The Impact of Merck's NotPetya Policy Claims and a Reported Settlement: The Cyber Insurance Pendulum Swings, Again

By definition, insurance policies represent an exercise in planning for (and hedging against) catastrophe. Cyber insurance for the healthcare industry is no exception. But any hedge is only as good as it's reliable. Many healthcare providers have been left high and dry when seeking to collect on their policies – finding their claims 'carved out' by exclusionary language. This swinging pendulum may be heading in the other direction, however, if a recent reported settlement is any indication.

Merck Settlement

Merck & Co. (Merck), a pharmaceutical company, was a 2017 target of the global NotPetya attack. Merck alleged $1.4 billion in damages. Involved cyber insurers tried to avoid payouts by relying on policy exclusions relating to war. A New Jersey appellate court upheld a lower court ruling that such exclusionary language did not apply to *cyber*warfare, which it distinguished from *physical* warfare. Before the New Jersey Supreme Court was set to hear oral arguments, Merck and several insurers recently reached a confidential settlement concerning the alleged damages (reported here). This may indicate a sea change in policy construction – one that providers inking policies should approach with eyes open, and that insurers likewise will approach with due care.

The Evolution of the Cyber Insurance Marketplace

Prior to 2017, cyber insurance was still emerging, and polices were comparatively less prevalent. Indeed, many insurers were competing for business, driving down the cost of cyber insurance. Within the last five years, however, there has been an increase in ransomware attacks, causing an uptick in the need for cyber insurance. Simultaneously, losses escalated, and insurers began to implement more stringent standards while charging higher premiums. This caused various entities to institute better 'cyber-hygiene' through tactics such as multifactor authentication (MFA) endpoint detection and response (EDR). (For more information on this dynamic, please see this 2023 presentation delivered by Gabriel Oberfield, one of this piece's co-authors.)

Indeed, insurers are requiring companies to implement and maintain specific security controls that comply with the evolving landscape, such as the National Institute of Standards and Technology (NIST) framework. Moreover, insurers now require details regarding a company's information security practices, including whether companies have MFA and EDR in place, and some insurers have begun mandating ongoing cybersecurity awareness trainings on the premise that when employees are informed, it mitigates risks and lessens any downtime an attack may cause.

Disputes concerning implementation of safeguards are far from unusual. For instance, at least one notable university sued Lloyd's of London for the expenses related to a breach that exposed the personal information of patients at the university's health facilities. According to Lloyd's of London, the university, which it insured, failed to comply with data security provisions under its policies.

The Pendulum Swings, Again

Whether driven by the Merck settlement or otherwise reading the writing on the wall, some insurers have begun to exclude coverage for the effects of *cyber*warfare, including but not limited to state-sponsored attacks. According to reports, Lloyd's of London has instituted numerous such exclusions.

Where Attorneys Can Help

As the pendulum sways, it is important for policyholders carefully to consider and negotiate the reach of exclusionary language during cybersecurity policy binding and renewal periods.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including in the cyber insurance space. If you have any questions about this memo, please contact Gabriel Oberfield, Victoria Okraszewski or any attorney in Bond's cybersecurity and data privacy practice.