(NYT) Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.

Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.
2019-04-16 13:32:49.256 GMT

By Adam Satariano and Nicole Perlroth

(New York Times) -- LONDON — Within days of a cyberattack, warehouses of the snack foods company Mondelez International filled with a backlog of Oreo cookies and Ritz crackers.

Mondelez, owner of dozens of well-known food brands like Cadbury chocolate and Philadelphia cream cheese, was one of the hundreds of companies struck by the so-called NotPetya cyberstrike in 2017. Laptops froze suddenly as Mondelez employees worked at their desks. Email was unavailable, as was access to files on the corporate network. Logistics software that orchestrates deliveries and tracks invoices crashed.

Even with teams working around the clock, it was weeks before Mondelez recovered. Once the lost orders were tallied and the computer equipment was replaced, its financial hit was more than $100 million, according to court documents.

After the ordeal, executives at the company took some solace in knowing that insurance would help cover the costs. Or so they thought.

Mondelez's insurer, Zurich Insurance, said it would not be sending a reimbursement check. It cited a common, but rarely used, clause in insurance contracts: the "war exclusion," which protects insurers from being saddled with costs related to damage from war.

Mondelez was deemed collateral damage in a cyberwar.

The 2017 attack was a watershed moment for the insurance industry. Since then, insurers have been applying the war exemption to avoid claims related to digital attacks. In addition to Mondelez, the pharmaceutical giant Merck said insurers had denied claims after the NotPetya attack hit its sales research, sales and manufacturing operations, causing nearly $700 million in damage.

When the United States government assigned responsibility for NotPetya to Russia in 2018, insurers were provided with a justification for refusing to cover the damage. Just as they wouldn't be liable if a bomb blew up a

corporate building during an armed conflict, they claim not to be responsible when a state-backed hack strikes a computer network.

The disputes are playing out in court. In a closely watched legal battle, Mondelez sued Zurich Insurance last year for a breach of contract in an Illinois court, and Merck filed a similar suit in New Jersey in August. Merck sued more than 20 insurers that rejected claims related to the NotPetya attack, including several that cited the war exemption. The two cases could take years to resolve.

The legal fights will set a precedent about who pays when businesses are hit by a cyberattack blamed on a foreign government. The cases have broader implications for government officials, who have increasingly taken a bolder approach to naming-and-shaming state sponsors of cyberattacks, but now risk becoming enmeshed in corporate disputes by giving insurance companies a rationale to deny claims.

“You’re running a huge risk that cyberinsurance in the future will be worthless,” said Ariel Levite, a senior fellow at the Carnegie Endowment for International Peace, who has written about the case. But he said the insurance industry’s position on NotPetya is “not entirely frivolous, because it is widely believed that the Russians had been behind the attack.”

Mondelez said in a statement that while its business had recovered quickly from the attack, Zurich Insurance was responsible for honoring an insurance policy that explicitly covers cyber events. The company added that it did not believe the war exemption clause fit the circumstances.

Zurich Insurance, based in Switzerland, and Merck declined to comment because of the active litigation. But court documents, public filings and interviews with people familiar with cases provided details about the disputes.

Cyberattacks have created a unique challenge for insurers. Traditional practices, like not covering multiple buildings in the same neighborhood to avoid the risk of, say, a big fire don’t apply. Malware moves fast and unpredictably, leaving an expensive trail of collateral damage.

“It cuts across practically every type of business activity,” Mr. Levite said. The risk, he said, “no longer can be contained in this interconnected world.”

NotPetya — which picked up the odd name because security researchers initially confused it with a piece of so-called ransomware called Petya — was a vivid example. It was also a powerful assault on computer networks that incorporated a stolen National Security Agency cyberweapon.

American officials tied the attack to Russia and its conflict with Ukraine. The original target was a Ukrainian tax software maker and its Ukrainian customers. In just 24 hours, NotPetya wiped clean 10 percent of all computers in Ukraine, paralyzing networks at banks, gas stations, hospitals, airports, power companies and nearly every government agency, and shutting down the radiation monitors at the old Chernobyl nuclear power plant.

The attack made its way to the software maker's global clients, eventually entangling Mondelez and Merck, as well as the Danish shipping conglomerate Maersk and FedEx's European subsidiary. It hit even Russia's state-owned oil giant, Rosneft.

In a statement in 2018, the White House described NotPetya as "part of the Kremlin's ongoing effort to destabilize Ukraine" and said it had demonstrated "ever more clearly Russia's involvement in the ongoing conflict."

Many insurance companies sell cyber coverage, but the policies are often written narrowly to cover costs related to the loss of customer data, such as helping a company provide credit checks or cover legal bills.

Mondelez, a former unit of Kraft Foods, argues that its property insurance package should cover the losses from the NotPetya attack. In court filings, Mondelez said its policy had been updated in 2016 to include losses caused by "the malicious introduction of a machine code or instruction."

The company lost 1,700 servers and 24,000 laptops. Employees were left to communicate through WhatsApp, and executives posted updates on Yammer, a social network used by companies.

Damage from NotPetya spread all the way to Hobart, Tasmania, where computers in a Cadbury factory displayed so-called ransomware messages that demanded $300 in Bitcoin.

Courts often rule against insurers that try to apply the wartime exemption. After hijackers destroyed a Pan Am airliner in 1970, a United States court rejected Aetna's attempt, determining that the action was criminal, not an act of war. In 1983, a judge ruled that Holiday Inn's insurance policy covered damage from the civil war in Lebanon.

In the Mondelez and Merck lawsuits, the central question is whether the government's attribution of the NotPetya attack to Russia meets the bar for the war exclusion.

Risk industry experts say cyberwar is still largely undefined. Attribution can be difficult when attacks come from groups with unofficial links to a state and the blamed government denies involvement.

“We still don’t have a clear idea of what cyberwar actually looks like,” said Jake Olcott, vice president at BitSight Technologies, a cyber risk adviser. “That is one of the struggles in this case. No one has said this was an all-out cyberwar by Russia.”

In the past, American officials were reluctant to qualify cyberattacks as cyberwar, fearing the term could provoke an escalation. President Barack Obama, for example, was careful to say the aggressive North Korean cyberattack on Sony Entertainment in 2014, which destroyed more than 70 percent of Sony’s computer servers, was an act of “cybervandalism.”

That label was sharply criticized by Senators John McCain and Lindsey Graham, who called the hack a “new form of warfare” and “terrorism.”

The description of the Sony attack was deliberate, said John Carlin, the assistant attorney general at the Justice Department at the time. In an interview, he said the Obama administration had worried, in part, that the use of “cyberwar” would have triggered the liability exclusions and fine print that Mondelez is now challenging in court.

Scott Kannry, the chief executive of the risk assessment firm Axio Global, said the insurance industry was watching the Mondelez case closely because many policies were created before cyberattacks were such an urgent risk.

“You have insurers who are sitting on insurance policies that were never underwritten or understood to cover cyber risk,” Mr. Kannry said. “Zurich didn’t underwrite the policy with the idea that a cyber event would cause the kind of losses that happened to Mondelez. Nobody is at war with Mondelez.”

Many insurance companies are rethinking their coverage. Since the lawsuits were filed, Shannan Fort, who specializes in cyberinsurance for Aon, one of the world’s largest insurance brokers, has been fielding calls from companies scrambling to be sure they’ll be safe if attacked, she said.

“I don’t want to scare people, but if a country or nation state attacks a very specific segment, like national infrastructure, is that cyberterrorism or is that an act of war?” Ms. Fort asked. “There is still a bit of gray area.”

Ty Sagalow, a former chief operating officer at the insurance giant A.I.G., helped pioneer the market for cyber risk insurance nearly two decades ago. He

said his team had contemplated a “Cyber Pearl Harbor” attack not unlike the NotPetya attack.

“Cyberwar and cyberterrorism has always been a tricky area,” Mr. Sagalow said. Insurers risk abusing the war exclusion by not paying claims, he said, particularly when an attack “can hit companies that were not the original target of violence.”

Collateral damage from attacks that get out of control are going to become more and more common, he added. “That is what cyber is today,” Mr. Sagalow said. “And if you don’t like it, you shouldn’t be in the business.”

Follow Adam Satariano and Nicole Perlroth on Twitter: @satariano and @nicoleperlroth. Adam Satariano reported from London, and Nicole Perlroth from San Francisco.

Click Here to see the story as it appeared on the New York Times website.

-0- Apr/16/2019 13:32 GMT