

Could NotPetya's Tail Be Growing?

Cyber catastrophe risk has been difficult to understand and analyze. New capacity providers, feeling like they're flying blind when it comes to catastrophe in cyber, have been reluctant to allocate to the sector. They might be interested in writing cyber, but not as long as their positions are exposed to cyber catastrophe risk.

This is particularly true for insurance-linked securities (ILS) funds. For them, part of the challenge of entering cyber (re)insurance has been understanding what a cyber catastrophe could look like, given that there hasn't been much history to evaluate. There's been a belief that cyber catastrophes would have long tails, particularly as a result of professional lines claims that could take years to sort out. This, in addition to the general risk of interrelated losses hitting a balance sheet at the same time, has made it hard for capacity providers to allocate to cyber, which in turn has constrained the sector's growth.

Initially, it looked like NotPetya would be a somewhat benign cyber catastrophe, leading the market to question the prevailing wisdom about long-tail risks from professional lines (such as D&O). However, the event has evolved, which provides more learning opportunity from the first PCS®-designated global cyber catastrophe.

Lesson 1: It's tough to predict exploding cyber cats

Careful analysis would normally be the solution to this problem, but the cyber (re)insurance sector is short of fodder for that sort of effort. The PCS team looked at the economic losses from major cyber events over the past 20 years, with a dozen of them reaching at least US\$500 million. While every major event comes with lessons for risk bearers, fast-changing circumstances compounded by time can erode the benefits of learning from the past and hamper capital deployment.

Historical Cyber Events: Economic Losses

Event	Year	Economic Impact
Melissa	1999	US\$1.2 billion
ILOVEYOU	2000	US\$15 billion
Code Red	2001	US\$2 billion
Sircam	2001	US\$1 billion
Nimda	2001	US\$635 million
Sobig	2003	US\$37 billion
SQL Slammer	2003	US\$750 million
Mydoom	2004	US\$38 billion
Sasser	2004	US\$500 million
Conficker	2007	US\$9.1 billion
WannaCry	2017	US\$4 billion
NotPetya	2017	US\$10 billion

Source: PCS internal research

Only two of the above cyber catastrophes resulted in directly meaningful losses for the global insurance industry: WannaCry and NotPetya. WannaCry caused significant economic losses, but the impact on the insurance industry amounted to only US\$50–60 million. Of course, NotPetya had insured losses of above US\$3 billion—and the event is still developing. Another, LockerGoga, seemed poised to cause nontrivial insured losses industrywide. Following the Norsk Hydro affirmative cyber loss, though, it looked like momentum slowed a bit, with the five other companies being monitored appearing to have economic exposure but little in the way of insurance implication. (We continue to monitor LockerGoga for insurance industry developments.)

Lesson 2: It's about much more than the cat's tail

So, what makes WannaCry and NotPetya different from each other? Some believe that WannaCry's economic impact was actually greater than that of NotPetya's, despite the imbalance in insurance industry implications.

NotPetya appears to have affected larger companies in a way that resulted in greater engagement with the insurance industry, given the business interruption implications that were relevant to property programs. That wasn't the only reason for the much larger loss reported for NotPetya. Two major risk losses contributed more than 80 percent of the event's insured loss of above US\$3 billion. Without them, the overall insured loss—not to mention the economic loss—would've been much more modest, with the impact on the global insurance industry commensurate with that of a particularly nasty single-state hailstorm.

The dearth of precedent has caused the global (re)insurance industry to examine NotPetya with particular care, combing it for every possible insight that could be used for analysis and prediction. Before this event, the global (re)insurance industry was fixated on the effect that a cyber attack could have on the professional lines market, but the property losses from NotPetya shifted our community's focus. However, it's worth revisiting the potential concerns associated with professional lines claims from a cyber event. It looks like this issue is about to become relevant to the market.

In past years, market players on the sidelines of the cyber sector would worry that a directors and officers (D&O) claim represented the nightmare scenario. D&O claims can drag on for years, and even successful claims handling can be an expensive and burdensome proposition. Now, think about what that means for a D&O claim resulting from a cyberattack. All the challenges that exist for professional lines claims on a good day are brought to bear on a "silent cyber" case—the sort of cause that may not have been contemplated by the original cover. This is the kind of difficulty that's kept some capacity providers out of the market—particularly collateralized markets that worry about the risk of a cash drag during a drawn-out claim-handling process.

For the first two years of its development, NotPetya remained mostly a property event. Approximately 85 percent of the insured loss from the event was non-affirmative property. Although there have been some questions and concerns along the way, NotPetya became fairly stable faster than anyone expected for a cyber catastrophe. That's not to say the industry loss was approaching finality; there are always disputes in catastrophe events. But the process was fairly smooth.

Now, that could change.

Lesson 3: D&O finally comes to bear?

According to [*The D&O Diary*](#), a shareholder class action lawsuit has arisen from the impact of NotPetya on FedEx subsidiary TNT Express. PCS Global Cyber™ has watched the economic impact informally and identified an economic impact in the bulletins we provide to our subscribers. The potential effect on the industry insured loss estimate is not trivial—likewise the duration of the post-event development.

The anecdotal collection of economic losses from PCS-designated cyber catastrophe events provides some sense of what's in play here. We found an economic impact of approximately US\$1 billion for FedEx from the NotPetya attack, up from an initial disclosure of US\$300 million. Whether this is the total at risk from the events discussed in *The D&O Diary* remains to be seen as the case unfolds. But the revealed economic impact so far provides a starting point for analysis. If this economic impact were to become an insured loss, it would result in an increase of more than 30 percent to the overall industry insured loss from NotPetya. Also, it would provide another dimension for analysis because cyber (re)insurance underwriters would be able to segment affirmative cyber, non-affirmative cyber losses to property, and non-affirmative cyber losses from professional lines.


The segmentation across classes of business could also turn the practical lessons of NotPetya into near-term risk-transfer flexibility. Cedents and capacity providers could use more granular triggers to shorten the tail and home in on specific risks that they want to trade in, rather than take an “all or nothing” approach to the tail. For example, an instrument could include affirmative cyber and non-affirmative cyber excluding D&O and E&O claims. In NotPetya, it took two years for the D&O claim to arise, while the property and affirmative cyber losses were fairly stable by then.

Cyber catastrophe remains a new and little-understood line of business, but lessons come every day. Of course, the only true source of experience is participation in the market. And where there's original risk to be covered, there's an opportunity for profitable growth.

Contact PCS

For more information, please contact:

 **Tom Johansmeyer** | Co-head, PCS

 **Office:** +1 201 469 3140 | **Mobile:** +1 201 377 8429

 tjohansmeyer@verisk.com

 [in/tjohansmeyer](https://www.linkedin.com/in/tjohansmeyer)

 [@tjohansmeyer](https://twitter.com/tjohansmeyer)

