Catastrophic Cyber Risks

External FAQs

beazley

Contents

1. What changes are being made to address Catastrophic Risk in Beazley policies?

We have introduced three new endorsements that specifically address the scope of exposure around catastrophic cyber whilst maintaining coverage for systemic events. The updated wordings cover the scope of exposure and details of the three new endorsements are listed below. Please refer to question *"2. What policies are affected?"* for further details about where these endorsements will be added to policies and when.

A. The war and cyber war exclusion replaces the war and civil war exclusion.

Our new definitions of **war** and **cyber war provide clarity for clients by directly** addressing **when potential threats from** computer systems, used in modern state conflict are excluded. **War** is defined as the use of physical force, and **cyber war** is defined as the use of negative digital force on an enemy state that negatively impacts their computer systems. The clarification and simplification of the meaning provides clarity for both brokers and clients alike. There is a carve back to **cyber war** exclusionary language, which applies to insureds that may be victim to a cyber-attack, but not physically located in the impacted state. This carve back doesn't cover **cyber war** events conducted as part of physical war.

B. First party loss amendatory exclusion (infrastructure), to replace first party loss exclusion.

Our updated infrastructure exclusion addresses infrastructure and utilities that fall outside the scope of coverage.

Our new definition of **digital and internet infrastructure** describes the basic components of telecommunications infrastructure: internet and communications infrastructure - that fall within the ambit of the exclusion. These entities, already included in our internet and communications infrastructure remain excluded. (See question 5 for details on the entities that are listed in the exclusion).

Our new definition of **financial market infrastructure** lists entities that facilitate financial markets and securities trading.

Issues affecting "backbone" components, by definition, are out of scope for coverage, additionally issues with off-premises utilities are excluded from property policies. Internet and communications capabilities use the backbone entities to function such that any outages necessarily cause too widespread an impact to appropriately underwrite or price.

Internet service provider (ISPs) and cloud service providers are not listed in our new definition of **digital and internet infrastructure**.

C. Catastrophic cyber event endorsement addresses two significantly high threshold scenarios for catastrophic risk.

Our new catastrophic cyber event endorsement addresses two theoretical potential scenarios. Both are remote possibilities, but should they occur have the potential to cause significant impact.

(1) An extended outage of a major **cloud service provider** exceeding 72 hours; and

(2) contagion malware in a **computer operating system**, causing a major detrimental impact to a state's ability to provide essential services and/or defend itself.

For covered first party loss arising from catastrophic cyber events, a 50% sub-limit of liability will now apply to stand-alone cyber insureds with revenues of less than 100M (USD/EUR/GBP). This endorsement introduces a sublimit to first party loss only and is not an exclusion. This sublimit, allows us to establish a carefully calculated ceiling for these two extreme events. (see questions 7 and 8 for further details).

Further, our insureds will maintain access to breach response coverage and third party liability coverage up to full policy limits, as well as the full range of our risk mitigation tools.

2. What policies are affected?

The chart below outlines the affected policies

- The revised infrastructure and war exclusion wordings apply to all primary cyber and MediaTech (E&O) policies of all account sizes

- The catastrophic event sublimit endorsement will only be added to primary cyber policies for accounts below 100M (USD/EUR/GBP) in revenues.

These wordings will be added to policies starting with January 1, 2023 effective dates for surplus lines and most admitted business, with admitted business changes subject to state approval.

	Catastrophic Event Sublimit	Infrastructure Exclusion	War Exclusion
Portfolio segments in scope	• All primary layer cyber policies for insureds with revenues 100m or less – not excess • Not applicable to E&O	• All primary layer cyber policies – not excess • Applicable to E&O	• All primary layer cyber policies – not excess* • Applicable to E&O
Territory segments in scope	• USA • London wholesale • International via Lloyd's • International via BDAC	• USA • London wholesale • International via Lloyd's • International via BDAC	• USA • London wholesale • International via Lloyd's • International via BDAC
Sub-limit level	• 50% with no option to buy-back the limits • No premium reductions	• USA	• USA
New/Renewal	• New and renewal business	• New and renewal business	• New and renewal business
Timings	• Applies to all 1/1/23 effective dates	• Applies to all 1/1/23 effective dates	• Applies to all 1/1/23 effective dates

Actual dates may be later than January 1 for admitted business.

* Unless the primary wording is deemed not compliant with Lloyds requirements as of 31 March 2023.

3. Does Beazley's revised war exclusion meet the Lloyd's requirements, which go live March 31, 2023?

Yes, our language satisfies the Lloyd's requirements.

4. Does Beazley's revised war exclusion require attribution to a state actor?

Our war exclusion references a harmful act that "is committed by, or at the direction or under the control of, a sovereign state," and does not include any additional attribution terms and conditions. With respect to the above phrase, ordinary principals of contract interpretation apply, and the burden of proof to assert this exclusion remains with Beazley.

Further (as mentioned in question 1, above) the words "hostilities", "warlike," and "acts of foreign enemies" are not used. A "major detrimental impact" maybe required. This alleviates the attribution requirement for lower level acts that may or may not have been committed by or on behalf of a sovereign state.

5. What are the key elements of Beazley's revised infrastructure exclusion? What is the scope of coverage for internet service providers (ISPs) and cloud service providers?

As mentioned in question 1, the new infrastructure exclusion addresses what is meant by Internet and communications infrastructure by specifying the backbone component entities that fall within the ambit of the exclusion.

These elements include the following:

1. **Financial market infrastructure**
   - Securities exchanges, central counterparty clearing houses, and central securities depositories

2. **Digital and internet infrastructure**
   - Internet exchange point providers
   - Domain name system (DNS) service providers
   - Trust service providers/certificate authorities
   - Content delivery network (CDN) providers
   - Timing servers (including stratum-1 and 2)
   - Electronic communications network infrastructure providers

3. **Electronic communications network infrastructure providers**

   Electronic communications network infrastructure used for the provision of publicly available electronic communications services which support the transfer of information between network termination points (e.g. radio, satellite and mobile networks). Providers of electronic communications network infrastructure may include providers of internet backbone components, including logical and physical network infrastructure (e.g. cables, ducts, switches, routers), as well as other components such as undersea cables or infrastructure for satellite communications.

ISPs are not specifically listed in the exclusion. If an ISP had an issue that was isolated to that ISP (assuming coverage was triggered), the exclusion would not apply. However, if there was a failure, interruption or malfunction of one of the named elements of **digital and internet infrastructure**, then the exclusion would apply.

Cloud service providers are also not specifically listed in the exclusion. If a cloud service provider e.g. Amazon Web Services (AWS) had an issue that was isolated to that cloud service provider (assuming coverage was triggered), the exclusion would not apply. If there was a failure, interruption or malfunction of one of the named elements of **digital and internet infrastructure**, then the exclusion would apply.

Please also note that the Beazley catastrophic cyber event endorsement may apply to a cloud service provider event, if such event involved one of the named four cloud providers and exceeded 72 hours.

6. The revised war exclusion and the catastrophic risk endorsements reference terms “major detrimental impact” and “essential services”. What is meant by these terms?

The term “major detrimental impact” describes the impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life. The determination is fact specific; in this context ‘”major detrimental impact” is an objective, not a subjective concept.

The term “essential services” means a service that is essential for the maintenance of vital functions of a state, including but not limited to financial institutions and associated financial market infrastructure, food, energy, transportation, emergency services, healthcare or utility services.

These terms and concepts are commonly referenced by governmental authorities when defining potential impact or disruption of critical infrastructure (e.g. UK Centre for the Protection of National Infrastructure, and the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency’s (CISA’s) list of Critical Infrastructure Sectors).

The ransomware attack against Colonial Pipeline (May 7, 2021) caused a several-day interruption of oil and gas delivery to the eastern United States when the pipeline was taken offline to prevent the ransomware from spreading. The shutdown affected oil and gas supply to consumers and airlines and caused President Joe Biden to declare a state of emergency, which enabled fuel supply from alternative sources. In some locations in the United States, gas stations reported shortages and consumers resorted to panic buying of gasoline; and airlines needed to adjust schedules to accommodate alternative jet fuel sources. Even so, this event did not rise to the level of “major detrimental impact” as this term is intended – the threshold of what constitutes “major detrimental impact” is higher yet than the impact seen in this case.

Other significant cyber incidents, including WannaCry (which impacted hundreds of thousands of computers around the world, including the National Health Service hospitals in England and Scotland) and Solarwinds (which impacted several US government agencies as well as prominent US companies), did not rise to the level of “major detrimental impact” to the availability, delivery or integrity of essential services. Rather, the impact threshold intended is higher than that which was observed by these two significant incidents.

7. Beazley's new catastrophic risk endorsement applies a 50% sublimit to a contagion malware event to a computer operating system: what does Beazley consider an operating system versus an application for purposes of this definition? Why is there not an hour clause for the computer operating system like we see on the cloud service provider outage?

Operating system software is a system software, not an application software. The differences are highlighted below:

System software: built to be used by the computer

- Utility software part of and installed at the same time the OS by the manufacturer
- Runs any time the computer is on
- Runs independently
- Is necessary for the system to function
- Works in the background and users don't usually access it
- Interacts closely with hardware.

Application software: built to be used by the user

- User or admin installs software when needed
- User triggers and stops the program
- Needs system software to run
- Isn't needed for the system to function
- Runs in the foreground and users work directly with the software to perform specific tasks
- Does not interact directly with hardware.

There is not an hours clause for computer operating system because it is under the operational control of the user – and therefore any outage or fix will be within the control of the owner or operator of the device or endpoint affected. Cloud services are generally provided by a third party and are therefore any outage or fix is under the control of the cloud services provider, as a dependency to any user.

8. Beazley's new catastrophic risk endorsement applies a 50% sublimit to a cloud service provider outage exceeding 72 hours. What happens if the outage is only 70 hours? What happens if a Saas provider experiences an outage?

In the event of a cloud service provider outage that lasts only 70 hours, the catastrophic risk endorsement sublimit does not apply, and the full policy limits would apply to that event.
The focus for the sublimit is on prolonged cloud outages. Further, in order to trigger the sublimit, the event must arise from one of the four scheduled cloud service providers: Amazon Web Services, Microsoft Azure, Google Cloud Platform or IBM Cloud.

Therefore, the sublimit does not apply to outages of Saas providers or services, unless the Saas outage is caused by an outage of one of the four scheduled cloud service providers for longer than 72 hours.

The descriptions contained in this communication are for broker preliminary informational purposes only. Coverages can be underwritten by Beazley syndicates at Lloyd’s or Beazlzey Insurance dac or Lloyd’s Insurance Company (“Lloyd’s Brussels”) and will vary depending on individual country law requirements and may be unavailable in some countries. The exact coverage afforded by the products described in this communication are subject to and governed by the terms and conditions of each policy issued. For more information, visit www.beazley.com