February 2020


THE BETTERLEY REPORT

# TECHNOLOGY ERRORS & OMISSIONS MARKET SURVEY—2020

***Decent Growth with Some Insurers Bumping Up Rates***

Richard S. Betterley, LIA
President
Betterley Risk Consultants, Inc.

## Highlights of this Issue

- New First-Party Coverage Tables Added
  - — Business Interruption
  - — Theft, Including Extortion and Deceptive Funds Transfer
- Corvus Added to this Report; NAS Removed Following Acquisition by Tokio Marine HCC
- ISO Marketstance Predicts That Tech Errors and Omissions (E&O) Premium Growth Will Outpace the Greater E&O Market

## Next Issue

*April*
*Intellectual Property and Media Liability Market Survey*

**Editor's Note:** *In this issue of* The Betterley Report, *we present our 19th annual evaluation of technology errors and omissions (E&O) insurance in which we review 21 of the leading insurers active in the market.*

*For 2020, we added Corvus and removed NAS, which was purchased by Tokio Marine HCC, which is included in this report.*

*First-party coverage for business interruption and theft (including extortion and deceptive funds transfer, also known as account takeover or social engineering) has become more available on tech E&O products. We have added three new tables to capture and present critical information about these coverages.*

*Some insurers contend that these coverages should not be a part of the tech product, which is based on third-party exposures. Instead, it should be a part of a cyber product. We see their point.*

*However, since many tech E&O sellers are offering cyber as an optional extension to their product, we felt it would be helpful to risk managers and their advisers to capture relevant information here.*

*Tech E&O is not immune from the continuing expansion of insurers into the specialty insurance segment, and insurers look to this expanding opportunity to help fuel their growth. Cyber exposures of tech companies make demand for this coverage stronger than in the past, and lawsuits by hacked clients will make the purchase even more compelling. Lawsuits such as that brought by Affinity Gaming (a breached casino) and its cyber-security provider Trustwave will become more common. This will increase demand but also increase pressure on rates.*

*While each insurer was contacted in order to obtain this information, we have tested their responses against our own experience and knowledge. Where they conflict, we have reviewed the inconsistencies with the insurers. However, the evaluation and conclusions are our own.*

*Of course, the insurance policies govern the coverage provided, and the insurers are not responsible for our interpretation of their policies or survey responses.*

*In the use of this material, the reader should understand that the information applies to the standard products of the insurers and that special arrangements of coverage, cost, and other variables may be available on a negotiated basis. Professional counsel should be sought before any action or decision is made in the use of this information.*

## List of Tables

## Introduction

Coverage for the liability arising out of the design and manufacturing of technology-related products, the creation and implementation of software, and the provision of related services is a growing business, with specialty coverages designed to cover the E&O liability that may not be covered under traditional liability policies. Tech E&O coverages can be purchased for technology consultants, systems integrators, application service providers, Internet service providers, Internet retailers, cloud services providers, network electronics manufacturers, medical technology manufacturers, and telecom companies. With a wide variety of coverages available, and each written on a nonstandard form, insureds and their advisers can be confused and bewildered by the choices.

The crush of data breaches affecting the clients of technology services providers is having an effect on the tech E&O line. Applicants for coverage that provide data security and/or breach forensic services are increasingly being questioned about their activities and E&O controls relating to data security products and services. As more clients realize that a data breach is expensive and, at best, only partially insured by their own cyber policy, we expect that there will be more lawsuits like *Affinity Gaming v. Trustwave Holdings Inc.,* No. 2:15-cv-02464 (D. Nev. Dec. 24, 2015).

At this time, we are not aware of any new standard policy wordings related to data security services, but we would not be surprised to see them pop up.

Coverage for breach of data privacy continues to be the hot topic in tech E&O product discussions, as both service providers and site owners grow increasingly anxious about loss of data. While most of the news has been about data breaches suffered by site owners, technology service providers have been—or ought to be—concerned about their own exposures. When we talk with our tech E&O readers, many express worries about their exposures emanating from both their client work and from breaches of their own data security.

There is confusion in the marketplace about data privacy coverage for service providers. This coverage is generally referred to as tech E&O and covers the professional liability exposure of the service provider. But what about the data breach that is not the fault of the service provider but that involves client data that it controls?

Our approach, adopted in 2012, makes the information presented more helpful to the readers. Our goal is to clarify the coverages for each of the three types of risk.

A service provider's data breach risk can arise from any or all of the following.

- Its failure to prevent a breach of its client's data, which is a third-party exposure and should be covered under an E&O form
- A breach of its own data, which would not be covered under E&O and is a first-party cover just like data breach coverage is in a cyber policy
- A breach of client data while in its possession, perhaps through a network breach, theft of a laptop, or similar means

Some insurers and brokers seem to assume that a claim for any client data breach is a result of a professional error or omission and, therefore, covered by the basic tech E&O policy. Our concern, though,

## Companies in this Survey

The full report includes a list of 21 markets for technology errors and omissions insurance, along with underwriter contact information, and gives you a detailed analysis of distinctive features of each carrier's offerings. For a sneak preview of the full report and all it has to offer, view the new 2020 Report Highlights.

is that coverage for breach of data that is not a result of an error or omission might also be needed.

Take, for example, a situation in which the tech provider finds that some of its client data have been breached. Would not the client expect the provider to arrange (or at least pay for) the response? Would not the provider want to step in and make the client whole? And would not that help reduce the chance of an E&O claim? We think the answer is "yes" to all of these questions.

For more on this topic, please see our discussion on data privacy beginning on page 7.

Tech E&O policy provisions should always be reviewed in connection with the insured's commercial general liability (CGL) policy provisions, especially with respect to new or emerging exposures of concern. Some insurer markets offer coordinated E&O and CGL coverage, whereas other markets may offer monoline E&O only. Coverage not provided or excluded by an E&O policy may well be addressed by the CGL. Given the complexity of the coverage choices, a good insurance broker can offer a lot of useful advice to prospective insureds, and their value in negotiating coverage is not to be underestimated.

## State of the Market

The tech E&O market is an attractive place for insurers, as economic growth is faster than in other areas. However, exposures are more difficult to evaluate, at least compared with more traditional risks.

Still, the technology sector is not exactly new. Some insurers have been writing this line for 30 or more years. Change comes fast, though, so sources of claims can appear suddenly and unpredictably.

### *Premium Volume and Growth Rates*

Annual premium volume information provided about the tech E&O market continued to be provided by some insurers. As in years past, we surveyed participating tech E&O product managers, asking them for a range of gross written premiums for US-based insureds and for non-US-based insureds.

Several key insurers do not provide information about their own premium volume, so we remain concerned about the reliability of any premium estimates. Interest is clearly strong, though, as insureds and their business partners see the need for coverage in a world where litigation alleging technology errors and omissions or a data breach is all too common. Unfortunately, rates remain somewhat weak, and that interest is being spread over more insurers.

Still, we unearthed a few useful nuggets of information about market size and rate direction.

One leading insurer estimates that the total global market is $1 billion–$2 billion of premium and that the United States is 60–80 percent of that. The market size is hard to estimate in part because some insurers include the premiums for the cyber and media coverage portions of the tech policy in their totals.

In our view, we would count the cyber and media-attributable premiums from a tech policy in the premium totals and, therefore, support the $2 billion estimate.