Published on *The National Law Review* https://natlawreview.com

Practical Implications of Travelers v. ICS for Cyber Insurance Brokers, Carriers and Policyholders: Emerging Trends & Predictions – Takeaways from the Cyber Insurance Webinar

Article By:

Richard J. Bortnick

Jonathan E. Meer

The need for cyber insurance has become increasingly critical due to more frequent and severe cyber breaches and mounting damages threatening the business practices of small to medium-sized enterprises (SMEs) and mega-entities alike. This vital risk transference mechanism is evolving rapidly, as are the expectations of carriers, brokers and potential insureds in light of the *Travelers v. International Control Services* case and other cyber-related matters. The December 7, 2022, Wilson Elser webinar "Practical Implications of *Travelers v. ICS* for Cyber Insurance Brokers, Carriers and Policyholders: Emerging Trends & Predictions," moderated by Richard Bortnick (Of Counsel-New York) and featuring Jonathan Meer (Partner-New York), J.P Wilson (CEO, Global Cyber Risk Advisors Corp.) and Dale Schulenberg (Claims Manager, Coalition, Inc.), offers perspectives on cyber insurance from their various vantage points of coverage counsel, cyber risk adviser and broker/claims manager.

For the playback webinar, click here (passcode: ga1*+%ug).

Procedural History

Travelers Property Casualty Company of America v. International Control Services Inc. was filed on July 26, 2022, in the U.S. District Court, Central District of Illinois. Travelers sought a declaratory judgment and the rescission of a cyber insurance policy it had issued to ICS, an electronics manufacturing services company, after a ransomware attack on a server lacking multi-factor authentication (MFA). Travelers denied coverage and sought to rescind the cyber policy due to alleged material misrepresentations in the ICS application signed by the CEO regarding the enterprise-wide use of MFA.

On August 30, 2022, an order and judgment were entered with Travelers and ICS stipulating Travelers asserted that it relied on incorrect statements made by ICS in its application in issuing the policy. Travelers and ICS further stipulated and agreed to the entry of an order rescinding the insurance policy and declaring it void from inception. While the case is limited to its facts on MFA and the rescission of the policy was stipulated by the parties and later ordered by the court, it spotlighted

the importance of MFA and the reliance on its use by insurance carriers.

Travelers Implications

There are essential takeaways from *Travelers v. ICS* to examine that have implications for coverage litigation going forward. The takeaways suggest strategies to help manage the expectations of the insurers feeling compelled to impose increasingly stringent measures to reduce future claims risk and educate the insured on the best path to follow in securing a new policy and maintaining it, year after year. Such coverage is vital to operational resiliency in a seemingly hardening market that has prompted harsh policy terms for the foreseeable future.

Takeaway *#1*

As a result of the Travelers *case and escalating cybercrime losses, underwriting questions may become more specific, requiring insurers to be more intensive in their applications and to explicitly look for minimum requirements and controls in place to protect an insured's network and any personal identifiable information.*

Important questions for cyber policy underwriters to consider:

- Is MFA in place for emails, third-party access to emails, on servers and VPNs, in remote access protocols, and on the network for domain controller-type credentials – adding an extra layer a threat actor would need to penetrate?
- Is the entity performing timely backups, and are these done online or offline?
- Are secure processes in place for initiating money transfers to prevent the fraudulent transfer of funds?

Takeaway *#2*

Representations made upon application for coverage or presumed to continue at the time of renewal require evidence to back them up, which could be requested at any time by insurers/carriers looking to protect their downside risk.

In conjunction with the growing need for cyber policies by SMEs and larger entities is the necessity for insurers to understand what is and isn't being disclosed by potential insureds, as occurred in *Travelers* with ICS's failure to employ the system-wide MFA it represented it had. When applying for coverage and making a representation about meeting cyber minimum requirements, a potential insured's assertion needs "teeth," with the entity able to back up and demonstrate with evidence the integrity of its security safeguards allegedly in place.

Tools to assess a potential insured's vulnerability to cyber-attack are increasingly available, such as external scans and penetration tests. Insurers can utilize these means and consider collaborating with cyber risk management firms to complete the job. At the same time, potential insureds can proactively seek out a technology consulting firm to work with their insurer and broker – to illuminate the best path to securing a new policy by identifying areas of cybersecurity weakness needing attention.

Takeaway #*3*

Pre-binder minimum requirements must evolve continually to keep pace with growing hacker sophistication.

Cybersecurity policies and language continue to evolve and contain more conditions in response to new security threats. There is the potential for new policies to stipulate different levels of coverage depending on the number or extent of security requirements met, particularly those related to MFA because of the *Travelers* decision. And ongoing proof of safeguards requested at the renewal stage of a cyber policy should apply to both past requirements and new ones added to the evolving lists.

Takeaway #*4*

Insureds Advised to Be Proactive

Potential insureds should put minimum requirements in place, including entity-wide MFA, and be prepared to demonstrate their existence with evidence before applying for a binder, during the renewal process or anytime an insurer asks. Keeping up with the expanding list of requirements arising from new threats also is key. This proactive behavior will engender the goodwill of the insurer in minimizing risk and accelerate both getting and keeping a cyber policy, not to mention avoiding any potential for rescission.

Emerging Trends in Cyber Security Cases

Growing Responsibility Borne by C-suite Executives

With cyber insurance applications becoming more complex, lengthy and technical due to increasing losses caused by cyber breaches, average CEOs may not possess the skills to fully comprehend the questions asked. They may look to others who better understand the technical nature of the questioning to respond or attest to the information provided. As such, it would behoove potential insureds, perhaps even in conjunction with the underwriters, to do penetration testing at the outset of the binder procurement process to better understand their entity's security vulnerabilities.

However, times are changing, and before long those in the C-suite may routinely be required to sign off on or attest to disclosures regarding cybersecurity measures. Until then, insurers should perform their due diligence before accepting the risk and strongly consider assessing their exposure through external scans that provide a better idea of the "attack surface" of the entity seeking coverage.

CTO & CISO Involvement in the Cyber Insurance Application Process

Another question arising more and more often is whether an entity's Chief Technology Officer and the Chief Information Security Officer, if there is one, should provide the technical information requested on the cyber insurance application. The answer may be regulated sooner rather than later, but it appears that the industry consensus is moving toward a resounding "yes."

D&O Suits Growing

Another trend in the cyber insurance arena is the emergence of more D&O suits arising from cyber incidents. As little as 10 years ago, D&Os weren't held to a high standard regarding representations made to the market about their company's security management. Today, it is increasingly incumbent

on C-suite executives and boards to be proactive, provide funding for cybersecurity, be knowledgeable about the protections used and ensure that the financing is ample to address the entity's security needs.

Cyber Claims

With increasing global tensions and the heightened risk for cyber-attacks, insurers are now reviewing the language and scope of their policies to ensure sufficient coverage should a cyber-attack occur. This likely will lead to an evaluation of the policy provision language, though a potential standard cyber policy language is unlikely. Going forward, cyber incidents will undoubtedly earn different classifications, parties (such as nation-state and non-state actors) will be redefined, and even the definition of what war-like scenarios and exclusions consist of could change within evolving cyber policy language.

Conclusion

Insurance companies are constantly adapting in underwriting cyber risk to combat increasingly sophisticated data breaches, ransomware and cyber-attacks. With the cost of cyber-attacks continually escalating, insurers are being asked to insure against revenue loss, business disruption, equipment damages, public relations expenses related to reporting and notification, forensic investigation, legal fees and potential third-party lawsuits, among other business growth challenges.

Key insurer and broker considerations arising from the *Travelers* decision and recent cyber-related actions suggest:

- Continually updating binder application questions to reflect additional details about cybersecurity procedures and technology in place to help address more sophisticated cyber threats.
- Requiring MFA on all digital assets as a minimum requirement.
- Helping to mitigate risk by using third-party scanning and penetration testing to point out concerns to the potential insured and facilitate the issuance of the proper amount of coverage.
- Ensuring the potential insured's funds transfer security protocols are adequate to prevent fraud and theft.

National Law Review, Volume XIII, Number 39