Cyber Insurance, Rescission, and Damages Exposure: Words No One Wants to See Together

A Practical Guidance® Article by Marc O. Dedman, Barton LLP

Marc O. Dedman
Barton LLP

This article addresses the practical, and potentially existential, impact to policyholders demonstrated in a recent Illinois case involving the rescission of cybersecurity insurance coverage resulting in no coverage to the policyholder post-loss.

For additional guidance on cyber insurance, see Cybersecurity Insurance, Cybersecurity Insurance Initial Considerations, and Cybersecurity Insurance Policies Review Checklist.

Overview

Between July 6, 2022, and August 26, 2022, two court filings were made in Illinois which will, unquestionably, impact businesses' approach to cybersecurity and insurance coverage. Those two court filings were:

- A complaint on July 6, 2022, brought by an insurance company against its policyholder –and–
- The voluntary dismissal of the lawsuit on August 26, 2022, by the insurance company with a concomitant stipulation by the policyholder that the policy was rescinded, and agreed between the parties to be null and void after the loss to the policyholder had occurred

The filings were made in litigation styled Travelers Property Casualty Company of America v. International Control Services, Inc., 2:22-cv-02145 in the U.S. District Court for the Central District of Illinois. Though the facts involved an agreed order between the two parties in that case, the practical impact is arguably as important to other policyholders as a citable decision would be.

Though the dates of the lawsuit's filing and dismissal were only 51 days apart, profound impact occurred illuminating the obligations and risks that exist if a cyber insurance application is incorrect. The ramifications of the lawsuit show the:

- Effort necessitated by a business in purchasing cybersecurity insurance
- Approach to be undertaken by management within that business regarding the application for cybersecurity and insurance coverage
- Obligation of companies in their efforts to demonstrate the existence of an acceptable cybersecurity program
- Responsibilities of in-house and outside counsel advising clients –and–
- Responsibilities of (and potential liability to) directors and officers

Case Analysis

The allegations in the complaint were that International Control Services, Inc. (ICS) submitted a CyberRisk Tech Application seeking insurance coverage from Travelers on March 31, 2022. In the CyberRisk Application, ICS gave the names of its CEO and President when asked to "[p]rovide the name and title of the person responsible for the Applicant's network and information security."

As part of its CyberRisk Tech Application, ICS, through its President, responded "Yes" to the inquiry:

> 60. Indicate whether the Applicant requires multi-factor authentication for:
>
> a. Administrative or privileged access

. . .

and responded "N/A" to the inquiry:

> 60. Indicate whether the Applicant requires multi-factor authentication for:
>
> . . .
>
> b. Remote Access to its network by its employees and third parties.

As part of its application for insurance coverage, ICS provided Travelers also with a Multi-Factor Authentication Attestation. It was signed by ICS's President on March 10, 2022. In that attestation, he responded "yes" to all the following inquiries:

MULTI-FACTOR AUTHENTICATION ATTESTATION

1. Multi-Factor authentication is required for all employees when accessing email through a website or cloud-based service.
2. Multi-Factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers.
3. In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:
    a. All internal & remote admin access to directory services (active directory, LDAP, etc.)
    b. All internal & remote admin access to network back environments.
    c. All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.)
    d. All internal & remote admin access to the organization's endpoints/servers.
4. The signer of this form has done so with the assistance of the person in charge of IT security.

In that Multi-Factor Authentication Attestation, it was explained to ICS that:

> Multi-factor authentication refers to the use of two or more means of identification and access control – sometimes referred to as "something you know, something you have, or something you are." A username and password, for example, is something you know. Requiring a code sent via text message (SMS) establishes "something you have," i.e., a mobile phone belonging to you. Biometric authentication, through a fingerprint or retina scan, establishes "something you are." Multi-factor authentication is successfully enabled when at least two of these categories of identification are required to successfully verify a user's identity when accessing systems.

Travelers alleged that the Multi-Factor Authentication Attestation made clear to ICS the importance of requiring multi-factor authentication and the minimum controls required to be present for an applicant to be eligible for a policy. Travelers alleged that the Multi-Factor Authentication Attestation further provided:

> The controls described above and listed below are the minimum controls that must be in place in order to be eligible for a Cyber policy. Because of the importance of the controls in preventing ransomware attacks the following attestation should be completed with the assistance of the person(s) in charge of IT security.

Travelers alleged that after receiving the application documents, and in reliance upon the statements and information contained in them, it issued the Cyberize Tech policy to ICS with effective dates of April 4, 2022, to April 4, 2023. The aggregate limit of liability for all loss was alleged to be $1,000,000, subject to applicable retentions. The policy premium was $22,193.00.

In its complaint, Travelers alleged that, on December 20, 2020, which was prior to the policy period that was involved in the litigation, ICS had been the victim of a ransomware attack. ICS disclosed the incident to Travelers during the policy application process and represented that it had instituted cybersecurity improvements following that 2020 event. However, on May 25, 2022 (coincidentally 51 days after the effective date of the policy) ICS was alleged by Travelers to have been targeted again by another ransomware attack. Travelers was given notice of the event on May 31, 2022.

During its investigation of the 2022 event, Travelers discovered that at the time ICS completed and submitted the application documents, ICS was not using multi-factor authentication to protect its server—ICS was using multi-factor authorization only to protect its firewall, not any other digital assets. Travelers alleged that because multi-factor authentication was not utilized to protect its server and various other digital assets at the time ICS applied for the policy, ICS's statements made in its application documents were misrepresentations, omissions, concealment of facts, and incorrect statements.

On August 26, 2022, Travelers and ICS filed a joint Stipulation for Rescission and Dismissal with the court in which they agreed that no insurance coverage was available to ICS under the policy, requested the court to rescind the policy, and requested that the court declare the policy null and void from its inception. An order to that effect was entered by the court four days later on August 30, 2022. The case was then terminated.

The complaint was not complicated. For the significant impact the lawsuit was intended to have on ICS, the complaint was

short and straightforward. Travelers asked the court for a post-loss rescission of the insurance policy, and a declaration that there was no insurance coverage available for any losses, costs, or claims submitted by ICS and a declaration that the insurance policy was null and void. The ruling obtained by Travelers was the one sought by Travelers.

Significantly, the result of the language of the court's Order for Rescission and Dismissal stating that ". . . no insurance coverage shall be available to any person or entity under the Policy for past, present, and future claims, suits, loss, costs, or expenses of any kind whatsoever," left ICS itself potentially exposed to the risks arising due to the loss of its cyber insurance coverage. That language would mean that under the Travelers policy, there was no indemnity available to ICS or obligation by Travelers to indemnify or defend anyone at ICS for claims that would have been encompassed within the policy, including claims that might be made against them personally.

Potential Exposure

Personal exposure of officers and directors, although existing and evolving, is more limited in the United States than in other jurisdictions; however, such exposure can be triggered in some jurisdictions, particularly civil law jurisdictions, for certain officers and directors who are found to be liable to claimants who were not made whole as a result of the bankruptcy of the company. In the case of a loss of cyber insurance coverage, claims could potentially be made by international vendors, creditors, or investors under the laws of their countries (not the U.S.) and in the language of that country against those who otherwise would have been covered under the rescinded cyber policy and potentially other coverages that might have been impacted by the rescission. The potential for exposure to directors and officers of a company whose policy was rescinded would be alarming even if the directors and officers (D&O) coverage were not impacted by the loss of cyber insurance coverage. If a loss of cyber coverage did impact the D&O coverage, the effort by a director or officer to locate an attorney for personal representation in a non-U.S. jurisdiction could be overwhelming, particularly in a country whose language is different than that used by the officer or director.

For attorneys advising their clients and for the companies for whom the attorneys do their work, in addition to the potential for devastating effect on the company and its officers and directors arising from the loss of insurance coverage, what are takeaways from the very short-lived Travelers v. ICS litigation? The answer is more than the conclusion that one seeking insurance must try to be accurate in what is stated on an application for cybersecurity insurance coverage. The application must be accurate. An inaccurate response may not be determined until after the loss occurs. How to be accurate in completing the insurance company's cybersecurity and data protection questions likely will require more than asking someone in the IT department for information, the completeness of which might have been wrongfully assumed to be known by that person asked. In fact, the information needed to fully answer such an insurance questionnaire, attestation, or application may be in an IT department and other departments including, for example, the chief information officer, the chief information security officer, HR (Human Resources), the insurance department, the law department, and potentially with others in the organization. A benefit in the process of obtaining answers from the various departments may be that the risks the company faces, and the types of coverage most needed, become more apparent. The inquiry will facilitate risk identification and make indemnity amounts that are necessary to cover that risk clearer. Utilizing an insurance broker that has experience with such insurance applications and risk exposures may be appropriate, particularly as risks and exposures to the company change over time. For some companies, depending on the risks identified and the premiums needed to mitigate those risks through an insurance company policy, perhaps the creation of captive insurance may be appropriate.

Looking Ahead

Potential exposure can be significant to owners and shareholders, directors and officers, creditors, and others whether a cyber loss is one that would be included in a first-party insurance policy which provides coverage for losses to those insured in the policy or in a third-party policy which provides coverage for those who are insured involving claims brought against them by others. The repercussions of a rescinded insurance policy, whether a first-party policy or a third-party policy, could be existential to policyholders, causing the policyholder to go out of business. As cyber exposures increase, and the information needed to obtain insurance coverage becomes more technical, those seeking coverage for such losses should be aware of the issues implicated in only 51 days in Travelers v. ICS.

Law360 Articles

- Misrepresentations Voided Co.'s Cyber Policy, Travelers Say (July 7, 2022)
- FTC Actions Highlight Companies' Cybersecurity Efficiency (Jan. 4, 2023)
- Cyber Hygiene Could Have Policyholders Awash In Litigation (Aug. 3, 2022)
- Policyholder Best Practices As Cyberattacks Escalate (Sept. 3, 2021)

Related Content

State Law Comparison Tool

- Punitive Damages

Practice Notes

- Cybersecurity Insurance
- Cybersecurity Insurance Initial Considerations
- Cyber Insurance, Related Coverage Litigation, and Insurance Coverage for Data Breach Risk
- Insurance Application Process
- Data Protection in the Insurance Industry
- Insurance Policy Rescission, Cancellation, and Nonrenewal of Commercial Property Insurance Policies
- Director and Officer (D&O) Insurance
- COVID-19 Directors and Officers (D&O) Coverage Litigation

Practice Videos

- Impact of New York Insurance Laws and Regulations on Cybersecurity Video
- NAIC Data Protection & Cybersecurity Models and Principles for Insurers Video

State Law Surveys

- Insurance Policy Rescission Standards State Law Survey
- Punitive Damages Standards State Law Survey
- Punitive Damages Insurability State Law Survey

Templates

- Director's and Officer's (D&O) Liability Insurance Policy

Checklists

- Cybersecurity Insurance Policies Review Checklist
- Data Protection in the Insurance Industry Checklist
- Insurance Policy Rescission, Cancellation, and Nonrenewal Checklist
- Insurance Application Process Checklist
- Directors and Officers (D&O) Liability Insurance Selection Checklist

Marc O. Dedman, Partner, Barton LLP

With over 30 years of civil and common law experience, Marc Dedman is a Partner in the Nashville office focusing on business transactions, insurance coverage and bad faith claims, litigation, and risk mitigation.

Marc successfully counsels his clients on the complexities of purchasing and managing insurance; and using insurance as part of an overall risk-management program. A significant portion of his practice focuses on first-party and third-party insurance claims, insurance recovery and dispute resolution, risk management and crisis management, loss prevention and cost containment. His clients include public and private companies, organizations, boards of directors, individual officers, and other policyholders. He also frequently advises and represents insurance brokers on coverage issues.

Marc is deeply familiar with the insurance companies and their policies. He can translate insurance wording for his clients so they understand, and effectively interpret, contracts so they are better able to avoid denial or delays in claims. He works with policyholders to analyze, negotiate, and manage terms and contracts to minimize risk or the possibility of future litigation. If litigation becomes inevitable, Marc's significant trial experience allows him to persuasively advocate in both state and federal litigation for the coverage his clients are entitled to and have purchased.

In addition to his insurance expertise, Marc puts his MBA to work in collaborating with the firm's transactional, cybersecurity, tax, and corporate attorneys to offer a comprehensive set of business services to clients. He remains an active and outstanding leader in the international business community, and he is also consulted by international law firms for his capabilities spanning across multiple practice areas.

Marc has a history as a strong advocate in the courtroom and alternate dispute resolution proceedings. His experience in resolving problems after they occur has also made him a valuable legal ally in helping to avoid problems before they occur for domestic and international clients alike.

He is a member of the Tennessee Bar Association International Law and Practice Section Executive Committee. He is Vice Chair of the International Practice Committee of the International Association of Primerus Law Firms, where he also serves as Chair of the Insurance Practice Group. He has moderated international panels, including at Belmont University School of Law in Nashville, Tennessee; Tulane University School of Law in New Orleans, Louisiana; and for the International Association of Primerus Law Firms at events in Washington, D.C. and Miami, Florida.

Marc has an "AV Preeminent" peer review by Martindale-Hubbell, has been selected to both Super Lawyers and Best Lawyers, and was named "Best of the Bar: International" by *Nashville Business Journal* in 2017 and 2019. He is also a Fellow of the Litigation Counsel of America, an invitation-only trial lawyer honorary society limited to less than one-half of one percent of American lawyers. Before entering private practice, Marc served four years in the U.S. Army Judge Advocate General's Corps, primarily in Washington, D.C. He was awarded the U.S. Army Commendation Medal, the Meritorious Service Medal, and the Army Air Assault Badge. Marc also enjoys running, having participated in 5 Boston Marathons, the New York City Marathon, the Marine Corps Marathon, the Bogotá, Colombia Half Marathon, and numerous other races of various distances.

Prior to joining Barton, Marc was with Spicer Rudstrom, PLLC in its Memphis and Nashville offices for 30 years. He was Spicer Rudstrom's managing partner from 2015-2018, managing six offices in three states, including the firm's HR and personnel, IT, finance, insurance, and strategic planning. Marc's clients have said they like working with him because he practices as a lawyer but thinks like a businessperson.

LexisNexis®