THOMSON REUTERS

Westlaw®

Cyberclaims and litigation against insurance professionals

By Robert A. Stines, Esq., *Freeborn & Peters*

MARCH 2, 2018

Technology such as cloud computing, machine learning, the "internet of things" and autonomous vehicles are changing society. Along with these rapid societal changes, cyberthreats are evolving more quickly than chief information security officers can deploy systems to anticipate and prevent breaches. While these breaches were once considered threats only for larger corporations, they since have become problems for smaller companies and individuals as well.

This increased risk of cyberevents presents a fertile market for the insurance industry to create new products. Insurance professionals who aim to serve the needs of their corporate clients (whether large or small) must market and provide advice about these new products.

The numerous vectors for cyberattacks — and the uncertainty surrounding how these new insurance products will respond to cyberclaims — has increased the risk of litigation against insurance professionals.

This analysis will briefly discuss uncertainty related to cyberinsurance policies, litigation against insurance agents and brokers, the evolving duty to advise clients about cyberinsurance, and risk management considerations to avoid litigation.

CYBERINSURANCE POLICIES

Although there are exceptions, courts have generally decided that commercial general liability insurance does not cover cyberevents. To avoid confusion, many insurance carriers now affirmatively exclude cyberclaims from CGL policies.

Carriers are clearly communicating to insureds that they must obtain separate coverage addressing today's cyberrisks in the form of cyberinsurance policies.

Unfortunately, the language in these policies is not standardized and is customizable depending on the carrier. Claims filed under them are frequently challenged in court, and each new court decision provides some answers — but also more confusion.

Confusion regarding coverage can easily arise when a social engineering vector causes an insured to wire funds to unintended recipients. A vector is the term used in the cybersecurity industry to describe the method of a cyberattack. Is the attack a cyberevent, criminal fraud, employee error or all of the above?

In *Medidata Solutions v. Federal Insurance Co.*, through a sophisticated scheme of spoofed emails, a Medidata employee was tricked into wiring $4.8 million to an overseas account. Medidata held a $5 million insurance policy with Federal. The policy contained a "crime coverage section" addressing loss caused by various criminal acts, including computer fraud coverage and funds transfer fraud coverage.[1]

Relying on the policy, Federal argued that Medidata's loss was not covered by the computer fraud clause because the emails did not require access to Medidata's computer system, a manipulation of those computers, or input of fraudulent information.

> The Medidata and American Tool cases illustrate the lack of agreement regarding what is and what is not covered under cyber-related policies.

In challenging causation, Federal argued that "there is no direct nexus" between the spoofed emails and the fraudulent wire transfer. The insurer also challenged coverage under the funds transfer fraud clause because the bank wire transfer was voluntary and with Medidata's knowledge and consent.

The court explained that "a thief sent spoofed emails armed with a computer code into the email system that Medidata used." To achieve the spoof, the thief's computer code changed data in email addresses. The fraud tricked several high-level employees to consent to the wire transfers out of Medidata's own bank account.

Ultimately, the court found coverage under the computer fraud clause and funds transfer fraud clause.

In a similar case, Travelers prevailed in a computer fraud claim case against its policyholder, American Tooling Center Inc.[2] After receiving emails that appeared to be from one of its vendors, ATC authorized payments to a bank account it believed belonged to the vendor. But the emails were fraudulent, and the fraudsters received the payments.

ATC sought coverage from Travelers under the computer fraud provision of its policy. Travelers argued ATC did not incur a covered loss under the policy. Specifically, it contended "computer fraud" encompasses a digital attack vector that causes loss but does

not encompass the use of a digital vector to defraud the organization through an employee's behavior.

The court decided that although spoofed emails were used to impersonate a vendor and dupe ATC into transferring funds, they did not constitute the "use of any computer to fraudulently cause a transfer."

There was no infiltration or "hacking" of ATC's computer system. The emails themselves did not directly cause the funds transfer; rather, ATC authorized the transfer based upon the information received in the emails. Hence, the court ruled that Travelers was not liable for losses from an email-based theft scheme.

The Medidata and American Tool cases illustrate the lack of agreement regarding what is and what is not covered under cyberrelated policies. Underwriters and courts are still grappling with what is considered a "cyberclaim." This creates a significant problem for insurance professionals who offer cyberinsurance policies to clients.

LITIGATION AGAINST INSURANCE PROFESSIONALS

Though it did not involve a sophisticated cyberevent, the fallout from a data breach experienced by Perpetual Storage, a Colorado Casualty Insurance Co. insured, illustrates the exposure insurance professionals may face.

Perpetual Storage stored certain records, including hard copies, microfilm, microfiche and magnetic computer tape on behalf of the University of Utah. Backup tapes containing personal information of 1.7 million patients were stolen from a Perpetual Storage employee's car.

The university said the theft caused it to incur more than $3 million in costs, consisting of one year of credit monitoring expenses for each impacted patient, printing and mailing costs, phone bank costs, and other miscellaneous expenses.

Colorado Casualty filed a declaratory judgment action contending that Perpetual Storage's policy did not cover the university's credit monitoring expenses or notice costs. Perpetual Storage file a third-party claim against its insurance broker alleging, among other things, negligent procurement of insurance, breach of fiduciary duty and failure to advise.[3]

After three years of litigation, the parties stipulated to a dismissal of all claims, counterclaims, cross-claims and third-party claims.

In 2011 an Illinois corporation engaged in electronic commerce sued its insurance broker alleging reduced revenues for a period of seven months due to a cyberattack that destroyed the corporation's electronic commerce capability. The agent procured a policy that included "business income extension for websites" coverage for only the first seven days of lost revenue.

The corporation filed claims against the insurance broker for negligence and breach of contract.[4] After several years of litigation, this case also ended with a dismissal by stipulation.

In a 2016 case, a Louisiana hotel alleged breach of contract, disputing the coverage limit of a cybersecurity policy issued through underwriters at Lloyd's of London. The hotel also named the insurance agent in the suit.

The hotel alleged that when it sought cyberinsurance coverage, it required a policy that would cover operational fraud and operational reimbursement amounts for fraudulent charges and the cost of replacing payment cards as a result of a cyberattack.

The agent procured a policy with total policy limits of $3 million; however, unbeknownst to the hotel, the policy contained a sub-limit of $200,000 for operational fraud and operational reimbursement amounts.

The retail agent filed a third-party claim against the wholesale broker who claimed to have specialized in cyberpolicies.[5] The parties quickly resolved the dispute and filed a joint motion to dismiss, which the court granted.

These cases are examples of situations in which a policy to cover cyberexposure was warranted based on the client's business operations. But what if the insured does not specifically request a cyberinsurance policy?

If every company, large or small, is theoretically at risk of a cyberbreach, then insurance professionals may have an affirmative duty to advise corporate clients about cyberrisks and available coverage.

DUTY TO ADVISE

Generally, an insurance agent or broker who undertakes to procure insurance for another and fails to do so may be held liable for damages resulting from the failure. As a general proposition, insurance agents and brokers do not have a duty to advise insureds as to the coverage needs.[6]

However, a well-developed body of case law has established an exception to this general rule. The exception applies if a "special relationship" exists between the broker and client, thereby triggering an enhanced duty of care to advise the client about the amount of coverage needed to completely meet its insurance needs.[7]

Case examples supporting a finding of a special relationship include situations in which:

- The agent misrepresented the nature of the coverage being offered or provided, and the insured justifiably relied on that representation in selecting the policy.[8]
- The agent voluntarily assumed the responsibility of selecting the appropriate insurance policy for the insured (by express agreement or promise to the insured).[9]

- The agent professed expertise in a field of insurance being sought by the insured, and the insured relied on that expertise.[10]
- The agent or broker exercised broad discretion to service the insured's needs and received compensation above the customary premium paid for the expert advice provided.[11]
- The agent was intimately involved in the insured's business affairs or regularly gave the insured advice or assistance in maintaining proper coverage.[12]

If an insurance professional has a corporate client and a special relationship exists, then there is arguably a duty to advise the client about the availability of cyberinsurance policies.

WHAT IS AT STAKE?

Cyberevents in which thousands of people have their personally identifiable information stolen (including events involving Equifax, Home Depot, Target and Yahoo) garner extensive media coverage. Less attention is paid to attacks carried out using other vectors, like ransomware, which prevents a company from accessing information unless a ransom is paid.

In 2017, the WannaCry and Petya ransomware attacks impacted thousands of computers and blocked user access to data systems unless and until users made ransom payments. And ransomware attacks have already been reported in 2018.

In January Hancock Regional Hospital was hit with a ransom demand for bitcoin from hackers who encrypted data files associated with the hospital's most critical information systems.[13] After notifying the FBI, its attorneys, cybersecurity specialists and the cybersecurity insurance company, the hospital made the decision to pay the hackers for decryption keys to access the data files and restore its information technology network.

Another troublesome vector is a denial-of-service attack that disrupts customers' access to an organization's system, such as an attack that affected Twitter, Netflix and Sony's PlayStation network.[14] There is also the social engineering vector in which an employee is tricked into transferring funds or confidential information.

These types of cyberattacks cause business interruptions that could lead to losses amounting to hundreds of thousands of dollars. While larger corporations may survive such an attack, smaller uninsured companies may be forced to shutter.

And companies may pursue litigation against the insurance professional who failed to procure adequate insurance. If found liable, an insurance professional may have to pay the difference between the coverage that should have been in force, but for the error, and the actual net insurance recovery, if any.

ISSUES TO CONSIDER

With all this in mind, insurance professionals should appreciate the demand and need for cyberinsurance policies for every company that relies on computers and the internet — essentially every company. Although cyberinsurance is still relatively new, there are many insurance professionals who have in-depth experience and knowledge in this area.

But beware: The risk of litigation is extremely high if an insurance professional claims expertise in cybersecurity and the client suffers a breach that results in a denied claim.

Likewise, when an insurance professional is intimately involved in the insured's business affairs (for example, handles all the insurance needs for the client or regularly provides advice in maintaining proper coverage), then the agent should advise about cyberrisks, in writing, and engage a broker with far more knowledge.

In addition, when offering a cyberpolicy, insurance professionals should take great pains to review the language of the policy with the client. The client should understand what is, and what is not, covered. Because courts are still grappling with the language in some policies, there are no guarantees. At the very least, the insurance professional and the client should review the policy's exclusions and definitions.

The definitions of "confidential information" and "personally identifiable information" are the most fundamental in a cyberinsurance policy.

Some policies define confidential information broadly as any information from which an individual may be uniquely and reliably identified or contacted. This may include an individual's name, address, telephone number, Social Security number, account relationships, account numbers, account balances, account histories or passwords. Under such a definition, an individual's name, on its own, could be considered PII.

In contrast, other policies may identify very specific items that are considered confidential information that may mirror state-specific definitions of PII. For example, Florida defines personal information as an "individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: a Social Security number; a driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account," etc.

Beware of exclusions for contractual liability; criminal conduct; terrorism, hostilities and claims arising from "acts of foreign enemies"; and unauthorized collection of customer data. These exclusions could have unintended consequences.

A criminal conduct exclusion would bar any claims that resulted from a social engineering scheme. An exclusion for terrorism could bar cyberbreaches that resulted from foreign actors or governments.

Similarly, an exclusion for unauthorized collection of consumer data could affect any company engaged in online activities, especially activities in which consumer financial data is collected.

Although not a bulletproof defense in litigation, an insurance professional could attempt to limit the scope of services, in writing, to exclude any advice regarding cyberinsurance. From a business perspective, an agent or broker may not want to refer clients to competitors to evaluate cyberrisks.

EMBRACE THE FUTURE

Like many industries, insurance will change and evolve as society embraces new internet-reliant technologies. Insurance professionals will have to understand how new technology and the advent of cyberspace will affect their clients.[15] Failing to embrace, evolve and implement strategies to offer insurance products for the cyberage will expose insurance professionals to litigation.

NOTES

[1] *Medidata Sols. Inc. v. Fed. Ins. Co.,* 268 F. Supp. 3d 471, 472 (S.D.N.Y. 2017).

[2] *Am. Tooling Ctr. Inc. v. Travelers Cas. & Sur. Co. of Am.,* No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017).

[3] Perpetual Storage Inc.'s Answer, Counterclaim and Third-Party Complaint, *Colo. Cas. Ins. Co. v. Perpetual Storage Inc.,* No. 10-cv-316 (D. Utah July 8, 2010), 2010 WL 1141910.

[4] Complaint, *Learning Enhancement Corp. v. Haywood & Fleming Assocs.,* No. 2011-L-013210 (Ill. Cir. Ct. Dec. 11, 2011), 2011 WL 6440349.

[5] Third-Party Complaint, *New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London,* No. 16-cv-61 (E.D. La. Mar. 28, 2016), 2016 WL 1221443.

[6] Gary Knapp, Annotation, Liability of Insurer or Agent of Insurer for Failure to Advise Insured as to Coverage Needs, 88 A.L.R. 4th 249, § 3, 1991 WL 741640 (1991); *Emerson Elec. Co. v. Marsh & McLennan Cos.,* 362 S.W.3d 7 (Mo. 2012).

[7] *See* generally *Peter v. Schumacher Enters. Inc.,* 22 P.3d 481 (Alaska 2001), and *Fitzpatrick v. Hayes,* 67 Cal. Rptr. 2d 445 (Cal. Ct. App., 1st Dist. 1997).

[8] See, e.g., Fitzpatrick at 452.

[9] *See, e.g., Harts v. Farmers Ins. Exchange,* 597 N.W.2d 47, 51-52 (Mich. 1999).

[10] *See, e.g., Meridian Title Corp. v. Gainer,* 946 N.E.2d 634 (Ind. Ct. App. 2011); *Warehouse Foods Inc. v. Corporate Risk Mgmt. Serv.,* 530 So. 2d 422 (Fla. 1st Dist. Ct. App. 1988).

[11] *See e.g., Sintros v. Hamon,* 810 A.2d 553 (N.H. 2002).

[12] *Buelow v. Madlock,* 206 S.W.3d 890 (Ark. Ct. App. 2005).

[13] Grace Johansson, Cyber-attack shuts down US Regional Hospital's online system, SC Media, Jan. 16, 2018, 2018 WLNR 1733059.

[14] Raphael Satter, Internet attack disrupts service, web-traffic manager Dyn Inc. struck twice, Associated Press, Oct. 22, 2016, 2016 WLNR 32536680.

[15] This article is not intended to provide an exhaustive risk analysis for insurance professionals; it is only the tip of the iceberg. The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

This article appeared in the March 2, 2018, edition of Westlaw Journal Insurance Coverage.

ABOUT THE AUTHOR

Robert A. Stines is a partner at **Freeborn & Peters** in Tampa, Florida. He is a trial lawyer focused on defending professionals against malpractice and errors-and-omissions claims. A part of his practice is concentrated on legal issues created by emerging technologies. He can be reached at rstines@freeborn.com.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.