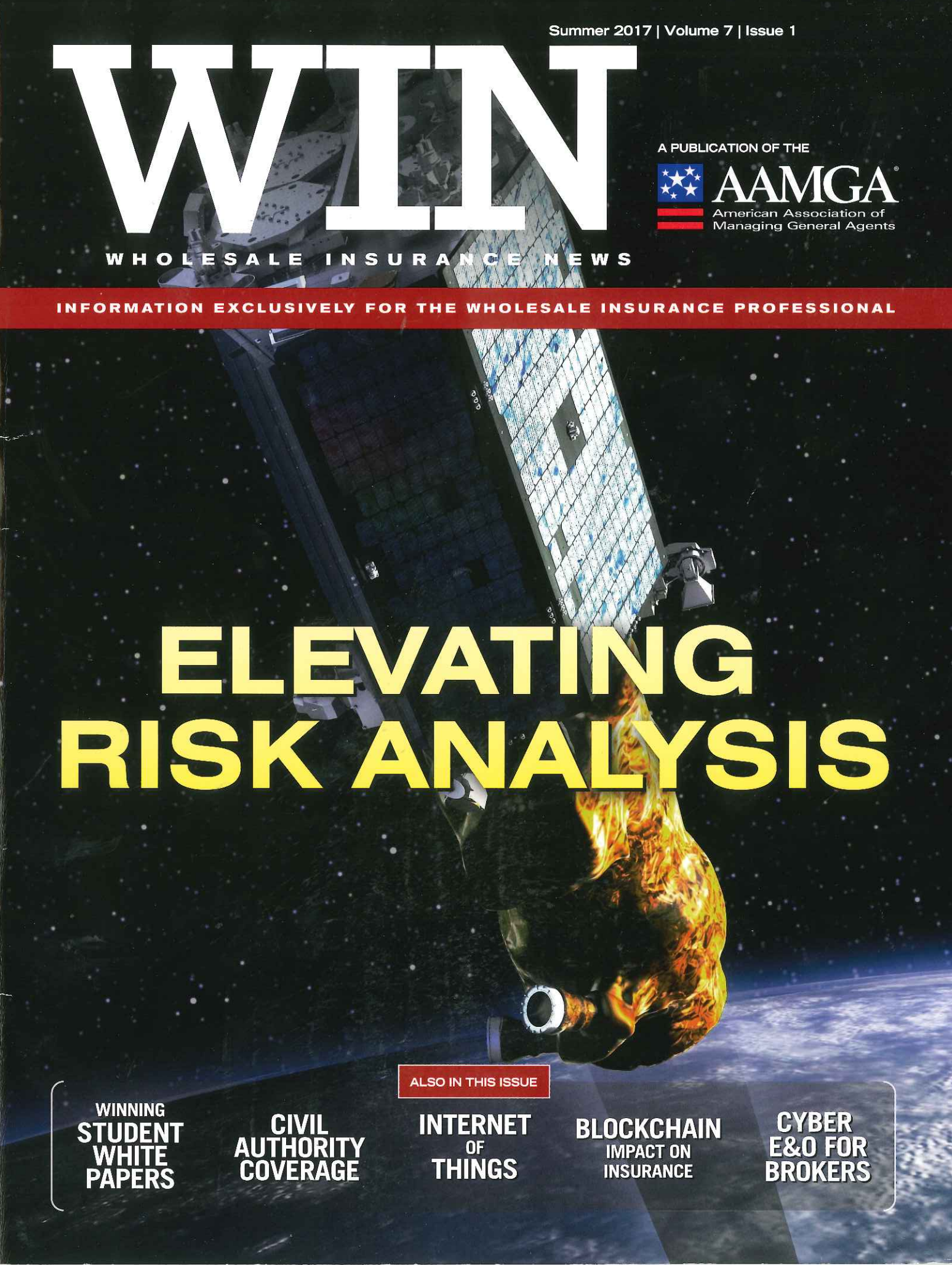
Summer 2017 | Volume 7 | Issue 1

WIN

WHOLESALE INSURANCE NEWS

A PUBLICATION OF THE
AAMGA
American Association of Managing General Agents

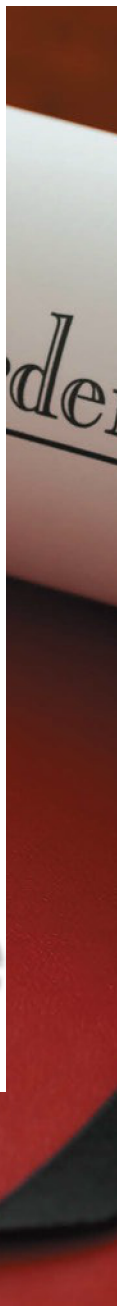
INFORMATION EXCLUSIVELY FOR THE WHOLESALE INSURANCE PROFESSIONAL



ELEVATING RISK ANALYSIS

ALSO IN THIS ISSUE

- WINNING STUDENT WHITE PAPERS
- CIVIL AUTHORITY COVERAGE
- INTERNET OF THINGS
- BLOCKCHAIN IMPACT ON INSURANCE
- CYBER E&O FOR BROKERS



The cyber broker insurance coverage conundrum

The first in a two-part series on cyber insurance.

by ELIZABETH S. FITCH, CIPP/US, AND THEODORE SCHAER, CIPP/US

Evolving E&O cyber-exposures against brokers include:

1. Failure to procure coverage for regulatory actions, fines and penalties;
2. Failure to recommend an adequate policy limit and to inform the insured of sub-limits;
3. Failure to procure coverage for payment card industry assessments; and
4. Failure to discuss ramifications of insured's failure to comply with the representations and warranties in the application.

IN 2014, BITPAY WAS DECEIVED INTO TRANSFERRING $1.85 million into a hacker's account. Imagine the shock when its cyber insurance carrier denied the claim.[1] More recently, a U.S. District Court ruled that P.F. Chang's China Bistro's insurer was not obligated under its cyber policy to reimburse the restaurant for $1.9 million in assessments levied by MasterCard following a massive data breach.[2] Why didn't the insurance agent or broker selling these insurance policies point out the critical policy deficiencies and the importance of the application representations?

Ignorance or lack of due diligence is the most probable explanation. According to insurance cyber coverage expert Kelly Geary, principal coverage counsel and claims leader for Integro, "cyber insurance products in the market today are still relatively immature largely because the underlying risk itself is not fully understood or appreciated. Part and parcel of this conundrum is the fact that there are few individuals within the cyber insurance marketplace — brokers, underwriters, claims professionals etc. — that have a deep understanding of the products or the risk. So, 'caveat emptor!'"

Insurance brokers are exposing themselves to risks by selling cyber insurance endorsements and policies without fully understanding them or their client's cyber risk profile. With the avalanche of cyber breach claims, companies are pressuring their brokers to procure comprehensive cyber coverage. Companies are assuming that the purchase of a cyber policy provides complete financial protection. They assume wrong, as do some wholesale agents and brokers. When the cyber insurer rightfully denies coverage, insureds are looking to their insurance agents and brokers to make them financially whole, in turn triggering a new wave of litigation: Errors and omission claims against retail producers, wholesale agents and brokers.

DUTIES IMPOSED ON CYBER INSURANCE BROKERS AND AGENTS

Jurisdictions have uniformly adopted a general duty to act with reasonable care, skill and due diligence in procuring requested insurance for clients. Most jurisdictions have also imposed a "duty to advise," in which the broker is held responsible for failing to offer the insurance coverage for which the insured "should have been" advised. For example, in *Southwest Auto Painting & Body Repair v. Binsfield*, the broker "fell below the standard of care" for failing to advise to procure "employee dishonesty and theft coverage," which resulted in the client's uninsured loss.

The duty to advise places a heightened burden on insurance agents and brokers to have a complete, working knowledge of the intricacies of the different cyber insurance policies available. Each client will require a unique analysis to determine which cyber policy or coverage will best suit their needs. This requires brokers to familiarize themselves with the risks faced by their client and to negotiate for a policy that is sufficient to encompass the risks in case of a cyber breach.

This is further complicated by insurance carriers' lack of knowledge in regard to underwriting cyber risks as well as reluctance to tailor policy language (manuscript policies versus standardized policy language) to meet a particular client's needs. Policy triggers for coverage are further blurred by definitions incorporated into the policy that leave room for ambiguities to arise. The summation of these issues coupled with the agent or broker's lack of understanding their customer's cyber needs creates an influx of new litigation being brought by dissatisfied customers against both brokers and agents.

CHALLENGES FACING CYBER INSURANCE BROKERS

The speed at which cyber risk has evolved, and continues to evolve, has left courts, legislators, regulators, insurance carriers, insurance brokers and the business world in a state of frustrated confusion. Insurance brokers are often on the front line when it comes to helping businesses transfer and manage cyber risks. As a result, brokers are in a highly precarious position with respect to liability exposure arising in connection with the counseling and placement of cyber insurance products.

The three current challenges facing agents and brokers are:

1. THE RAPID EVOLUTION OF THE EXPOSURES AND THE INSURANCE PRODUCT. The cyber insurance cover is in a state of relative infancy and is developing with rapid inconsistency. Over 50 carriers offer stand-alone cyber insurance products and almost all carriers offer some level of cyber insurance via endorsements to traditional products. These stand-alone cyber insurance policies are lengthy and complex and can be heavily endorsed. Most policies contain multiple insuring agreements — a combination of third-party "liability" coverage and first-party "direct"

coverage. Unfortunately, because this is still a "new" product, the market has not yet reached a level of standardization in coverage scope, defined terms or terminology. As a result, comparing coverage offered by one carrier to that offered by another is difficult.

2. **THE ADEQUACY OF LIMITS.** Companies often heavily rely on insurance brokers to advise them on the amount of insurance they should purchase. When answering this question in connection with traditional lines of insurance, the broker has significant historical and industry/peer-group data upon which they can rely. This data does not yet exist when it comes to cyber insurance products. To further complicate things, many cyber insurance products contain multiple different limits, with sub-limits and even sub-limits *within* sub-limits.
3. **STAND-ALONE COVERAGE.** Cyber risk does not (yet) fit squarely within any one insurance product. As a result, insurance brokers must consider and advise clients on how a stand-alone cyber insurance policy would interact with the company's other traditional insurance policies, such as comprehensive general liability, crime, property and professional liability. Evaluating the overlap and interaction is challenging and time consuming and requires an in-depth knowledge of insurance products and coverage across multiple lines of business. Unfortunately, the challenges facing brokers will likely multiply; at least until the cyber insurance market has some sufficient loss data behind it and finds some semblance of standardization.

The learning curve is steep because technology is rapidly changing, hackers are becoming more sophisticated and laws are constantly evolving. There is no question that brokers are in a conundrum. No policy is "one-size fits all" in the cyber insurance world. At a minimum, cyber insurance brokers should be asking the right questions to ensure the business is covered for potential losses from a cyber breach. Rigorous training and education is the best way for agents and brokers to prepare themselves. As Benjamin Franklin once said, "An investment in knowledge pays the best interest."

SOURCES:

1 Smith (2015). "Cyber Insurance rejects claim after BitPay lost $1.8 million in phishing attack." *Network World*. Retrieved from http://www.networkworld.com/article/2984989/security/cyber-insurance-rejects-claim-after-bitpay-lost-1-8-million-in-phishing-attack.html

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).

Elizabeth S. Fitch, CIPP/US, is managing partner with the Righi Fitch Law Group in Phoenix, AZ; contact her at ***beth@righilaw.com****.*

Theodore M. Schaer, CIPP/US, is a partner in the Zarwin, Baum, DeVito, Kaplan, Schaer & Toddy law firm in Philadelphia, Pennsylvania; contact him at ***tmschaer@zarwin.com****.*