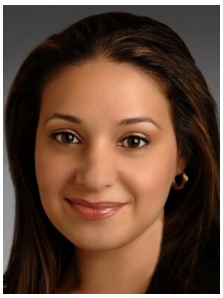
Less Cyber Coverage, More Compliance Risk For Cos.

By **Luma Al-Shibib and Steven Pudell** (May 12, 2023)



Luma Al-Shibib

Steven Pudell

Last year, policyholders received several favorable decisions recognizing coverage for cyber losses under various types of policies, including crime and all-risk property policies.

Before companies seeking to ensure adequate coverage for cyber risks had the opportunity to realize benefits from these decisions, insurance companies introduced new policy exclusions seeking to further limit their exposures.

The new policy exclusions, coupled with new regulatory requirements, potentially create a new set of liability risks for cyber defense and compliance to which companies must devote resources.

New Cases

One of the most significant decisions on cyber risk coverage last year was issued on Jan. 13 by the Superior Court of New Jersey, Law Division, Union County, in Merck & Co. v. ACE American Insurance Co.[1]

The court in Merck refused to apply the war exclusion in an all-risk property policy to bar coverage for $1.4 billion in losses the German pharmaceutical company suffered as a result of the NotPetya cyberattack.

The exclusion barred coverage, in pertinent part, for losses from "hostile or warlike action … by any government … or by any agent of such government."

Merck's insurance carrier, ACE, argued that the exclusion was triggered — and precluded coverage — because the NotPetya malware attack had been deployed by the Russian Federation as part of its ongoing hostilities with Ukraine.

The court disagreed with the insurance company, and instead interpreted the exclusion as applying only to traditional warfare involving armed hostilities. Significant to the court's decision was the fact that the exclusion had never been applied outside the ordinary confines of traditional warfare.

Additionally, the court noted that cyberattacks have been a known risk for some time, and if ACE had wanted to exclude coverage for such attacks it could have, but failed to do so.

The court, therefore, found Merck's interpretation of the exclusion, as applying only to traditional forms of warfare, to be reasonable.

In affirming on May 1, the Superior Court of New Jersey, Appellate Division, held that the plain meaning of the war exclusion "require[d] the involvement of military action," and "did not include a cyberattack on a non-military company that provided accounting software for commercial purposes to non-military consumers, regardless of whether the attack was instigated by a private actor or a 'government or sovereign power.'"

In November 2022, after the trial court's decision in Merck, but while the appeal was still

pending, another case addressing the applicability of the war exclusion to NotPetya-related losses, Mondelez International v. Zurich American Insurance Co. in the Circuit Court of Cook County, Illinois, Chancery Division, settled in the middle of trial for an undisclosed sum.[2]

New Insurance Directives and Forms

Possibly reading the tea leaves, Lloyd's of London issued a directive last summer, effective March 31, 2023, requiring all Lloyd's stand-alone cyber policies to include a cyber war exclusion in addition to any traditional war exclusion already part of those policies.

According to Lloyd's, the cyber war exclusion is meant to exclude losses arising from cyberattacks attributed to state actors. Under the new exclusion, attribution of cyberattacks is to be determined by the government of the affected state.

If no attribution has yet been made by the government of the affected state, the new exclusion allows insurance companies to make an objectively reasonable inference as to attribution.

Although the insurance industry apparently was reluctant to adopt the new cyber war exclusion, such exclusion appears to be gaining traction among other insurance carriers — outside of Lloyd's — which also have added similar exclusionary language to their policies.

The vague wording used in these new cyber war exclusions raises numerous questions and concerns. The most significant of them are:

- What entity within the government decides attribution?
- What if different entities reach different conclusions?
- What constitutes an objectively reasonable inference regarding attribution?

Although most litigation for cyber-related losses has involved claims under non-cyber-specific policies, this will likely change with the introduction of these new cyber war exclusions in cyber-specific policies.

In addition to the cyber war exclusions, insurance companies have introduced other limitations to their cyber coverage in response to the evolving nature of cyber threats, including a 50% sublimit for losses occurring as a result of catastrophic cyber events.

Moreover, losses from cyberattacks because of a failure to timely patch known software vulnerabilities, which constitute a substantial cause of cyber breaches, are now being excluded from coverage under recently introduced policy wording.

For example, one new policy provision excludes coverage for a breach that exploits a known software vulnerability that is not patched within 45 days of its publication on the National Vulnerability Database.

New Regulatory Actions

These same risks have also garnered the attention of regulatory authorities. For example, in March, law firm Heidell Pittoni Murphy & Bach LLP settled with the New York attorney general for $200,000 for a cyberattack it suffered as a result of its failure to timely fix a known vulnerability within the Microsoft Exchange server, for which a patch had been released months earlier.

The attack resulted in the exposure of confidential health data for over 100,000 firm clients. Going forward, insurance companies adding the failure-to-patch software vulnerability exclusions to their policies likely may invoke these exclusions in an effort to deny coverage for similar settlements.

As this last example demonstrates, while cyber insurance carriers are rewriting their policies to limit the type and scope of losses they cover, regulatory entities are imposing more onerous reporting requirements and adopting harsher penalties for noncompliance.

The New York Department of Financial Services Cybersecurity Regulation — Title 23 of the New York Codes, Rules and Regulations, Part 500 — which applies to banks, insurers and financial services companies, went into effect in 2017 and has already been updated once, with a second amendment now pending.

The second amendment to the regulation includes enhanced controls and reporting requirements, greater cybersecurity governance at the C-suite level, 24-hour notification for any extortion payment and an obligation to review and test cybersecurity controls annually.

The regulation already authorizes heavy penalties for violations, which the DFS has demonstrated its willingness to use — even without the added notification and enhanced control requirements proposed by the second amendment.

In October 2022, for example, EyeMed Vision Care LLC, which is licensed to sell insurance in New York, settled with the DFS for $4.5 million because it failed to implement multifactor authentication and conduct threat assessments as required under the regulation.

Due to its failure to implement sufficient cybersecurity controls, a cyberattack EyeMed suffered exposed more than six years' worth of customer data, comprising the sensitive, nonpublic, personal health information of hundreds of thousands of consumers, including minors.

In addition to the monetary settlement, EyeMed also agreed to undertake significant remedial measures to shore up the vulnerabilities in its system and comply with the regulation's security controls.

This March, the U.S. Securities and Exchange Commission also proposed new cybersecurity rules to its existing framework.

The new proposed rules, including a reopened comment period for cybersecurity rules proposed in 2022, are intended to create more stringent reporting requirements and greater cyber controls on investment companies, broker dealers and other market entities, including clearing agencies, and national securities exchanges.

Under the proposed amendments, various regulated entities must, among other things, (1) adopt written cyber breach response procedures; (2) provide notice, within 30 days of becoming aware of the incident, to individuals who are reasonably likely to be affected; (3) annually assess the effectiveness of their incident response plans and procedures; (4) notify the SEC of an incident within 48 hours of having concluded that it is a significant cybersecurity incident; and (5) make public disclosures regarding the nature and scope of any cybersecurity incidents that occurred.

The new proposed reporting requirements increase the SEC's management over regulated

entities' implementation of cybersecurity policies, controls and systems.

On the one hand, the rules force regulated entities to adopt stringent cybersecurity and hygiene controls, to the extent they have not already done so, thereby presumably better protecting those entities from successful attacks, but also better positioning them to meet the onerous conditions that insurance companies are now imposing, and hopefully enabling them to realize a recovery under their policies.

On the other hand, the focus on reporting may shift already scarce resources and attention away from actual breach response and mitigation efforts. Hester Peirce, one of the five SEC commissioners, has criticized the reporting requirements as onerous and burdensome:

the Commission has apparently decided its role is to be an enforcer demanding that a firm dealing with a cybersecurity attack first and repeatedly attend to the Commission's voracious hunger for data.

[T]his proposal demonstrates that our priority is to create even more legal peril for a firm in this situation, legal peril that will distract employees of the firm from mitigating immediate threat to the firm and its customers as they navigate the aggressive deadlines and open-ended information demands of the Commission.

Whatever final iteration of the rules is ultimately adopted, it will set the cybersecurity compliance and reporting standards to which all companies — not just regulated entities — likely will adhere.

Nonregulated entities — which don't come within the purview of the proposed rules — nevertheless will have to meet the SEC's requirements if they want to do business with regulated entities.

Thus, at the same time that insurance companies are trying to craft ways to offer less coverage for cyber losses, the potential liability companies are facing from cyber incidents is increasing, with companies being forced to spend more to meet the new strict reporting requirements, while simultaneously facing potential fines and penalties for significant sums, for any failure to satisfy the new reporting requirements.

Conclusion

In the current environment, companies seeking to minimize their own exposure are advised to review their current policies to understand the scope of coverage and the potentially applicable exclusions and limitations thereto.

Luma Al-Shibib is a shareholder and co-chair of the cyber insurance recovery group at Anderson Kill PC.

Steven Pudell is a managing shareholder at the firm.

[1] No. UNN-L-002682-18, 2022 WL 951154, *1 (N.J. Super. Ct. Law Div. Jan. 13, 2022), aff'd, No. A-1879-21, A-1882-21, (N.J. App. Div. May 1, 2023).

[2] Case No. 2018-L-011008 (Cook County Illinois Chancery Court).