

PCS Global Cyber™: An Overview of Our Global Loss Index Suite

While the cyber (re)insurance market is still small, market expectations are high—and seem to be increasing every day. For cyber to become “the next Florida wind” for the reinsurance market, though, some structural changes must occur. Among them is the entry of capital markets capacity to provide both reinsurance and retrocessional protection for companies assuming cyber insurance risk. As is the case in the property-catastrophe market, the use of industry loss warranties (ILWs)—and eventually index-triggered catastrophe bonds—can help drive collateralized capacity into the cyber sector, creating more opportunity for industry growth.

The most significant barrier to capacity entering the market is the lack of industrywide data. And it’s challenging to get relevant data when the industry is small. Take the Target, Home Depot, and Anthem losses from several years ago. Cover for each was exhausted well before the final economic losses were determined. As a result, it’s difficult for the (re)insurance industry to learn from those events. With higher limits, the texture of each loss becomes more evident, providing greater insight to enable a company to write larger lines, allocate more capacity to the space, and ultimately manage risk and capital in a more sophisticated manner.

The cyber (re)insurance sector needs to grow—after all, original insureds’ exposures are growing rapidly. For the industry to live up to its social mission and support the public good, cyber cover needs to become larger, more relevant, and more pervasive. The upshot of this is the potential for greater profitability and the creation of shareholder value in a market that craves diversification from peak-peril property-catastrophe risk.

PCS Global Cyber™ provides the data assets the global (re)insurance industry needs to understand loss events around the world, analyze exposures, make pricing decisions, and improve risk and capital management. PCS Global Cyber includes solutions for both affirmative cyber risk losses and cyber catastrophe events that include impacts to both cyber and non-cyber insurance programs.

Background on PCS and specialty

Since 1949, the property/casualty insurance industry has relied on catastrophe loss estimates from PCS® and its predecessor organizations to set catastrophe reserves and optimize the deployment of adjusters. Our mission has grown to include reinsurance, insurance-linked securities (ILS), and other forms of risk transfer. For more than 20 years, PCS has been a trusted source of North American natural catastrophe data for the ILS market.

In 2017, PCS expanded its mission beyond the property-catastrophe sector, growing into global specialty lines.

PCS Global Marine and Energy™ marked our first initiative in this category, providing industry loss estimates on large nonelemental risk losses for use in a wide range of

internal functions as well as reinsurance and alternative risk transfer, such as ILWs. The database has loss estimates for 24 events of at least US\$250 million around the world, including Costa Concordia, Gryphon Alpha, Deepwater Horizon, and Jubilee/Kwame.

PCS Global Terror™ provides an industrywide view of terror events around the world, including both physical damage and business interruption. Users can find information on industry loss events of at least US\$25 million worldwide going back to 1992, including the “7/7” event in London, Barajas/Madrid, and the three events in the United States.

PCS Global Cyber helps risk bearers improve their understanding of the insured losses that can result from a covered (affirmative) cyber event. Further, when used as an industry loss index trigger, PCS Global Cyber can support the entry of more capacity into the cyber (re)insurance market. The solution has estimates on 13 affirmative cyber risk losses of at least US\$20 million going back to 2013 as well as Petya/NotPetya, the first cyber catastrophe loss event in PCS Global Cyber, where the threshold for both affirmative and silent cyber losses is a combined US\$250 million.

Everything You Need to Know about the PCS Global Cyber Index Suite

PCS affirmative cyber risk loss aggregation: How it works

The PCS team will regularly monitor news reports and other publicly available data sources to ascertain when a particular loss event should be investigated. Additionally, PCS will regularly reach out to participating insurers, reinsurers, and intermediaries for their feedback on loss events that might not reach the public domain. When, through either channel, PCS believes an individual loss has occurred that will cause an insurance industry loss of at least US\$20 million, PCS will designate it a “PCS Cyber Risk Loss Event” and initiate loss aggregation and estimation procedures.

Event designation: PCS will publish a bulletin through the ISONet® PCS platform indicating that a PCS Cyber Risk Loss Event has occurred, generally within 48 hours of identification through publicly available data sources or through companies participating in PCS cyber data contribution. This bulletin will be available to all registered users that have opted for access to the cyber platform.

Initial data call: PCS will engage participating insurers and reinsurers to provide an initial view of the loss event.

This should include:

- date the event occurred (to the extent possible)
- date the event was discovered (to the extent possible)
- date of public announcement of the event
- heads of cover affected by the event
- (re)insurer’s share of the loss
- (re)insurer’s projected ultimate loss
- (re)insurer’s view of the projected industry loss

PCS will then synthesize the loss data and market shares from (re)insurers to arrive at an industry loss estimate for the insurance industry. Throughout this process, the PCS operations team may engage participating (re)insurers for more information and context regarding the loss information they provide.

Initial PCS cyber risk loss estimate: Since it can take time for large cyber risk losses to develop, PCS will plan to publish its first PCS Cyber Risk Loss Event estimate four weeks after announcing the designation of the event. Every event designated will be subject to a resurvey process, meaning that the first estimate will never be the last.

Subsequent data calls: Until PCS has arrived at a final industry loss estimate, PCS will engage participating (re)insurers quarterly to refresh the information provided in the first data call.

Subsequent resurvey estimates: PCS will revisit all open PCS Cyber Risk Loss Events every quarter until the team believes it has arrived at a stable estimate that it can call final. The data requested by PCS does not change, although the estimate is generally expected to develop based on the nature of the information that becomes available throughout the claim life cycle. PCS will publish resurveys quarterly for open events, even if there's no change to the underlying data.

PCS Global Cyber Index

Final estimate: When the PCS operations team believes it has arrived at a stable estimate, it will declare a final estimate.

For this to occur:

- The estimate and most underlying data must not have changed for two consecutive quarters.
- It must be confirmed that there are no outstanding issues that could significantly change the estimate (such as outstanding class action litigation).
- Most data participation companies agree that the loss estimate is unlikely to change materially.

Throughout this process, PCS strives to balance speed and accuracy. With this in mind, the organization would accept an early conclusion that may not capture smaller, later changes to an estimate to get a final number to market to facilitate streamlined risk-transfer transactions for the cyber insurance market as a whole.

Post-event activity: Following the closure of an event, the PCS operations team will review its tracking spreadsheet of individuals involved in creating the PCS Cyber Risk Loss Event estimate and provide post-event document destruction instructions, in accordance with existing PCS policy. Verisk Analytics internal audit will then verify that all relevant documents have been destroyed in accordance with company policy. All that will remain of the loss estimation will be the industrywide data contained in each of the bulletins—although PCS will maintain a list of companies it should call for data contribution throughout the loss aggregation process. That said, no other information from a participating company will be retained.

What it will look like: The bulletins published for each PCS Cyber Risk Loss Event will include:

- date the event occurred (to the extent possible)
- date the event was discovered (to the extent possible)
- date of public announcement of the event
- heads of cover affected by the event
- insurance industry loss estimate
- economic loss estimate (to the extent available)
- narrative explaining the nature of the event based on information from publicly available sources and insights from participating (re)insurers

The preliminary bulletin, indicating the designation of a PCS Cyber Risk Loss Event, will not include industry or economic loss information. The final bulletin will be labeled “Final,” as is the case with current PCS procedure.

PCS cyber catastrophe loss aggregation: How it works

The PCS team will regularly monitor news reports and other publicly available data sources to ascertain when a particular industrywide cyber event should be investigated, based on our event definition and methodology. Additionally, PCS will regularly reach out to participating insurers, reinsurers, and intermediaries for their feedback on events that might not reach the public domain. When, through either channel, PCS believes an individual loss has occurred that will cause an insurance industry loss of at least US\$250 million, PCS will designate it a “PCS Cyber Catastrophe Loss Event” and initiate loss aggregation and estimation procedures.

Event designation: PCS will publish a bulletin through the ISOnet PCS platform indicating that a PCS Cyber Catastrophe Loss Event has occurred, generally within 48 hours of identification through publicly available data sources or through companies participating in PCS cyber data contribution. This bulletin will be available to all registered users that have opted for access to the cyber platform.

Initial data call: PCS will engage participating insurers and reinsurers to provide an initial view of the loss event.

This should include:

- event dates (to the extent possible)
- heads of cover affected by the event, as well as lines of business outside affirmative cyber
- (re)insurer’s understanding of underlying companies affected, as well as projected ultimate loss for each insured (for large losses)
- (re)insurer’s view of other, smaller losses from the event (such as small-business cyber and kidnap and ransom)
- (re)insurer’s view of the projected industry loss for the event as a whole

PCS will then synthesize the loss data and other information from (re)insurers to arrive at an industry loss estimate for the insurance industry. Throughout this process, the PCS operations team may engage participating (re)insurers for more information and context regarding the loss information they provide.

Initial PCS cyber catastrophe loss estimate: Since it can take time for large losses from cyber events to develop, PCS will plan to publish its first PCS Cyber Catastrophe Loss Event estimate four weeks after announcing the designation of the event. Every event designated will be subject to a resurvey process, meaning that the first estimate will never be the last.

Subsequent data calls: Until PCS has arrived at a final industry loss estimate, PCS will engage participating (re)insurers quarterly to refresh the information provided in the first data call.

Subsequent resurvey estimates: PCS will revisit all open PCS Cyber Catastrophe Loss Events every quarter until the team believes it has arrived at a stable estimate that it can call final. The data requested by PCS does not change, although the estimate is generally expected to develop based on the nature of the information that becomes available throughout the claim life cycle. PCS will publish resurveys quarterly for open events, even if there's no change to the underlying data.

Final estimate: When the PCS operations team believes it has arrived at a stable estimate, it will declare a final estimate.

For this to occur:

- The estimate and most underlying data must not have changed for two consecutive quarters.
- It must be confirmed that there are no outstanding issues that could significantly change the overall estimate and underlying loss estimates (such as outstanding class action litigation).
- Most data participation companies agree that the loss estimate is unlikely to change materially.

Throughout this process, PCS strives to balance speed and accuracy. With this in mind, the organization would accept an early conclusion that may not capture smaller, later changes to an estimate to get a final number to market to facilitate streamlined risk-transfer transactions for the cyber insurance market as a whole.

Post-event activity: Following the closure of an event, the PCS operations team will review its tracking spreadsheet of individuals involved in creating the PCS Cyber Catastrophe Loss Event estimate and provide post-event document destruction instructions, in accordance with existing PCS policy. Verisk Analytics internal audit will then verify that all relevant documents have been destroyed in accordance with company policy. All that will remain of the loss estimation will be the industrywide data contained in each of the bulletins—although PCS will maintain a list of companies it should call for data contribution throughout the loss aggregation process. That said, no other information from a participating company will be retained.

What it will look like: The bulletins published for each PCS Cyber Catastrophe Loss Event will include:

- event dates (to the extent possible)
- heads of cover affected by the event, as well as lines of business outside affirmative cyber
- industrywide affirmative cyber loss estimate
- industrywide silent cyber loss estimate
- narrative explaining the nature of the event based on information from publicly available sources and insights from participating (re)insurers

The preliminary bulletin, indicating the designation of a PCS Cyber Catastrophe Loss Event, will not include industry or economic loss information. The final bulletin will be labeled “Final,” as is the case with current PCS procedure.

Appendix A: Historical loss aggregation

To launch the PCS Global Cyber loss aggregation program, PCS developed a historical loss database for events that meet the criteria described above (going back to 2013):

- Southwest
- Sony
- Home Depot
- Target
- Anthem
- Premera

Realizing that this list of losses is a starting point, PCS welcomes the reporting of additional events not listed above that meet the PCS criteria for large risk losses. Some high-profile events, such as the Delta and British Airways outages of 2017, are excluded because recoveries are being attempted through policies outside cyber (such as property and general liability). Other events—like WannaCry, Dyn, and Amazon Web Services—had low levels of insured loss as a result of waiting periods.

Appendix B: About PCS

ISO is a Delaware stock corporation organized on September 25, 1997. On October 1, 1997, ISO purchased the assets of American Insurance Services Group, Inc. (AISG), which was a not-for-profit Delaware corporation providing services to the property/casualty insurance industry since 1984. PCS, formerly a division of AISG, is a division of ISO. ISO is a wholly owned subsidiary of Insurance Services Office, Inc., a for-profit Delaware stock corporation that is the leading provider of information about property/casualty insurance, including statistical information, actuarial analyses, standardized policy language, and a variety of insurance rating and underwriting services. In October 2009, Insurance Services Office, Inc., became a wholly owned subsidiary of Verisk Analytics, Inc. (Verisk). Verisk completed its initial public offering on October 7, 2009, and is now publicly traded on the Nasdaq Stock Market under the ticker symbol VRSK.

PCS performs a variety of services of interest to the property/casualty industry, principally relating to catastrophes affecting the industry. PCS services include weather monitoring, catastrophe identification, monitoring judicial decisions relating to property insurance issues, and monitoring proposed and actual regulations relating to property claims

handling. PCS provides a series of bulletins, monthly previews, reports, and news to its subscribers concerning the foregoing information and other issues of interest to the property/casualty industry.

From its inception in 1965 and continuing under the auspices of ISO, PCS has maintained a program under which it designates, and numbers sequentially as catastrophes, various natural or man-made events and prepares estimates of total insured property damage believed to have been caused by each such event. A similar program was carried out by predecessor organizations (the National Board of Fire Underwriters and American Insurance Association) from 1949 until the establishment of AISG. In 2010, PCS launched the PCS Canada® service for the dissemination of estimates and other catastrophe information pertaining to Canada. In 2015, PCS launched the PCS Turkey™ service for the dissemination of estimates and other catastrophe information pertaining to the Republic of Turkey. In 2017, PCS launched the PCS Global Marine and Energy service for the dissemination of estimates and other information pertaining to man-made, noncatastrophic loss events relating to the offshore energy and ocean marine sectors.

Appendix C: PCS Global Cyber catastrophe event definition


PCS designates a global **cyber catastrophe** event when it expects an industry-wide, estimated insured loss of at least US\$250 million from an unauthorized or malicious act or a series of related unauthorized or malicious acts or other accidental or unintended consequences involving a computer system that is covered by insurance and results in insured loss based on the sole judgment of PCS. Such event would be regardless of time and place, or the threat or hoax thereof and would have a direct affect prompted from access, processing, use or operation of any computer system or any data by any person or group(s) of persons. Any such act/acts must be connected by a common source, cause, scenario, or mechanism—and must affect more than one insurer and more than one insured.


Such events may include (for the purposes of illustration):

- Cyber Extortion
- Cyber Terror/State-Sponsored
- Data – Malicious Breach
- Data – Physically Lost or Stolen
- Data – Unintentional Disclosure
- Denial of Service (DDOS)/ System Disruption
- Digital Asset Loss or Theft
- Digital Breach/Identity Theft
- Digital Data Breach, Loss, or Theft
- Identity – Fraudulent Use/ Account Access
- Identity Theft/Fraudulent Use or Access
- Industrial Controls and Operations
- Improper Disposal/Distribution, Loss, or Theft (Printed Records)
- IT – Configuration/Implementation Errors
- IT – Processing Errors
- Network/Website Disruption
- Phishing, Skimming
- Spoofing, Social Engineering
- Privacy – Unauthorized Contact or Disclosure
- Privacy – Unauthorized Data Collection
- Physical Tampering
- System/Network Security Violation or Disruption
- Other – as determined by PCS team

Contact PCS

For more information about PCS Global Cyber, please contact:

 **Tom Johansmeyer**
Assistant Vice President –
PCS Strategy and Development


 **Phone:** +1 201 469 3140
Mobile: +1 201 377 8429

 tjohansmeyer@verisk.com

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

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

 **Ted Gregory**
Director, PCS

 **Phone:** +1 201 469 3144

 tgregory@verisk.com

 [teddie-gregory](https://www.linkedin.com/in/teddie-gregory)



© 2018 Insurance Services Office, Inc. Verisk Analytics, the Verisk Analytics logo, ISO, and ISOnet are registered trademarks and Verisk and the Verisk logo are trademarks of Insurance Services Office, Inc. PCS, Property Claim Services, and PCS Canada are registered trademarks and PCS Turkey, PCS Global Cyber, PCS Global Marine and Energy, and PCS Global Terror are trademarks of ISO Services, Inc. All other product or corporate names are trademarks or registered trademarks of their respective companies.
ca18087 (8/18)