Mondelez and Zurich reach settlement in NotPetya cyberattack insurance suit

therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit/

October 31, 2022

Image: Colin Lloyd

Mondelez International and Zurich American Insurance reached a settlement late last week in their multi-year legal battle over the food company's $100 million claim regarding damage from the NotPetya cyberattack in 2017.

The insurer had initially refused to cover the damage to Mondelez, which in court documents attested it lost more than 1,700 servers and 24,000 laptops to the malware. Details of the final settlement have not been disclosed.

NotPetya was a destructive attack which masqueraded as ransomware, and reportedly caused more than $10 billion in global damages. While it encrypted its victims' machines and left a demand for a ransom payment, it was not actually designed to be decrypted.

The malware used an exploit which allowed the virus to spread automatically through trusted networks. It had first been introduced into a popular Ukrainian accounting company's software but quickly spread beyond Ukraine to hit numerous other countries and companies, including Mondelez and Merck.

Mondelez, the multinational corporation behind Oreos, Ritz crackers, and dozens of other snack food brands, did not respond to The Record for comment. A spokesperson for Zurich Insurance said they could only provide a short statement in response: "The parties have

mutually resolved the matter."

The case between the two was complex because Mondelez had not taken out an explicit cyber insurance policy but a property policy that it argued covered cyberattacks.

Zurich claimed in response that the damage caused by NotPetya was excluded from this policy on the grounds it was a "hostile or warlike action" conducted by a "government or sovereign power."

The settlement will "fuel growth for the cyber insurance market," according to Billy Gouveia, the chief executive of incident response business Surefire Cyber.

"As cyber risk remains a top concern for businesses, it is important for organizations to prepare and protect themselves on all fronts," he told The Record, referencing a range of preparations from incident response planning through to insurance.

Craig Dunn, the head of Cyber M&A Insurance EMEA for Aon, told The Record he didn't think the settlement was "much of a surprise."

"In short, the policy was not a cyberinsurance policy — it was a property policy that provided some cover for cyber events — and Zurich was in a bit of hot water while Mondelez felt like they were in a fairly strong position."

Dunn, who previously led Hiscox Europe's cyberinsurance business, explained that NotPetya left the whole market feeling the war exclusions included in most policies were not fit for purpose. Lloyds of London recently led an effort to revamp these exclusions and find some kind of solution that balanced the needs of the customers and the insurance market.

The exercise involved different insurers and brokers who ultimately came up with four different exclusions that can be used to reject claims for state-based attacks in different ways.

"Despite the negative press that Lloyds of London got for some of the exclusions they've come up with, the vast majority of insurers are adopting variants where the intention is to only exclude nation state attacks that form part of an armed conflict or impact the underlying functioning of a state. In short, the intention is generally not to exclude something like North Korea hacking Sony back in 2014," said Dunn.

While one of the exclusions would not cover incidents like the Sony hack, Dunn said "most insurers realize this does not meet their clients' needs and are happy to provide cover for events that impact individual companies. This important detail was missed by previous reporting."

Act of War?

The settlement follows earlier this year a New Jersey court ruling in favor of Merck, which had sued its insurer, Ace American, for refusing to cover the damages it suffered because of NotPetya.

In that case, the court dismissed Ace Americans' defense that the attack was an "Act of War" and therefore excluded by the insurance contract. Merck's lawyers successfully argued that "Acts of War" as defined in the contract referred exclusively to "official state actions," which the NotPetya attack did not count as.

The United States and United Kingdom have attributed the NotPetya malware to the Russian Federation, with the National Cyber Security Centre finding the Russian military was "almost certainly responsible" — the highest confidence rating the intelligence agency gives. The Kremlin has repeatedly denied it orchestrated the attack.

NotPetya highlighted the risks that a catastrophic cyberattack could pose for the insurance industry, which could find itself without the capital to support claims.

"There are a lot of concerns about aggregation of risk. Unlike in property insurance where insurers can diversify risk by simply ensuring they don't insure too many homes or businesses in one geographical region – the same cannot be said of cyber," explained Dunn.

Part of the problem is a lack of diversity within the technology sector, with so many businesses using Windows and relying on cloud services provided by a limited number of vendors, Dunn said, "meaning risk can't be diversified based on geographical location, so insurers must be careful not to take on too much risk."

The four different exclusions which Lloyds had come up with included the concept of an impact state, where the only losses excluded will be those that are incurred within a war zone or within the state where the critical national infrastructure has been severely damaged. "Losses suffered in other countries, where critical national infrastructure (CNI) remains operational and where no state of war exists, would be covered," explained Dunn.

"For instance, if a company operating both inside and outside of Ukraine is attacked today by the Russians and they happened to have this version of the war exclusion in their cyber insurance policy, then any losses incurred as a result of their IT infrastructure being taken out inside of Ukraine, which is in a state of war and as such is an 'impacted state,' would be excluded," he said. "However, if their operations in the U.S. or U.K. are also impacted, any losses stemming from this would be covered, since the U.S. and U.K. are outside of the war zone and have not suffered attacks against their CNI."

Tags

- Cyber insurance
- cybercrime

- Mondelez
- NotPetya
- Russia
- Zurich

Alexander Martin is the UK Editor for The Record. He was previously a technology reporter for Sky News and is also a fellow at the European Cyber Conflict Research Initiative.