Merck’s $1.4 billion cyberattack claim – the specter of NotPetya

Insurance Business Magazine

Court ruled insurers could not rely on exclusion

A US state appeals court last week dealt a blow to a group of insurers relying on a war exclusion to avoid paying up for a chunk of a $1.4 billion insurance claim from NotPetya cyberattack victim Merck.

The appeal ruling is expected to add further fuel to a flurry of wording tightening and exclusions, and a cyber insurance expert has said that were a NotPetya equivalent to hit today then many payouts would likely be triggered.

In June 2017, malware NotPetya snuck into the systems of organizations worldwide after infecting Ukrainian accounting software. The White House and others would go on to condemn Russian action against Ukraine for the cyber onslaught, which drove collateral damage in the billions, with swathes of businesses affected across a reported 65 countries. Among the biggest NotPetya victims was pharmaceuticals giant Merck.

Now, Merck’s insurers have been told by the New Jersey appeals court that they could indeed be on the hook to payout for its $1.4 billion cyberattack claim, despite a “hostile/warlike action” exclusion in Merck’s all-risks property policies.

An avenue for escalation within the US court system remains, meaning the result may not be a foregone conclusion. Eight insurers are directly affected by the ruling, with many others attached to the suit having already settled; 26 policies were originally at issue. Nevertheless, the industry has been watching this appeal outcome carefully following what’s been seen as an anticlimactic end to food and beverage giant Mondelez and insurer Zurich’s $100 million NotPetya war exclusion case, which settled out of court last November.

Court's Merck NotPetya insurance appeal decision to "get the ball rolling".

The NJ appellate division said that the "exclusion of damages caused by hostile or warlike action by a government or sovereign power in times of war or peace requires the involvement of military action.

"The exclusion does not state the policy precluded coverage for damages arising out of a government action motivated by ill will."

Further, it said that "the plain language of the exclusion 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'."

It may prove a controversial decision for some insurers. The court's interpretation of a warlike or hostile act was lambasted as "wrong" and overly "traditional" by Kennedys partners Joshua Mooney and Judy Selby, who said in a January blog post prior to the appeal result: "The reasoning of this decision looks backward to a century past, and we believe it will not age well."

Prior to the court rulings, though, insurers have "routinely" covered NotPetya claims from companies facing smaller losses than Merck. That is according to Reed Smith partner Nick Insua, part of a team that supplied an Amici brief in the case on behalf of United Policyholders.

"The language at issue in Merck has been used by insurers in one form or another since the 1950s, and the appellate division's decision is consistent with the body of case law addressing similar exclusions," he told Insurance Business in the days following the appellate division's decision.

While the NJ affirmation "by no means establishes an underwriting guideline or an industry coverage position", it should "start to get the ball rolling" on more certainty for policyholders, Peter Hedberg, Corvus VP of cyber underwriting, said in a comment shared with Insurance Business.

The damaging potential of cyberattacks
NotPetya and predecessor worm ransomware WannaCry, which spread across 120 countries and was reportedly linked to North Korean hackers The Lazarus Group shortly thereafter, opened eyes to the potential reach and damaging impact of cyber bad actors.

Six years on, some insurers, spurred by concerns over systemic risk and soaring ransomware costs, have been taking action. Cyber insurance, which has started to see signs of stabilization, is becoming more targeted as carriers' risk appetite and understanding undergoes a shift.

Last August, Lloyd's looked to tighten language around state-backed or nation state attacks in standalone cyber policies, having already moved in 2020 to eliminate silent cyber from broader all-risks policies (such as the one at issue in NJ) through mandatory cyber exclusions or affirmative cover. While some brokers spoke out against the latest change, other cyber insurance stakeholders, like CFC head of cyber strategy James Burns, have said that the fresh wordings are only intended to "exclude attacks that are so catastrophic in nature that they destroy a nation's ability to function."

In a blog posted in April, defending the Lloyd's changes, Burns said that as the NotPetya attack was neither an attack on the US nor an attack that had a major detrimental impact on the country, "American companies, like Merck and Mondelez, should have had clear, unambiguous cover."

Instead, Burns said, the lay of the land meant that "broad traditional war exclusions in both standalone and package cyber policies mean customers are at the mercy of whatever their insurer decides."

Outside of the war issue, policies continue to be refined, with some cyber underwriters having drilled down further in a bid to combat systemic risk fears. For example, some might now take a dim view of covering a widespread operating system infection wherein the "bones that run" a computer system are down. There has also been greater stress on insureds' cybersecurity measures, and debates continue over whether there is need for federal cyber backstops or other means of boosting firms' cybersecurity.

The timing for adjustments could be critical: amid current geopolitical turbulence including Russia's Ukraine war, 93% of cyber leaders believe a "catastrophic" cyber event is likely in the next two years, the World Economic Forum's (WEF) Global Cybersecurity Outlook 2023 found.

A NotPetya type incident – many policies would pay out today

Despite changes, under the recent ruling, many current policies likely would still cover incidents like NotPetya even if insurers claimed they were not built with this in mind, and exclusions had been woven in. Others may have tighter language. It's a mixed landscape, and some carriers – domestic US insurers in particular – have been slower to "jump on board" with underwriting changes, according to Steve Robinson, RPS cyber practice leader.

Source: https://uphelp.org/mercks-1-4-billion-cyberattack-claim-the-specter-of-notpetya/ Date: April 25, 2024

“Cyber policies were not intended, nor are they designed to cover wide-scale physical war, or when cyber ops are a tactical element of such wide-scale physical war,” Robinson said. “The new exclusions are designed to bring more clarity to that intent. But, many carriers are citing NotPetya as a type of single incident that was not a part of a physical war directed at Merck, as a type of incident that would still be covered, even with the new exclusions.

“There are, of course, varying approaches, so this would not apply to all carriers.”

Those carriers that currently exclude “merely nation-state attribution” would likely be able to argue that any future NotPetya event could be excluded, according to Robinson.

“Ultimately, as cyber insurance matures, [insurers are] looking to provide good cover for … targeted, single attacks that can really be detrimental to an organization, while at the same time [the insurers] also want to be clear that neither cyber insurance policies nor any other types of policies were ever priced for appropriately to contemplate such a wide scale event where there wouldn’t be enough capital to support the business if something were to happen,” Robinson said.

Cybersecurity vulnerabilities – the “perfect storm” that could lead to a NotPetya repeat
It does not have to take long for an organization to feel the force of a cyber incident. On that fateful June day in 2017, 10,000 machines in Merck’s global network were infected with NotPetya within 90 seconds. Within five minutes, this had doubled to 20,000. Ultimately, more than 40,000 machines were brought down.

More than half a decade on, vulnerabilities in many businesses’ systems persist, even as insurers push for tighter security. RPS has continued to witness claims come in from large organizations, some of which have not had segmented backups needed to restore systems, resulting in some seeing a costly ransom payment as the “only option”. Ransomware frequency, meanwhile, has been back on the up in the last couple of months, though organizations’ propensity to pay attackers has dropped.

All that could be sitting between the world and a NotPetya repeat is “the perfect storm” of a software provider without proper security controls in place that unwittingly passes on malware to similarly unwitting customers, Robinson said.

The best offense may be a good defense, but even as cyber fortifications evolve, so too do malignant

technologies develop. Like cyber-hygiene-conscious insureds plugging security gaps, carriers may well be left patching up policy language vulnerabilities and errors for some time to come. In the interim, whatever twists the courts may churn up and whatever bad actors may throw insureds' and insurers' way, it falls to agents and brokers to explain just what the patchwork quilt of cyber policies means for clients, to keep on top of exclusion advancements, and to advocate for and fulfill their clients' insurance needs to the best of their ability.