LLOYD'S

EM 426 v1.0

RDS 2023

Realistic Disaster Scenarios
Scenario Specification
January 2023

Key Contacts

Head of Portfolio Risk Management

Kirsten Mitchell-Wallace
020 7327 5839
kirsten.mitchell-wallace@lloyds.com

Head of Exposure Management and Aggregation

Emma Watkins
020 7327 5719
emma.watkins@lloyds.com

Exposure Management

Lauren Restell
020 7327 5644
lauren.restell@lloyds.com

Graham Clark
020 7327 5647
Graham.clark@lloyds.com

Ceara Howey
020 7327 6228
ceara.howey@lloyds.com

Edward Nicholas
020 7327 5306
edward.nicholas@lloyds.com

Charlotte Spears
020 7327 5893
charlotte.spears@lloyds.com

Mark Tilbury
020 7327 5021
Mark.tilbury@lloyds.com

Aggregation

Luke Knowles
020 7327 5842
luke.knowles@lloyds.com

IT Support

ITG Data Management Helpdesk
020 7327 5252
ITGApplicationSupport2@lloyds.com

Acknowledgements

In producing the documentation for the RDS framework, Lloyd's has worked closely with the Lloyd's Market Association (LMA) to incorporate market expertise via various market panels and groups. The assistance of the individuals involved and the support of their respective organisations has been invaluable and their contribution is greatly appreciated.

The spatial data used to generate the revised maps within this document were as follows: -

- *Gulf of Mexico blocks - the Bureau of Ocean Management (http://www.boem.gov/Oil-and-Gas-Energy Program/Mapping-and-Data/Maps-And-Spatial-Data.aspx);*
- *all other maps - Natural Earth (http://www.naturalearthdata.com/downloads/)*

Disclaimer

Document history

v1.0	January 2023	Original publication

Contents

1 Introduction

The purpose of this document is to describe the loss assumptions for each of Lloyd's Realistic Disaster Scenarios [RDS].

For information about Lloyd's 2023 reporting requirements, please see the 2023 RDS Guidance & Instructions.

1.1 Specification of the RDS events

For each compulsory scenario (see section 1.2.1) this document contains:

- a definition of the physical event, with a map showing the footprint or storm track;
- the assumed industry insured loss for property, split by primary class of business;
- additional lines of business that managing agents are recommended to consider;
- where applicable, a catalogue of major infrastructure (i.e. ports) that may be affected by the event;
- where applicable, supplementary information that managing agents are required to provide (e.g. offshore energy).

For each *de minimis* scenario this document contains: -

- a description of the event, or type of event;
- additional information to the loss return which managing agents should provide;
- where applicable, examples of scenarios - or types of scenarios - which managing agents may choose;
- where applicable, assumptions about reinsurance protections.

For details of the Political Risks scenarios, please see the separate 2023 RDS Political Risks Scenario Specification document which is available on request from Lloyd's Exposure Management team.

1.2 Scenarios

1.2.1 Compulsory scenarios

There are twenty compulsory scenarios (including Alternatives A&B) which managing agents must complete for all syndicates.

Lloyd's does not prescribe how managing agents should calculate losses from these scenarios. The Calculation Principles in the RDS Guidance & Instructions describe some possible methodologies and the reporting conditions applying to each.

Managing agents who use the Lloyd's damage factors and/or Lloyd's suggested property distributions will find them in the RDS Damage Factors and Cyber Calculation Tools spreadsheets. Table 1 shows the scenarios for which this data is available.

RDS		Industry Loss	Lloyd's damage-factors provided?	Lloyd's property distribution tables provided?	Scenario ID
Two events – North-East windstorm		USD 81bn	Yes	No	41
Two events – South Carolina windstorm		USD 39bn	Yes	No	42
Florida Windstorm – Miami-Dade		USD 131bn	Yes	No	2
Florida Windstorm – Pinellas		USD 134bn	Yes	No	3
Gulf of Mexico Windstorm	Onshore	USD 111bn	Yes	No	12
	Offshore	USD 7.1bn	No	n/a	
European Windstorm		€ 24bn	Yes	Yes	8
Japanese Typhoon		¥ 1.7trn	Yes	Yes	13
California Earthquake – Los Angeles		USD 78bn	Yes	Yes	4
California Earthquake – San Francisco		USD 80bn	Yes	Yes	5
New Madrid Earthquake		USD 44bn	Yes	Yes	6
Japanese Earthquake		¥ 8trn	Yes	Yes	9
UK Flood		GBP 6.2bn	No	No	51
Terrorism – Rockefeller Center		n/a	No	No	43
Terrorism – One World Trade Center		n/a	No	No	78
Cyber – Business Blackout II		n/a	Yes	n/a	82
Cyber – Ransomware Contagion		n/a	Yes	n/a	83
Cyber – Cloud Cascade		n/a	Yes	n/a	84
Cyber – Major Data Security Breach		n/a	No	n/a	76

Table 1

Managing agents should report two further realistic events (Alternative A and B) that represent potential material impact to the syndicate but are not listed in either the compulsory or de minimis scenarios.

1.2.2 De minimis scenarios

The following scenarios are subject to *de minimis* reporting. Please see RDS Guidance & Instructions 2023 for definition of *de minimis* thresholds.

	RDS	Scenario i/d
1	Marine (two scenarios)	79,80
2	Loss of Major Complex	17
3	Aviation Collision	18
4	Satellite risks (four scenarios)	70,71,72,73
5	Liability risks (two scenarios)	53,54
6	Political risks *(see RDS Political Risks Scenario Specification 2023 document)*	

Table 2

Compulsory Scenarios

2 Two Windstorm events

A North-East US hurricane, immediately followed by a South Carolina hurricane.

Managing agents should return separate loss estimates for each event.

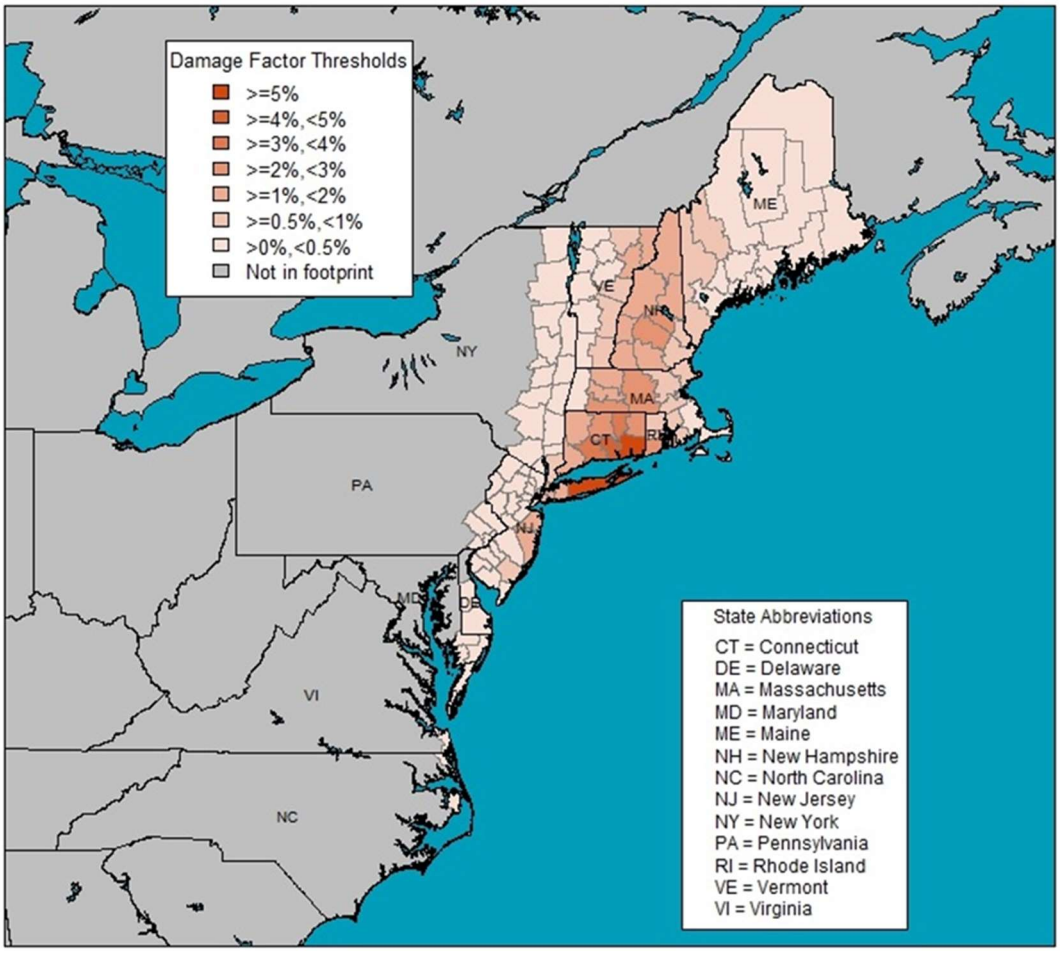
Managing agents should assume that these events fall in the same reinsurance year, and that there has not been sufficient time between events to purchase additional reinsurance protection.

2.1 Event definition 1 - North East hurricane

A North East hurricane making landfall in New York State, including consideration of demand surge and storm surge. The hurricane also generates significant loss in the States of New Jersey, Connecticut, Massachusetts, Rhode Island and Pennsylvania.

2.1.1 Event footprint 1 – North East hurricane

Map 1 illustrates the footprint and combined damage levels for the North East Hurricane Event.



Map 1

2.1.2 Industry Loss Levels – North East hurricane

This event results in an estimated Industry Property Loss of USD81bn with the following components:

Residential Property	$49.50bn
Commercial Property	$31.50bn
Auto	$1.75bn
Marine	$0.75bn

Table 3

Managing agents should consider all other lines of business that would be affected, including:

1) Specie/Fine Art
2) Personal Accident
3) Aviation
4) Liability
5) Cancellation

2.2 Exposure information for North East hurricane

2.2.1 Major ports

Table 4 lists the main affected ports that managing agents should consider in assessing their potential exposures. They should also consider smaller ports that fall within the footprint of the event.

Port	County	State
Camden	Camden	New Jersey
New York/New Jersey		
Philadelphia	Delaware	Pennsylvania

Table 4

2.2.2 Major airports

Table 5 lists the main international airports in the affected areas. Managing agents should also have regard to exposures in smaller airports that fall within the footprint of the event.

Airport	County	State
Atlantic City International Airport (ACY)	Atlantic	New Jersey
Bradley International Airport (BDL)	Hartford	Connecticut
Edward Lawrence Logan International Airport (BOS)	Suffolk	Massachusetts
John F. Kennedy International Airport (JFK)	Queens	New York
La Guardia Airport (LGA)	Queens	New York
Lehigh Valley International Airport (ABE)	Lehigh	Pennsylvania
Newark International Airport (EWR)	Essex	New Jersey
Philadelphia International Airport (PHL)	Delaware	Pennsylvania
Providence - T.F. Green Airport (PVD)	Kent	Rhode Island
Tetarboro Airport (TEB)	Bergen	New Jersey
Wilkes-Barre/Scranton International Airport (AVP)	Luzerne	Pennsylvania

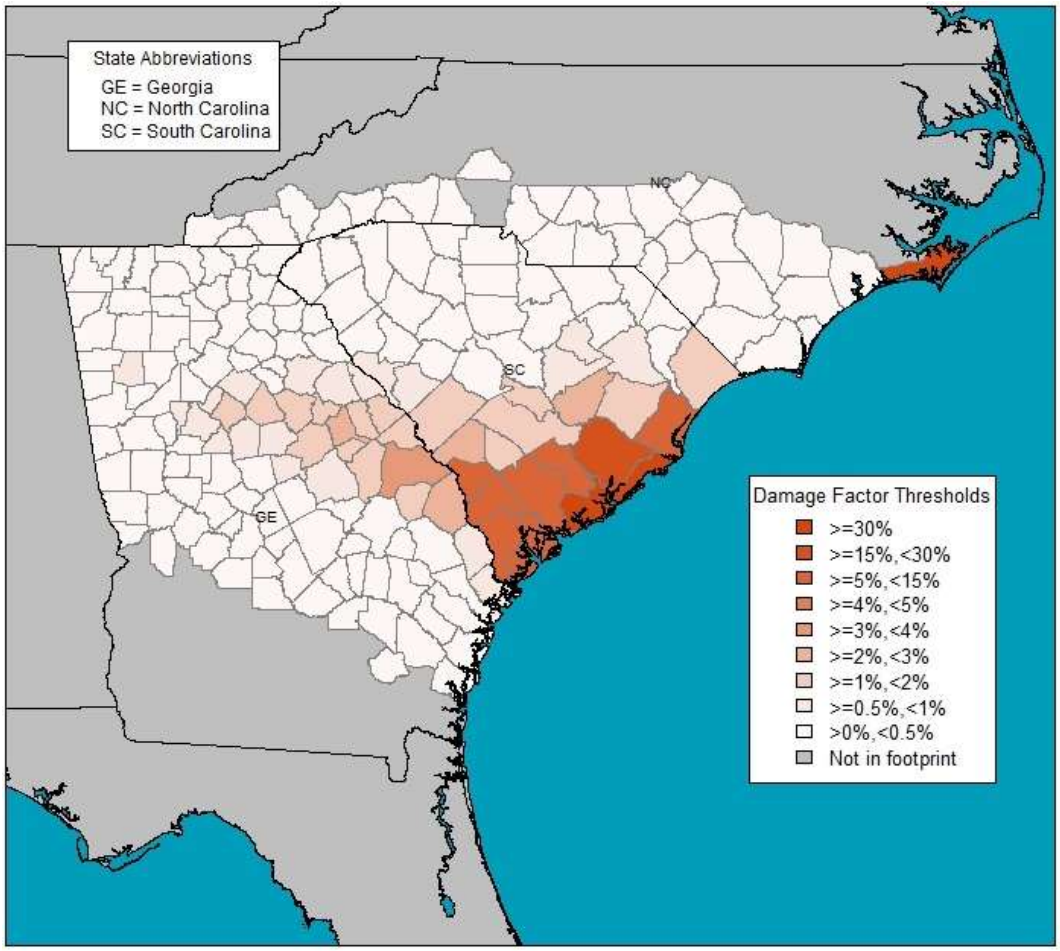
Table 5

2.3 Event definition 2 – South Carolina hurricane

A hurricane making landfall in South Carolina, including consideration of demand surge and storm surge.

2.3.1 Event footprint 2 – South Carolina hurricane

Map 2 illustrates the footprint and combined damage levels for the South Carolina Windstorm Event.



Map 2

2.3.2 Industry Loss Levels – South Carolina hurricane

This event results in an estimated Industry Property Loss of USD 39bn including consideration of storm surge and demand surge. Managing agents should assume the following components of the loss.

Residential Property	$26.00bn
Commercial Property	$13.00bn
Auto	$0.53bn
Marine	$0.27bn

Table 6

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Specie/Fine Art
2) Personal Accident
3) Aviation
4) Liability
5) Cancellation

2.3.3 Reinsurance

For reinsurance purposes, managing agents should assume that the South Carolina hurricane falls in the same reinsurance year as the North East hurricane, and that there has not been sufficient time between events to purchase additional reinsurance protection.

2.4 Exposure information for South Carolina hurricane

2.4.1 Major Ports

Table 7 lists the main ports in South Carolina that would be affected by the windstorm that managing agents should consider in assessing their potential exposures. They should also have regard to exposures in smaller ports that fall within the footprint of the event.

Port	County
Charleston	Charleston
Georgetown	Georgetown
Port Royal	Beaufort

Table 7

2.4.2 Major Airports

Table 8 lists the main international airports in the affected areas, which managing agents should consider in assessing their potential exposures. They should also have regard to exposures in smaller airports that fall within the footprint of the event.

Airport	County
Charleston International Airport (CHS)	Charleston
Greenville - Spartanburg International Airport (GSP)	Greenville

Table 8

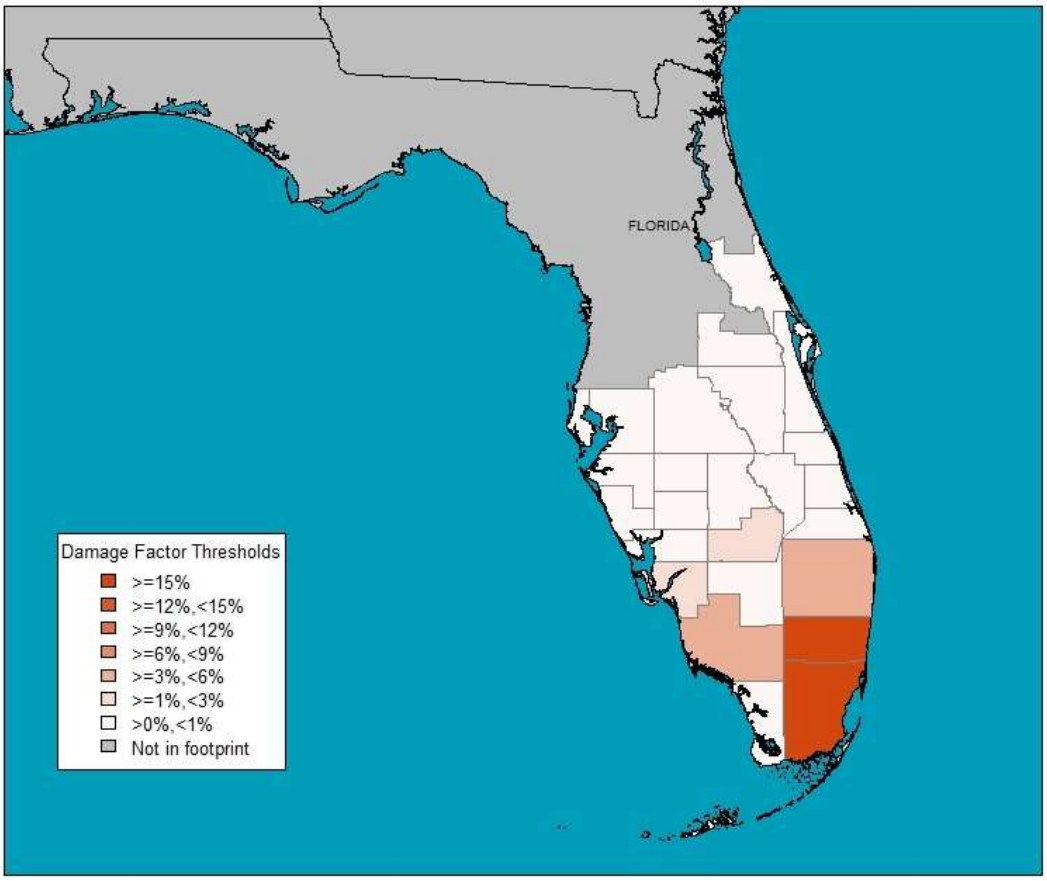
3 Florida windstorm: Miami Dade

3.1 Event definition

A Florida Windstorm landing in Miami-Dade County, including storm surge and demand surge.

3.1.1 Event footprint

Map 3 illustrates the event footprint and combined damage levels for the Miami-Dade Windstorm Event, which are detailed in the RDS Damage Factors available from Lloyd's.



Map 3

3.1.2 Industry Loss Level

This event results in an estimated Industry Property Loss of USD 131bn including consideration for storm surge and demand surge. Managing agents should assume the following components of the loss: -

Residential Property	$66.00bn
Commercial Property	$65.00bn
Auto	$2.25bn
Marine	$1.00bn

Table 9

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Specie/Fine Art
2) Personal Accident
3) Aviation
4) Liability
5) Cancellation

3.2 Exposure information

3.2.1 Major ports

Table 10 lists the main ports in Florida, which managing agents should consider in assessing their potential exposures.

They should also have regard to exposures in smaller ports that fall within the footprint of the events.

Port	County
Jacksonville	Duval
Miami	Miami-Dade
Palm Beach	Palm Beach
Port Canaveral	Brevard
Port Everglades	Broward
Port Manatee	Manatee
Tampa	Hillsborough

Table 10

3.2.2 Major airports

Table 11 lists the main international airports in Florida, which managing agents should consider in assessing their potential exposures.

They should also have regard to exposures in smaller airports that fall within the footprint of the events.

Airport	County
Fort Lauderdale/Hollywood	Broward
Miami	Miami-Dade
Orlando	Orange
Tampa	Hillsborough

Table 11

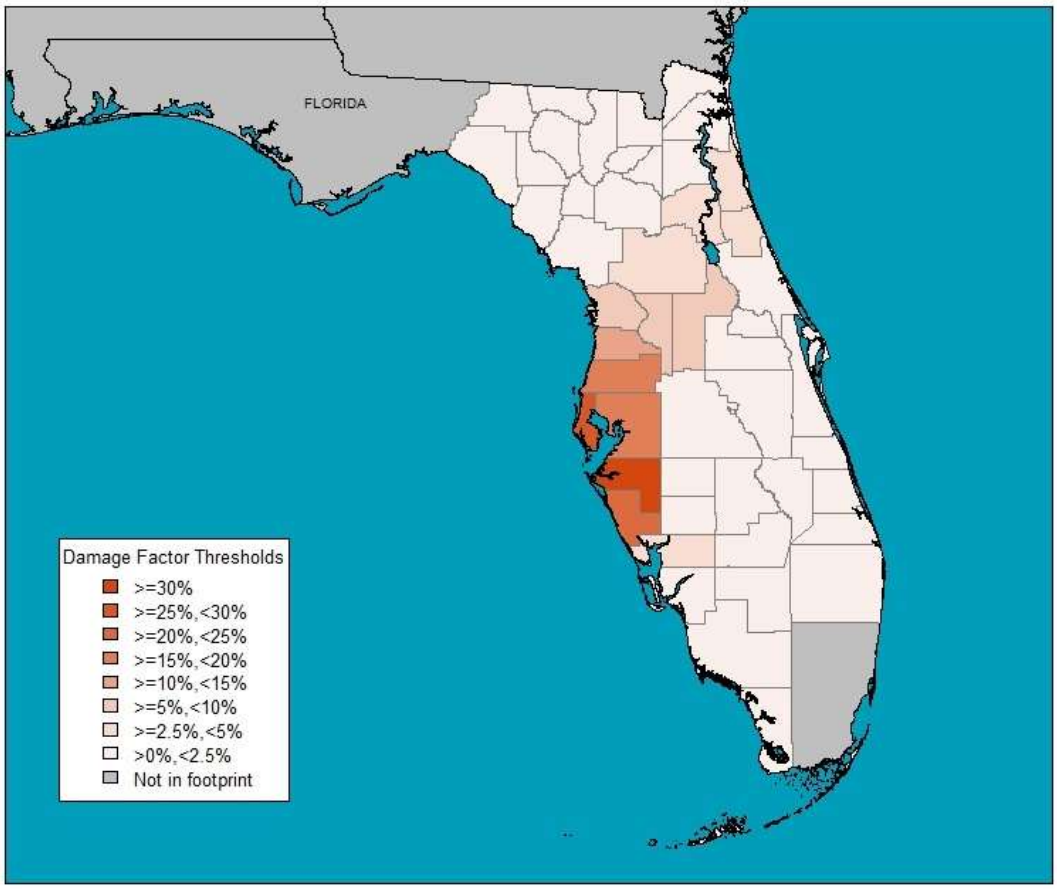
4 Florida windstorm: Pinellas

4.1 Event definition

A Florida Windstorm landing in Pinellas County, including storm surge and demand surge.

4.1.1 Event footprint

Map 4 illustrates the footprint and combined damage levels for the Pinellas Windstorm Event, which are detailed in the RDS Damage Factors that are available from Lloyd's.



Map 4

4.1.2 Industry Loss Levels

This event results in an estimated Industry Property Loss of USD 134bn, including consideration for storm surge and demand surge. Managing agents should assume the following components of the loss: -

Residential Property	$94.5bn
Commercial Property	$39.5bn
Auto	$2.00bn
Marine	$1.00bn

Table 12

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Specie/Fine Art
2) Personal Accident
3) Aviation
4) Liability
5) Cancellation

4.2 Exposure information

Please see section 3.2 above.

5 Gulf of Mexico windstorm

5.1 Event definition

A Gulf of Mexico hurricane resulting in: -

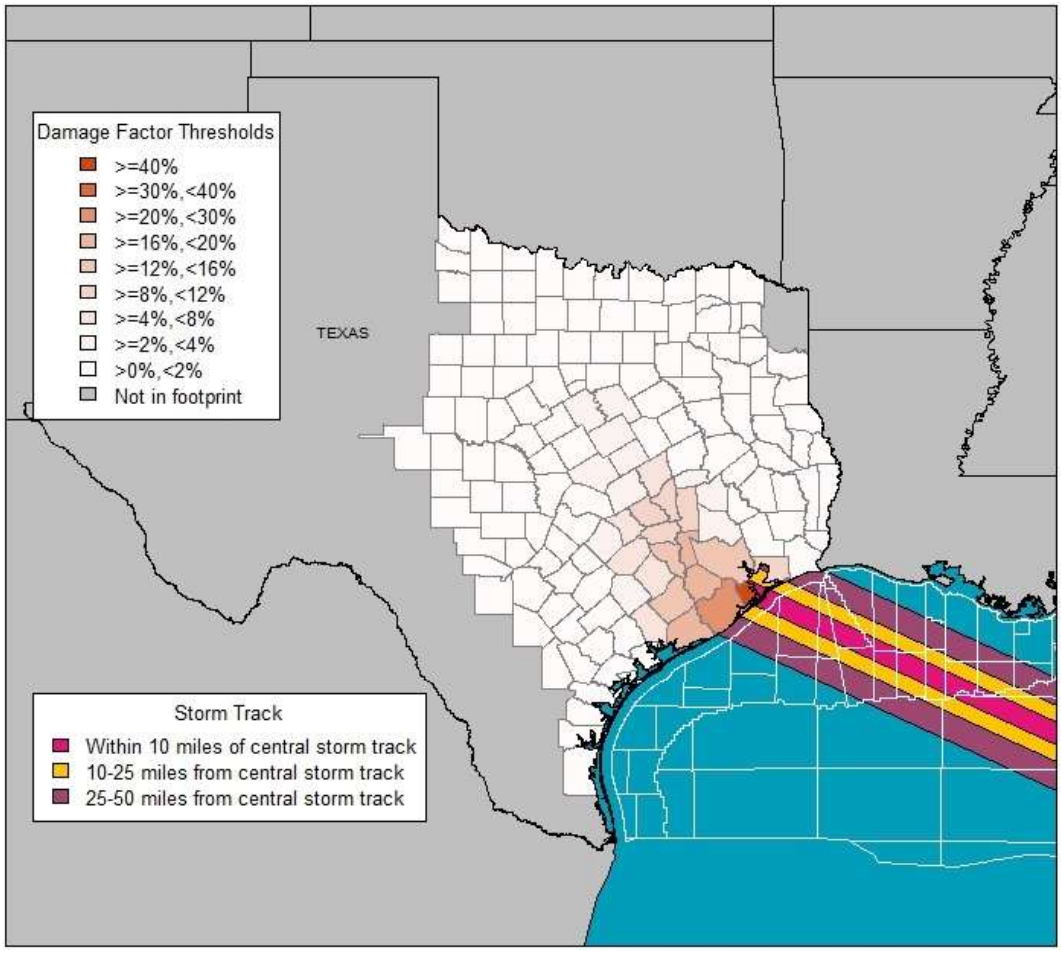
- mainland property losses including the consideration of demand surge and storm surge; and
- offshore energy insured losses.

Managing agents should return a single combined loss (onshore and offshore) for this scenario.

5.2 Offshore component

5.2.1 Storm track

Map 5 below illustrates the damage track of the windstorm in the Gulf of Mexico.



Map 5

Position of centre of damage track: -

Start	Latitude 25° 50’ 30.8401" North	Longitude 86° 00’ 50.0400" West
End	Latitude 30° 52’ 53.7600" North	Longitude 98° 43’ 16.3200" West

Table 13

5.2.2 Industry Loss Levels - offshore

This event results in offshore energy insured loss of USD7.1bn (estimated USD17bn insurable loss).

5.3 Onshore component

5.3.1 Storm track - onshore

The map in section 5.2 highlights the footprint and combined damage levels for the onshore component of the affected counties. These damage levels are detailed in the RDS Damage Factor Tables that are available from Lloyd's.

5.3.2 Industry Loss Levels - onshore

This event results in onshore insured loss of USD111bn including consideration of storm surge and demand surge. Managing agents should assume the following components of the loss: -

Residential Property	$67.5bn
Commercial Property	$43.5bn
Auto	$1.00bn
Marine	$1.00bn

Table 14

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Specie/Fine Art
2) Personal Accident
3) Aviation
4) Liability
5) Cancellation

5.4 Exposure information

5.4.1 Major Ports

Table 15 lists the main ports in Texas that would be affected by the windstorm, which managing agents should consider in assessing syndicate potential exposures. They should also have regard to exposures in smaller ports that fall within the footprint of the event.

Port	County
Beaumont	Jefferson
Freeport	Brazoria
Galveston	Galveston
Houston	Harris
Matagorda Ship Channel	Calhoun
Orange	Orange
Port Arthur	Jefferson
Texas City	Galveston
Victoria	Victoria

Table15

5.4.2 Major Airports

Table 16 lists the main airports in Texas that would be affected by the windstorm, which managing agents should consider in assessing their potential exposures. They should also have regard to exposures in smaller airports that fall within the footprint of the event.

Airport	County
Brazoria County	Brazoria
Clover Field	Brazoria
David Wayne Hooks Memorial	Harris
Easterwood Field	Brazos
Ellington Field	Harris
George Bush Intercontinental	Harris
Killeen Municipal	Bell
Robert Gray Army Air Field	Bell
Salaika Aviation	Brazoria
Scholes International	Galveston
Southeast Texas Regional	Jefferson
Sugar Land Municipal	Fort Bend
Victoria Regional	Victoria
Waco Regional	Mclennan
William P. Hobby	Harris

Table 16

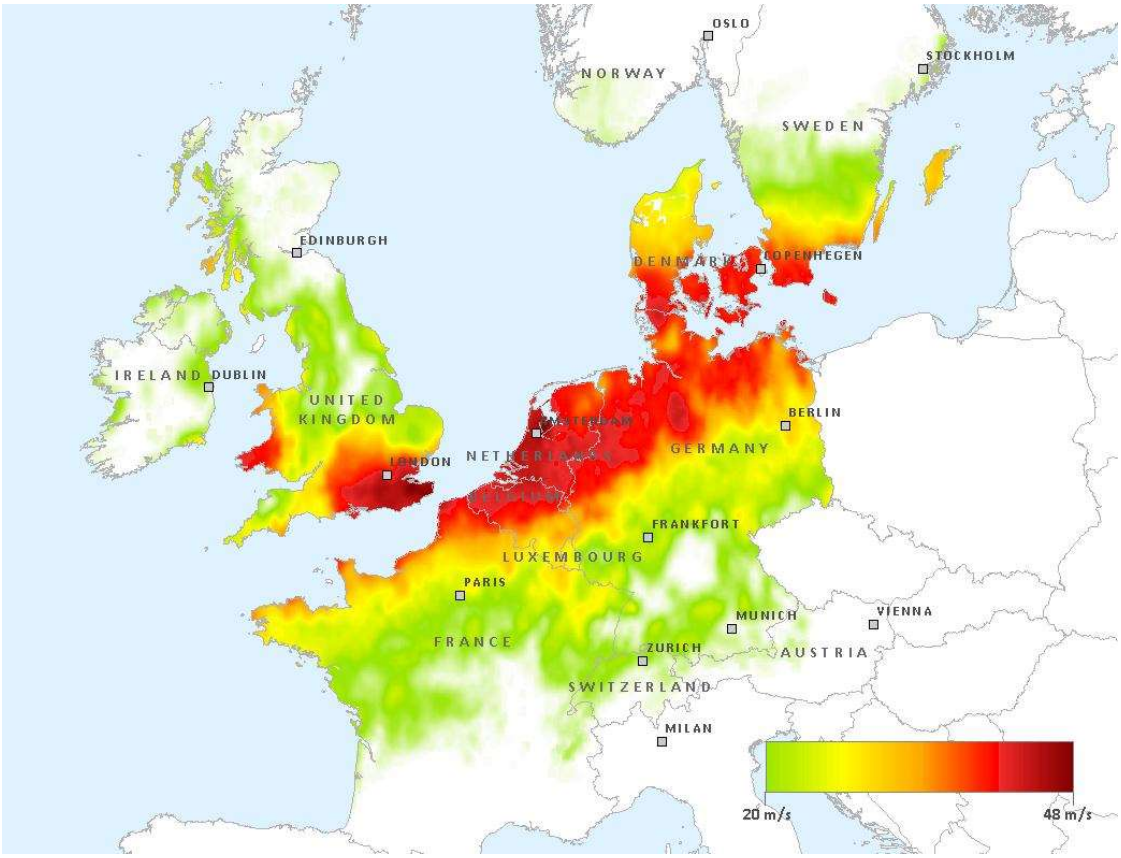
6 European Windstorm

6.1 Event definition

This event is based upon a low-pressure track originating in the North Atlantic basin resulting in an intense windstorm with maximum/peak gust wind speeds in excess of 20 metres per second (45 mph or 39 knots). The strongest winds occur to the south of the storm track, resulting in a broad swath of damage across southern England, northern France, Belgium, Netherlands, Germany and Denmark.

6.1.1 Storm track

Map 6 illustrates the windstorm track and affected regions (image courtesy of Verisk).



Map 6

6.1.2 Industry Loss Levels

This event results in an estimated Industry Property Loss of €24bn. Managing agents should assume the following components of the loss: -

Residential Property	€16.00bn
Commercial Property	€6.5bn
Agricultural	€1.50bn
Auto	€0.75bn
Marine	€0.40bn

Table 17

Managing agents should consider all other lines of business that would be affected by the event, including: -

1) Specie/Fine Art
2) Personal Accident
3) Aviation
4) Liability

6.2 Exposure information

6.2.1 Property value distribution

Tables outlining Lloyd's assumptions for the distribution of property values for this event are listed in the RDS Damage Factors that are available from Lloyd's.

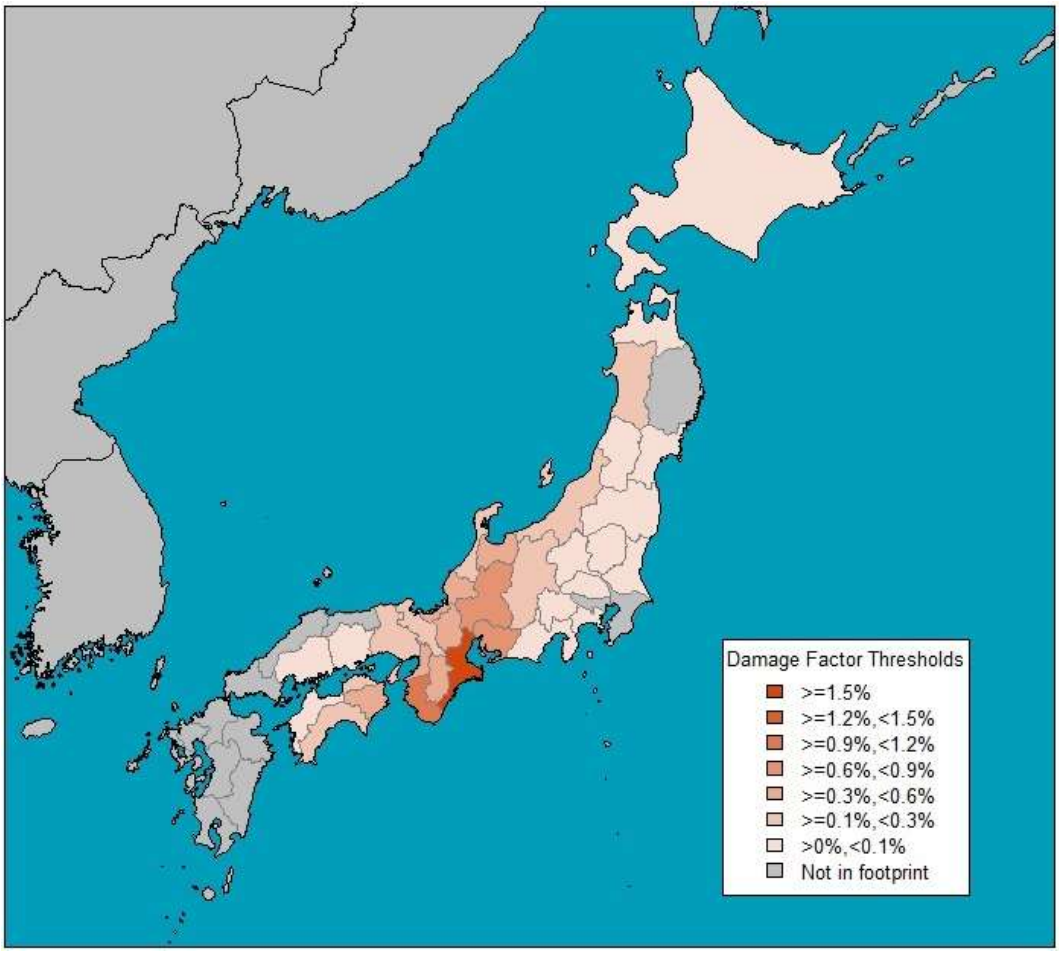
7 Japanese typhoon

7.1 Event definition

This event is based on the Isewan (‘Vera’) typhoon event of 1959.

7.1.1 Storm track

Map 7 highlights the footprint and residential ground-up damage levels for the Japanese typhoon event. These damage levels are detailed in the RDS Damage Factor Tables that are available from Lloyd’s.



Map 7

7.1.2 Industry Loss Levels

This event results in a present-day Industry Property Loss estimate of ¥1.7trn. Managing agents should assume the following components of the loss: -

Residential Property	¥750bn
Commercial Property	¥950bn
Marine	¥50bn

Table 18

Managing agents should consider all other lines of business that would be affected by the event, including particularly: -

1) Specie/Fine Art
2) Personal Accident
3) Aviation
4) Liability
5) Marine

7.2 Exposure information

7.2.1 Property value distribution

Lloyd's assumptions for the distribution of property values at prefecture level are detailed in the RDS Damage Factors that are available from Lloyd's.

7.2.2 Major Ports

Table 19 below lists the main Japanese ports in the Typhoon Isewan (Vera) footprint, which managing agents should consider in assessing syndicate potential exposures. They should also have regard to exposures in smaller ports that fall within the footprint of the event.

Port
Chiba Port
Nagoya Port
Yokohama Port
Kawasaki Port
Mitzushima Port
Kitakyushu Port
Tokyo Port
Osaka Port
Tomakomai Port
Kobe Port

Table 19

7.2.3 Major Airports

Table 20 lists the main international and domestic airports potentially impacted by the Typhoon, which managing agents should consider in assessing syndicate potential exposures.

Airport
Narita International Airport
Central Japan International Airport
Kansai International Airport
Tokyo International Airport
Osaka International Airport

Table 20

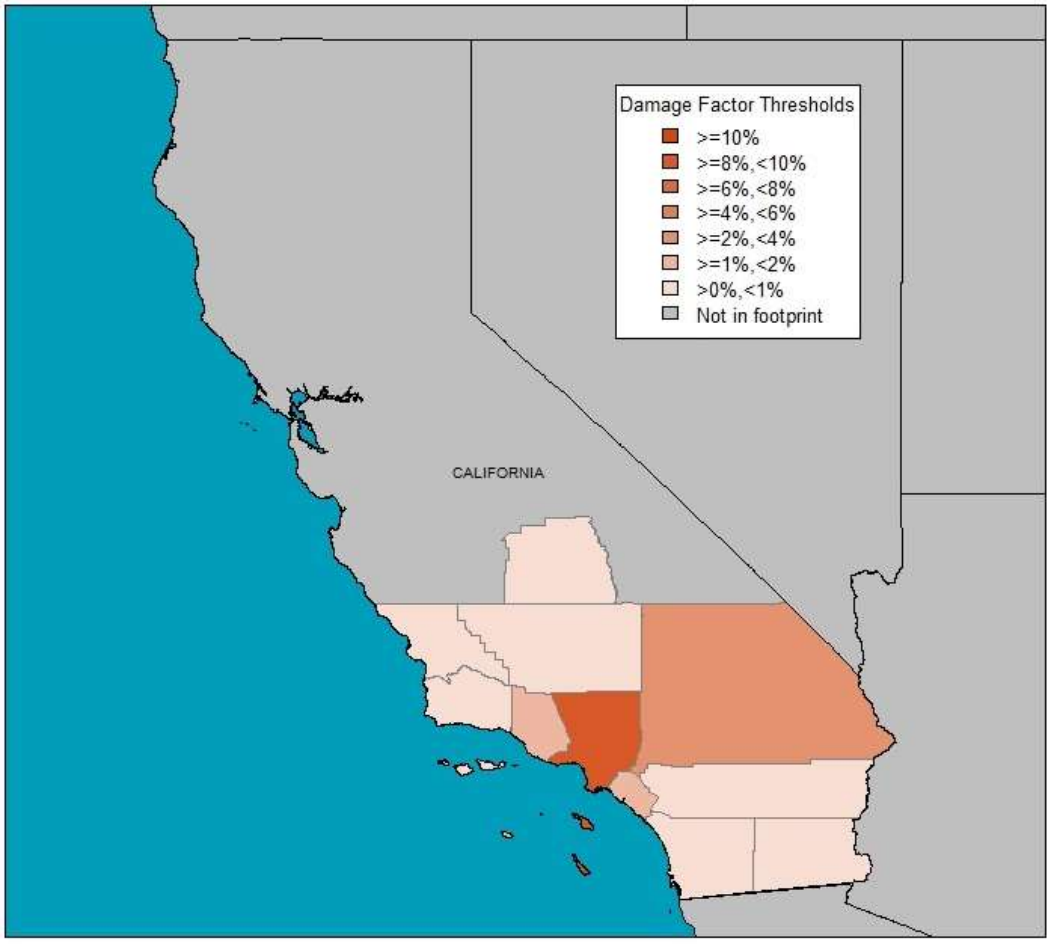
8 California Earthquake: Los Angeles

8.1 Event definition

An earthquake causing major damage to Los Angeles from shake and fire-following, gross of take-up rates and including consideration of demand surge.

8.1.1 Event footprint

Map 8 illustrates the footprint and residential, ground-up shake damage levels for the Los Angeles earthquake event.



Map 8

8.1.2 Industry Loss Levels

This event results in an estimated USD78bn Industry Property Loss (shake and fire following), *after* taking into account take-up rates but *before* applying policy terms. Demand surge is included. Managing agents should assume the following components of the loss:

Residential Property	$36.00bn
Commercial Property	$42.00bn
Workers Compensation	$5.50bn
Marine	$2.25bn
Personal Accident	$1.00bn
Auto	$1.00bn

Table 21

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Specie/Fine Art
2) Liability
3) Cancellation
4) PA and WCA losses – it should be assumed that there will be 2,000 deaths and 20,000 injuries as a result of the earthquake. Managing agents should assume that 50% of those injured will have PA cover.
5) Estimation of Aviation Hull losses – Lloyd's has commissioned research that indicates that minimal Aviation Hull losses would be expected to arise from an earthquake. Managing agents should take account of these findings in calculating syndicate loss estimates.

8.2 Exposure information

8.2.1 Property value distribution

Lloyd's assumptions for the distribution of property values are detailed in the RDS Damage Factors spreadsheet available from Lloyd's.

8.2.2 Major Ports

Table 22 lists the main ports in California, which managing agents should consider in assessing their potential exposures. They should also give regard to exposures in smaller ports that fall within the footprint of the events.

Port	County
Long Beach	Orange
Los Angeles	Los Angeles
Oakland	Alameda
Port Hueneme	Ventura
Richmond	Contra Costa
San Diego	San Diego
San Francisco	San Francisco
Stockton	San Joaquin

Table 22

8.2.3 Major Airports

Table 23 lists the main international airports in California, which managing agents should consider in assessing their potential exposures. They should also have regards to exposures in smaller airports that fall within the footprint of the events.

Airport	County
Los Angeles (LAX)	Los Angeles
San Diego-Linderbergh (SAN)	San Diego
San Francisco (SFO)	San Francisco
San Jose (SJC)	San Jose

Table 23

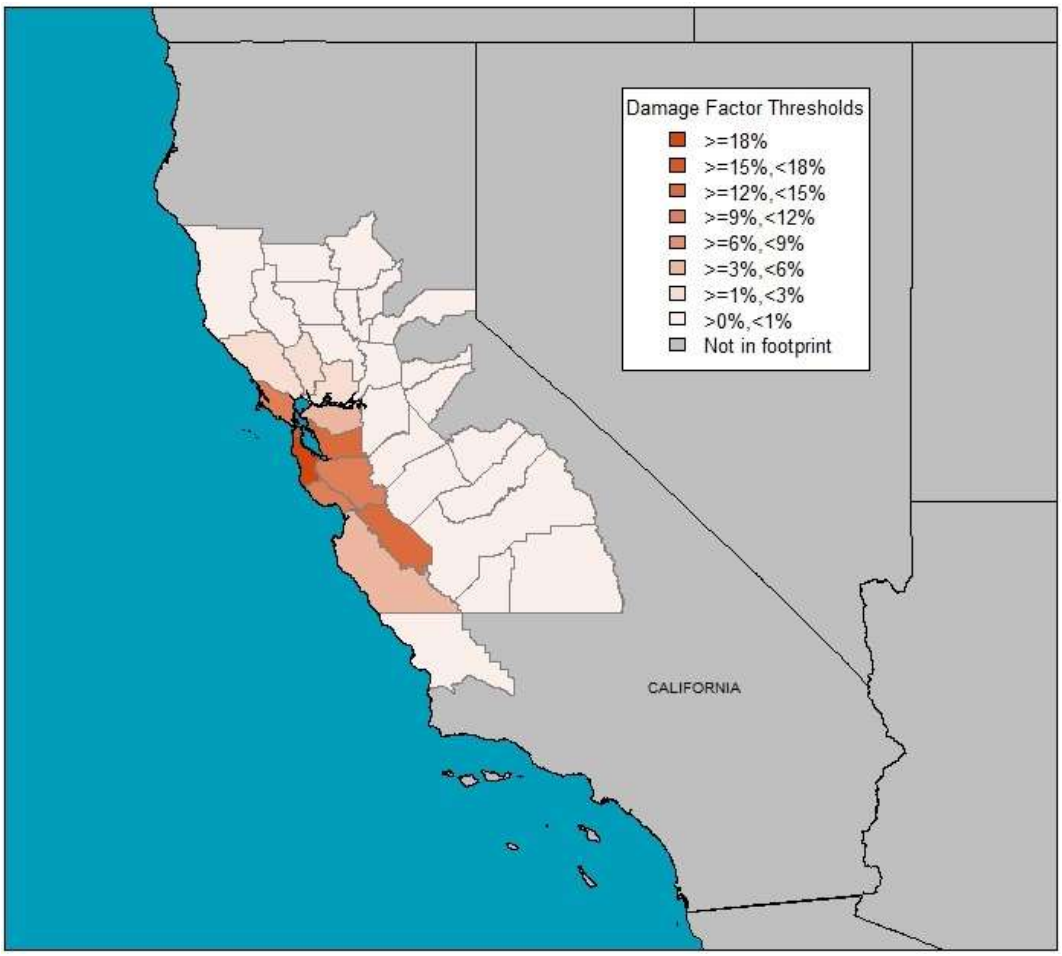
9 California Earthquake: San Francisco

9.1 Event definition

An earthquake causing major damage to San Francisco, from shake and fire-following, gross of take-up rates and including consideration of demand surge.

9.1.1 Event footprint

Map 9 illustrates the footprint and residential, ground-up shake damage levels for the San Francisco earthquake event.



Map 9

9.1.2 Industry Loss Levels

This event results in an estimated USD80bn Industry Property Loss (shake and fire following), *after* taking into account take-up rates but *before* applying policy terms. Demand surge is included. Managing agents should assume the following components of the loss:

Residential Property	$40.00bn
Commercial Property	$40.00bn
Workers Compensation	$5.50bn
Marine	$2.25bn
Personal Accident	$1.00bn
Auto	$1.00bn

Table 24

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Specie/Fine Art
2) Liability
3) Cancellation
4) PA and WCA losses – it should be assumed that there will be 2,000 deaths and 20,000 injuries as a result of the earthquake. Managing agents should assume that 50% of those injured will have PA cover.
5) Estimation of Aviation Hull losses – Lloyd's has commissioned research that indicates that minimal Aviation Hull losses would be expected to arise from an earthquake. Managing agents should take account of these findings in calculating syndicate loss estimates.

9.2 Exposure information

See section 8.2.

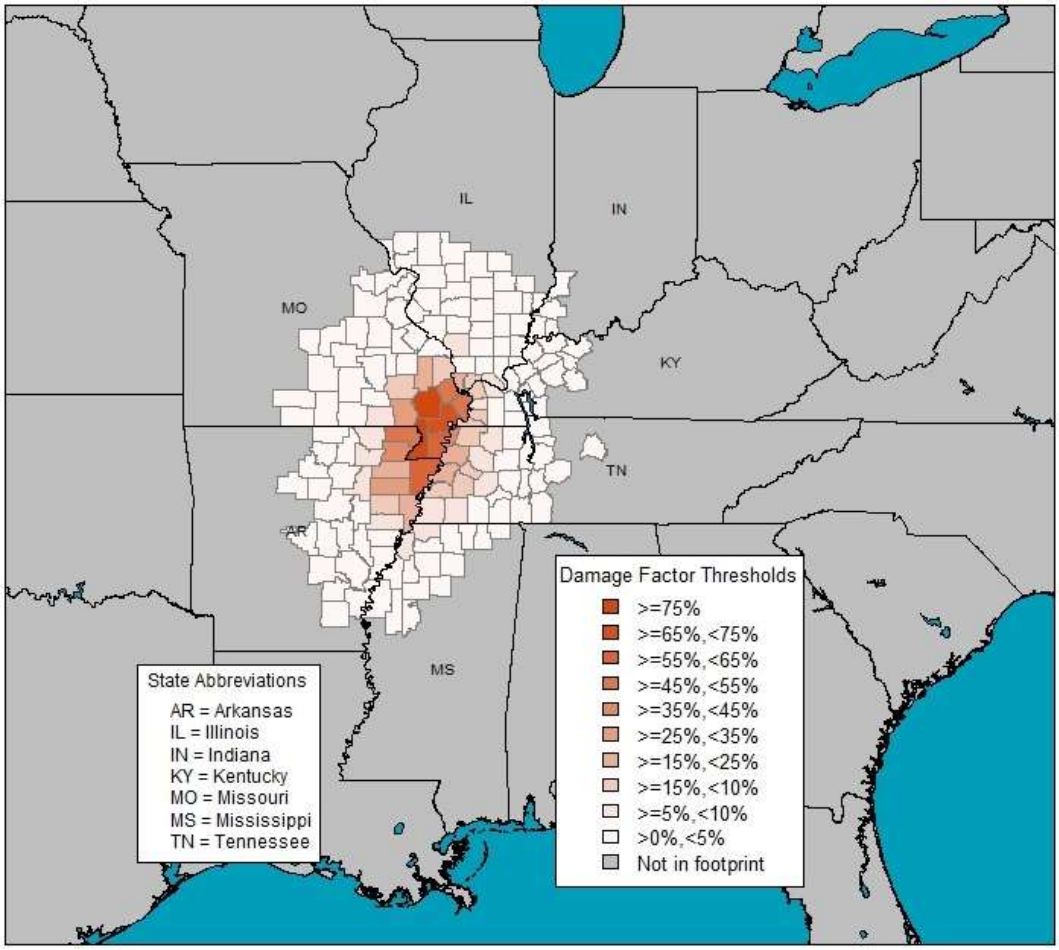
10 New Madrid earthquake

10.1 Event definition

An earthquake causing major damage within the New Madrid Seismic Zone ('NMSZ'), from shake and fire-following, gross of take-up rates and including consideration of demand surge.

10.1.1 Event footprint

Map 10 illustrates the footprint and residential, ground-up shake damage levels for the New Madrid earthquake event.



Map 10

Industry Loss Levels

This event results in an estimated USD44bn Industry Property Loss (shake and fire following), *after* taking into account take-up rates but *before* applying policy terms. Demand surge is included. Managing agents should assume the following components of the loss:

Residential Property	$30.50bn
Commercial Property	$13.50bn
Workers Compensation	$2.50bn
Marine	$1.50bn
Personal Accident	$0.50bn
Auto	$0.50bn

Table 25

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Specie/Fine Art
2) Liability
3) Cancellation
4) PA and WCA – it should be assumed that there will be 1,000 deaths and 10,000 injuries as a result of this earthquake. Managing agents should assume that 50% of those injured will have PA cover.
5) Aviation – Lloyd's has commissioned research that indicates that minimal Aviation Hull losses would be expected to arise from an earthquake. Managing agents should take account of these findings in calculating syndicate loss estimates.
6) Business Interruption – overland transport systems are severely damaged and business impacted, leading to significant business interruption exposure for a period of 30 days. This is restricted to the inner zone of maximum earthquake intensities (highlighted on the event footprint).

10.2 Exposure information

10.2.1 Property value distribution

Lloyd's assumptions for the distribution of property values are detailed in the RDS Damage Factors spreadsheet available from Lloyd's.

10.2.2 Major Ports

Table 26 lists the main ports in the NMSZ, which managing agents should consider in assessing syndicate potential exposures. They should also have regard to exposures in smaller ports that fall within the footprint of the events.

Port	County	State
Pascagoula	Jackson	Mississippi
Gulfport	Harrison	Mississippi
South Louisiana	St John the Baptist	Mississippi
Baton Rouge	West Baton Rouge	Louisiana
Mobile	Mobile	Alabama
Memphis	Shelby	Tennessee
St. Louis	St Louis	Missouri

Table 26

10.2.3 Major Airports

Table 27 lists the main domestic and international airports in the NMSZ, which managing agents should consider in assessing syndicate potential exposures. They should also have regard to exposures in smaller ports that fall within the footprint of the events.

Airport	County	State
Jonesboro Municipal	Craighead	Arkansas
Cape Girardeau Regional	Scott	Missouri
Barkley Regional	McCracken	Kentucky
McKellar-Sipes Regional	Madison	Tennessee
Memphis International	Shelby	Tennessee
Lambert-St Louis International	Saint Louis	Missouri

Table 27

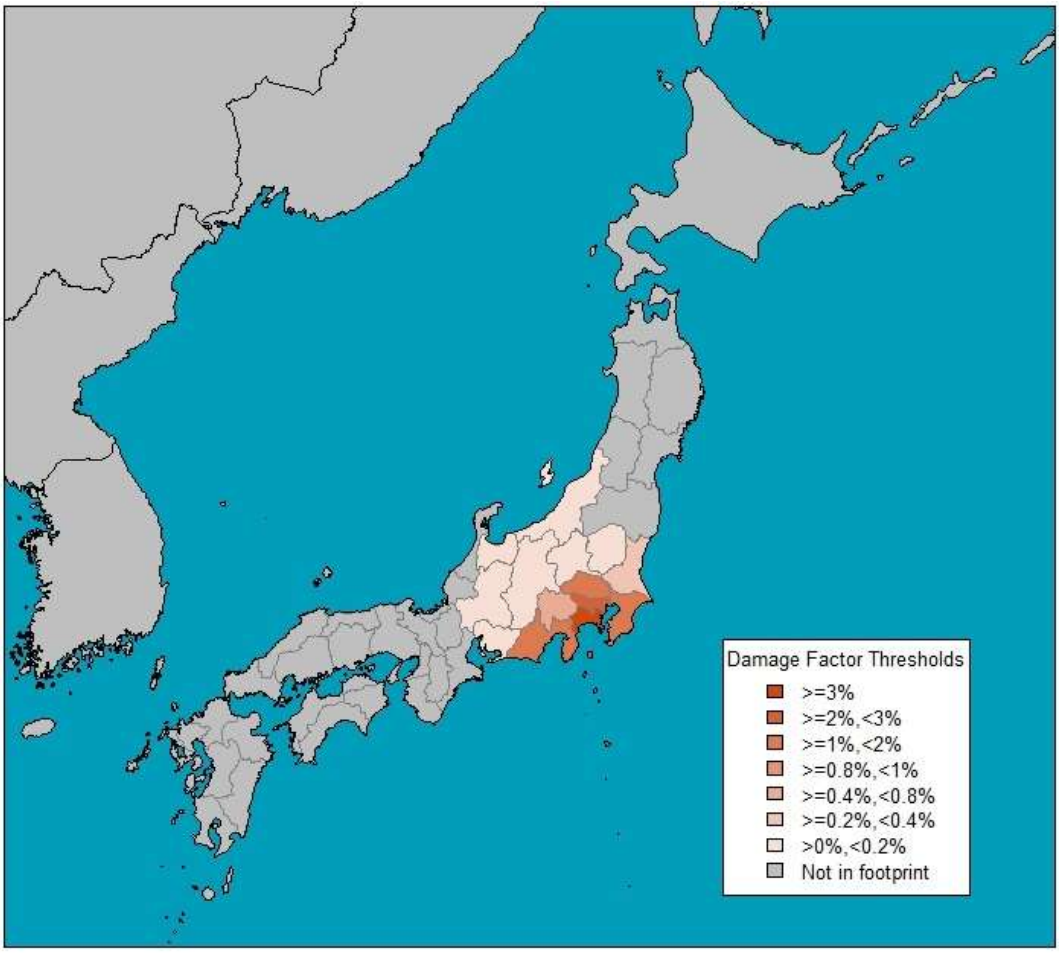
11 Japanese earthquake

11.1 Event definition

This event is based on the Great Kanto earthquake of 1923.

11.1.1 Event footprint

Map 11 illustrates the footprint and residential, shake only damage levels for Japan, which are detailed in the RDS Damage Factor Tables that are available from Lloyd's.



Map 11

11.1.2 Industry Loss Levels

This event results in a present-day Industry Property Loss estimate of ¥8trn. Managing agents should assume the following components of the loss:-

Residential Property	¥2.5trn
Commercial Property	¥5.5trn
Marine	¥150bn
Personal Accident	¥50bn

Table 28

Managing agents should consider all other lines of business that would be affected by the event. Particular consideration should be given to losses arising from:

1) Personal Accident - it should be assumed that 2,000 deaths and 20,000 injuries will arise as a result of this major earthquake. Assume that 50% of those injured will have PA cover.
2) Liability Business
3) Aviation - following research undertaken by Lloyd's, managing agents should assume that minimal Aviation Hull losses will arise from an earthquake of this magnitude.
4) Business Interruption - overland transport systems are severely damaged and businesses impacted, leading to significant business interruption exposure for a period of 60 days. This is restricted to the inner zone of maximum earthquake intensities (highlighted on Event footprint).

11.2 Exposure information

11.2.1 Property value distribution

Lloyd's assumptions for the distribution of property values at prefecture level are detailed in the RDS Damage Factors that are available from Lloyd's.

11.2.2 Major Ports

Table 29 lists the main ports in the Great Kanto footprint, which managing agents should consider in assessing syndicate potential exposures. They should also have regard to exposures in smaller ports that fall within the footprint of the event.

Port
Chiba Port
Nagoya Port
Yokohama Port
Kawasaki Port
Mizushima Port
Kitakyushu Port
Tokyo Port
Osaka Port
Tomakomai Port
Kobe Port

Table 29

11.2.3 Major Airports

Table 30 below lists the main international and domestic airports potentially impacted by the Great Kanto earthquake event, which managing agents should consider in assessing syndicate potential exposures. They should also have regard to exposures in smaller airports that fall within the footprint of the event.

Airport
Narita International Airport
Central Japan International Airport
Kansai International Airport
Tokyo International Airport
Osaka International Airport

Table 30

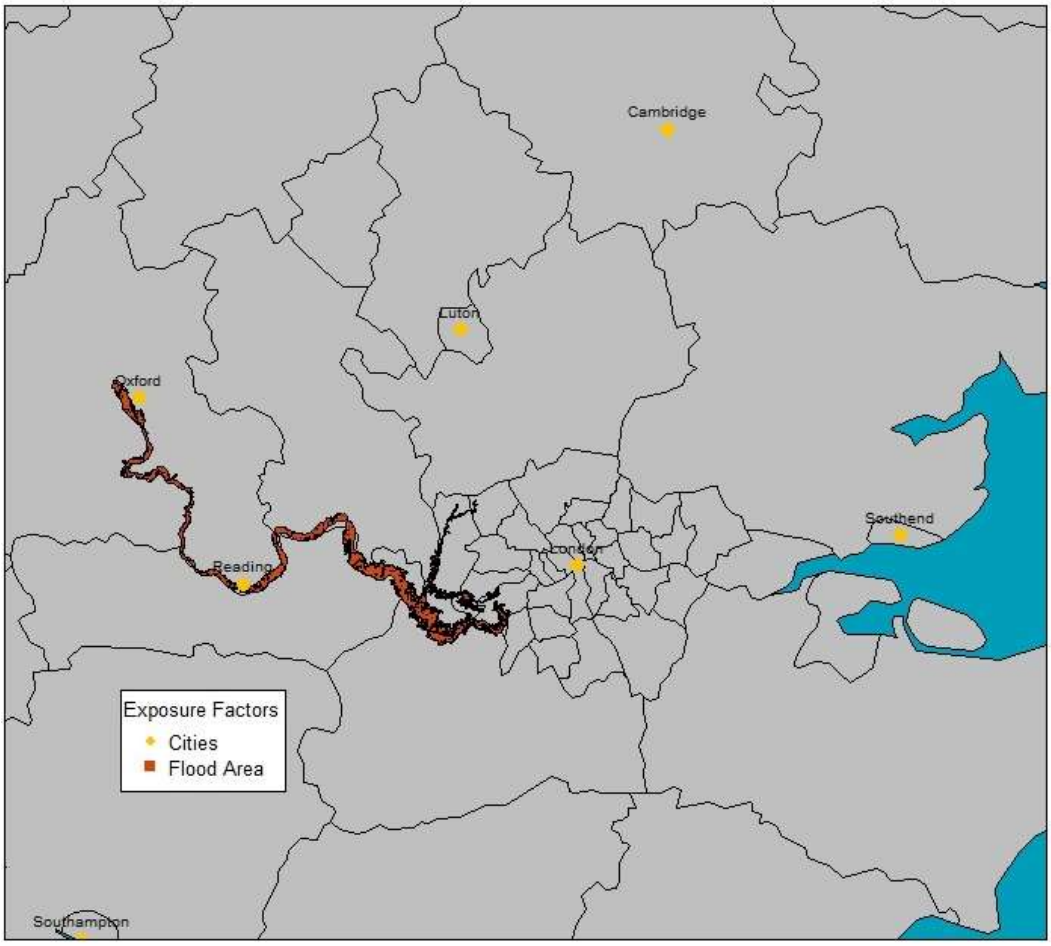
12 UK Flood

12.1 Event definition

This scenario is based on a heavy rainfall event moving from west to east across south east England resulting in extensive flooding of the River Thames from Oxford to Teddington with secondary flooding on the River Colne from Ruislip south and surface flooding on the western and southern edges of Heathrow. The total flood extent covers 194 km^2 and would cause significant impact on the major populated areas of Oxford, Reading, Slough, and the Henley areas of western London.

12.1.1 Event footprint

Map 12 illustrates the flood footprint for the UK flood event.



Map 12

12.1.2 Industry loss levels

This event results in an Industry Property Loss of £6.2bn. Managing agents should assume the following components of the loss:

Residential	£4.50bn
Commercial/Industrial	£1.60bn
Agriculture	£0.05bn
Motor	£0.05bn

Table 31

Managing agents should also consider other lines of business that may be affected by the event. Particular consideration should be given to the potential for losses arising from:

1) Cargo
2) Specie/Fine Art
3) Cancellation (Event \ Travel)

12.1.3 Event duration

Managing agents should assume that the flood event will not exceed 168 hours.

12.2 Other loss characteristics

12.2.1 Major roads

Table 32 lists the major roads within the flood footprint which managing agents should consider in assessing business interruption:

Major Roads
M25
M3
M4
A40
A34
A404
A437
A4180

Table 32

12.2.2 Major rail

Rail disruption will occur between London (Waterloo) and western services towards Oxford, Bristol, and Cardiff. There will be little disruption to the London Underground system except for flooding of Pinner station on the Metropolitan line.

12.2.3 Heathrow airport

Surface flooding will cause disruption to Heathrow Airport with flooding from the west encroaching into Terminal 5 and the end of both runways. Further flooding from the south will affect cargo transit and handling facilities.

12.2.4 Treatment of pollution

Managing agents are advised that pollution may follow the flood event. Although no specific details are provided here, managing agents should consider the impact and operation of Seepage and Pollution exclusions, and consider the impact of pollution as an aggravating factor in residential losses. Managing agents may wish to refer to historical analogues, including the Carlisle floods of 2005. The impact of pollutants should also be considered for indirect losses at London Heathrow airport. Liability associated with potential pollution episodes will be difficult to calculate and as such should not be included in managing agents' assumptions.

12.2.5 Contingent Business Interruption Losses

Wherever possible, managing agents should consider the potential for additional losses from Named Customer/Supplier extensions in respect of policies identified as sustaining direct losses. For the purpose of the RDS, the potential for CBI losses from policies not directly affected by the flood event can be discounted.

13 Terrorism: Rockefeller Center

13.1 Event definition

The Midtown Manhattan area, New York, at 11:00am on 1 January 2023 suffers a 2 tonne bomb blast attack causing:

Zone	Impact Description	Damage Zones	Property Damage	Fire Loss
1	Collapse and fire following	Inner zone, radius 200m	100%	10%
2	Massive debris damage to surrounding properties	400m radius	25%	2.5%
3	Light debris damage to surrounding properties	500m radius	10%	1%

Table 33

Radii measurements are taken from the Rockefeller Center as a reference point.

Figure 1

13.2 Loss characteristics

13.2.1 Number of Deaths and Injuries

1,000 blue/white collar worker deaths in total and 2,500 injuries in total. Managing agents to determine a worst case split across lines of business (WCA, PA, Group PA, etc.) and document assumptions using the commentary facility in CMR form 990. The following percentage split should be used for non-fatal injuries:

- 14% life threatening
- 35% moderate
- 51% minor

13.2.2 Business Interruption

Overland/underground transport systems are partially damaged, leading to significant business interruption exposure for a period of three months.

13.2.3 Affected Classes of Business

All possible affected business classes should be included in the calculations, such as Contingent Business Interruption and Specie/Fine Art.

13.2.4 Fire Following

Taking 'Fire Following' into consideration, managing agents should assume the same damage zones with the appropriate Fire Loss percentage applied. Managing agents should assume that all property policies are impacted, given the New York state ruling that property policies cannot exclude fire. Any assumptions concerning Fire-Following Terrorism are to be documented using CMR form 990.

13.2.5 'CBRN' Status

It should be assumed that there are no Chemical, Biological, Radiological or Nuclear hazard exposures arising from these events.

13.2.6 Granularity of Treaty Exposures

Syndicates with low resolution treaty exposure data should use a damage factor based upon claims experience from the World Trade Center attacks of 2001.

14 Terrorism: One World Trade Center

14.1 Event definition

The lower Manhattan area, New York, at 11:00am on 1 January 2023 suffers a 2 tonne bomb blast attack causing:

Zone	Impact Description	Damage Zones	Property Damage	Fire Loss
1	Collapse and fire following	Inner zone, radius 200m	100%	10%
2	Massive debris damage to surrounding properties	400m radius	25%	2.50%
3	Light debris damage to surrounding properties	500m radius	10%	1%

Table 34

Radii measurements are taken from One World Trade Center as a reference point.

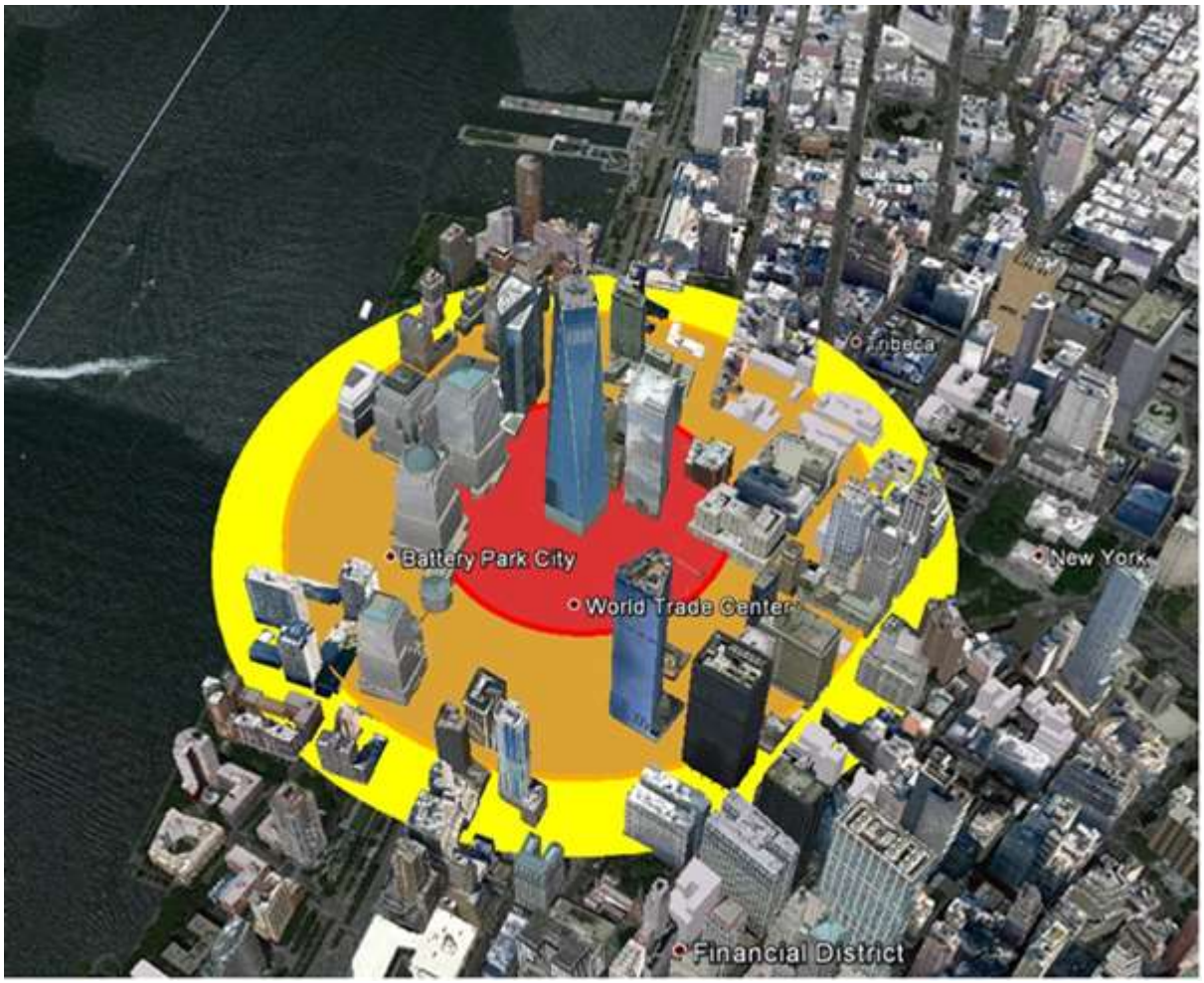


Figure 2

14.2 Loss characteristics

The loss characteristics for this event are the same as for Terrorism: Rockefeller Plaza. Please see section 13.2 above for details.

15 Alternative scenarios A & B

Managing agents should report two further realistic events that represent the most material accumulation risks that are not already covered by compulsory or *de minimis* scenarios.

Examples include:

1) Earthquakes other than those occurring in the US (California, New Madrid) and Japan – for example in China, Australia, South America, New Zealand;
2) A ‘Selby-type’ liability loss;
3) A major flood incident;
4) Accumulation of casualties to members of sports team
5) Caribbean/USA hurricane windstorm clash;
6) Pandemic risk;
7) Terrorism accumulations other than Manhattan;

16 Cyber - Major Data Security Breach

16.1 Event definition

A series of simultaneous cyber-attacks are launched on large multinational organisations across one industrial sector[1] with the intention of causing major disruption and financial loss to organisations. During the attacks, customer data (e.g. IP, credit card details and other information) is lost.

The attacks target vulnerabilities in the operating systems, web applications and/or software used by these organisations. For the purposes of this exercise it is assumed that multiple systems and/or multiple organisations using the same systems/software are affected.

The hacking attacks may take the form of a virus, or an alternative vector of attack.

For the purposes of this exercise it is assumed that multiple organisations across the world in one sector come under attack at the same time.

As a result of the breach, customer management and trading systems, networks and supply chains are disrupted at these organisations for a duration of 24 hours.

The organisations affected have adopted reasonable network security processes, including anti-virus software and patching.

16.2 Assumptions

Please assume that your ten largest clients (based on exposure to policies including cyber liability) worldwide are targeted, in the one sector where you expect to have the greatest exposure.

Please assume that all client data at these organisations is lost (i.e. assume total losses for your top ten companies). Please assume that class actions are pursued and you will face third party liability claims.

For reinsurance purposes please calculate separately on the basis that these attacks are deemed both as one event and as ten separate events, returning whichever causes the largest net loss.

16.3 Losses

What are your estimated losses (split out) taking into account the following lines of business: -

16.3.1 Cyber losses

- First party loss notification, associated costs and breach management costs, including crisis management
- Business Interruption (excl physical damage)
- Contingent business interruption
- Third party liability losses
- Regulatory defence, legal fees and fines covered amounts
- Other losses

16.3.2 Other losses

- Crime
- E&O policies with cyber endorsements
- Technology E&O
- D&O
- GL / failure to supply
- Other policies that may respond

1 i.e. relating to any sector you deem relevant, including financial, retail and healthcare

17 Lloyd’s “New” Cyber scenarios

17.1 Introduction

The purpose of this section is to describe in summary the specifications for each of Lloyd’s three “new” Cyber scenarios.

Lloyd’s recognises that cyber-attacks can cause a wide variety of types of loss and these scenarios are designed to impact business written across the breadth of the Lloyd’s market.

Lloyd’s is interested in testing the level of loss that could arise should the scenarios occur. The plausibility of these scenarios must be tested in the future; at this stage, the tests should be carried out assuming the events have occurred.

Lloyd’s reserves the right to test extreme losses without commenting on their likelihood or indeed whether they can arise at all.

The tests should be carried out assuming that none of the events are classified as acts of War.

Lloyd’s prescribed Cyber scenarios for data collection are:

1. Business Blackout II
2. Cloud Cascade
3. Ransomware Contagion

A technical specification document and calculation template accompany each scenario listed within this document.

These have been produced by Guy Carpenter and CyberCube jointly.

Please note that the document in question is the property of Lloyd's and is strictly private and confidential to managing agents.

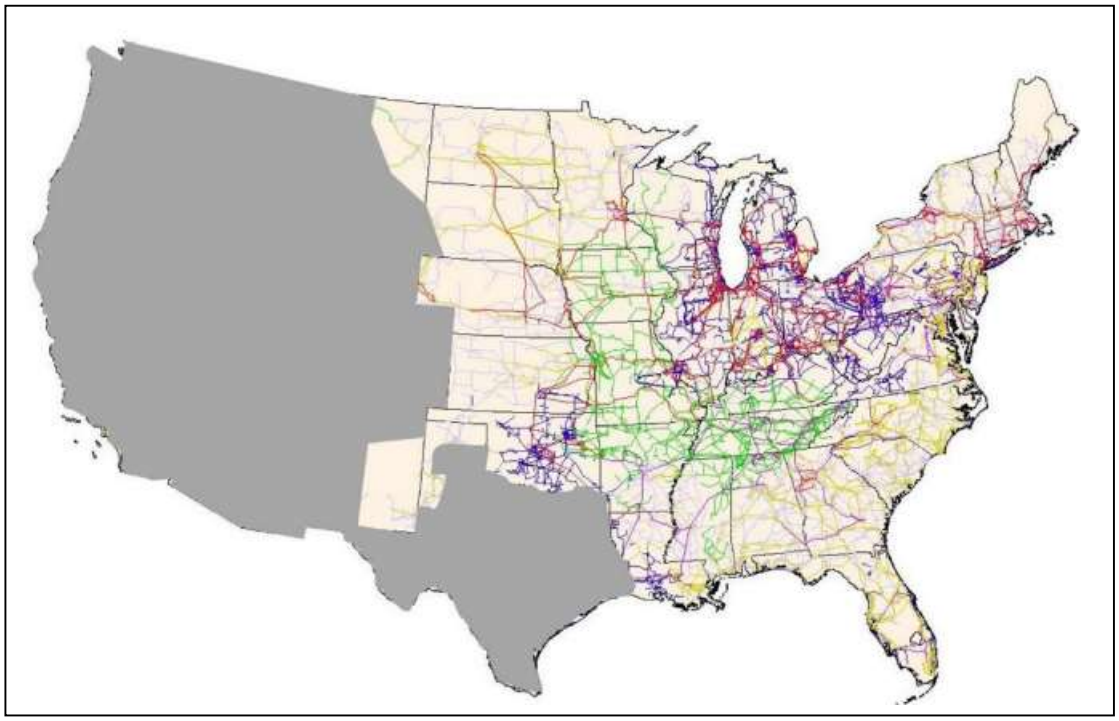
Lloyd’s has also provided a calculation template and detailed technical specification for each scenario. All other Cyber-related reporting requirements remain unchanged.

For further information about the scenarios, please contact Lloyd’s Exposure Management.

17.2 Business Blackout II

17.2.1 Event Description

On a weekday in June, the lights go out in 36 States (1) of the USA. Homes and businesses in dispersed areas report power cuts, and it becomes apparent that a cascading outage is sweeping the Eastern United States. The outage is not total, however, and some areas are unaffected as existing infrastructure technology mitigates the spread, and responders work to contain the impact. Power is gradually restored to the affected areas, with 50% restored after three days. This timeline was determined given the widespread geographical scope of the blackout while still taking into consideration past electricity restoration processes after major disruption events in the US. Full restoration occurs three weeks after the initial outage. The disruption originates with transmission infrastructure. This means that grid electricity transmission and distribution systems are severely disrupted, and impacts are felt across all 36 States of the connected transmission infrastructure of the Eastern Interconnection, with some regions suffering more extensive outages than others. Even undamaged substations across the region are shut down until the cause of the damage can be understood.



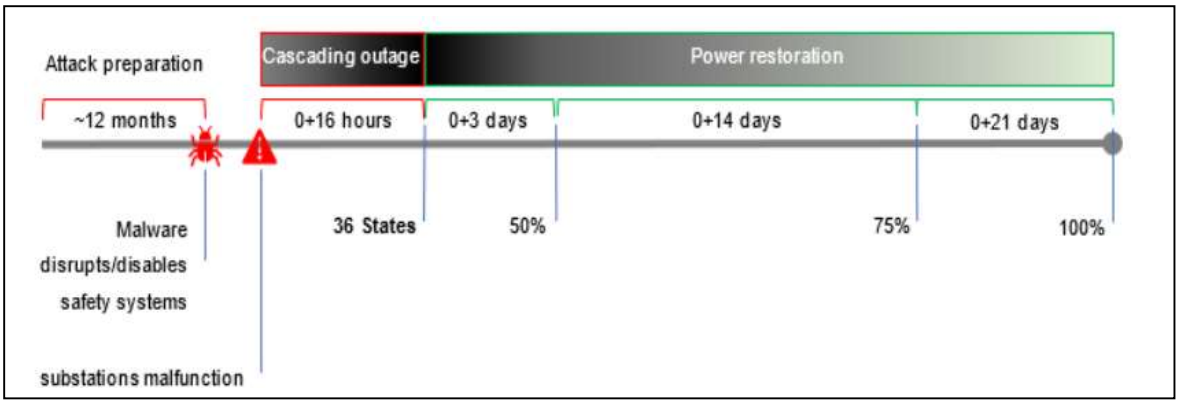
The Eastern Interconnection region with major power transmission lines

Investigation reveals that the outage was caused by a sophisticated cyber-attack, which had successfully targeted electrical substations housing power transformers in the Eastern Interconnection region. The sophistication of the attack leads to suspicion falling on several threat actor groups linked to Nation States; nevertheless, no group claims responsibility and attribution is not definitively established.

(1) Plus Washington DC. The Eastern Interconnection also incorporates small parts of an additional 3 States, but these do not include any metropolitan/industrial areas.

17.2.2 Detailed narrative

The timeline of the event is shown below:



17.2.3 Threat Actor

An attack of this nature requires highly sophisticated expertise across a range of disciplines, together with significant resources. The motivation of such an attack would be to inflict major disruption to the USA (economic, social, and political). It is plausible that a sophisticated actor would engage the assistance of the hacking community and purchase the services of skilled programmers who are knowledgeable of how to reverse engineer and penetrate vulnerabilities in the US domestic electricity sector and grid systems. This combination of capability and motive means it is likely that such an attack would be perpetrated by an actor able to call on the support of a Nation State, but this does not imply that the attack could definitively be attributed to a given Nation State. The ability of insurers to claim this event as an Act of War is therefore limited.

17.2.4 Threat vector

A sophisticated actor would enforce effective operational security, meaning that hired hackers would have very little idea of what they were working on as a collective. They would conduct months of research and reconnaissance focused on the US electricity markets, control systems and networks. Once they had identified critical information flows, networks, devices and companies, they would design bespoke malware designed to disable safety systems within substations which would usually protect the power transformers from ‘desynchronization’ events. The team would employ a range of tactics in their attempt to penetrate the security protecting the electrical grid. Not all the deployed malware attack attempts would be successful, owing to the range of variables affecting success against a given substation target. The malware has the capability to propagate within the transmission infrastructure, and in the scenario the malware successfully penetrates enough substations to generate a cascading power outage.

17.2.5 Precedents

The scenario uses the 2003 ‘Northeast blackout’ as a baseline for assessing the duration and footprint of a realistic disaster. A further reference point is the power outage and restoration rates following Superstorm Sandy in 2011. Cyber-attacks against Ukrainian power companies in 2015 and 2016 demonstrated the potential for hostile actors to successfully target the industrial control systems of power distribution utilities, causing widespread power outages. Threat intelligence points to a credible threat of cyber-attack against power infrastructure worldwide and specifically in the USA; see for example ‘Cyber Threat and Vulnerability Analysis of the US Electric Sector’ published by the Idaho National Laboratory.

17.2.6 Plausibility

The 2003 ‘Northeast blackout’ is used as a baseline for assessing how realistic an attack of this nature on transmission and distribution can be. Lessons learned from the 2003 blackout not only indicate that transmission and distribution is a major vulnerability in the security of the US electricity system, but also assist in the understanding of how easily cascading blackouts can spread across the US grid

infrastructure. Note that a “cascading event” on the grid’s transmission and distribution system refers to a power outage event that originates at the targeted infrastructure (select substations) and spreads across the grid for a duration of time, leading to power outages as it spreads. During a cascading event, automated and manual communication between grid operators across states and utilities may be disrupted, preventing the ability to mitigate the spread of an outage.

The 2003 blackout involved a combination of human and technical error, starting with software problems, followed by physical and computer equipment failures, with these issues then being exacerbated by human error in failing to recognize the appropriate course of remediation. From such initial human and technical failures, cascading blackouts can then spread across the Eastern grid system, with voltage surges leading to physical damage to the lines as well: as load increases, the lines heat up and sag, getting too close or touching tree overgrowth, causing the lines to trip and fail. Due to contact with trees, a critical transmission route fails, leading to voltage surges, lags, and ultimately cascading failures across the 36-state Eastern interconnected grid system.

Electricity transmission across the US is heavily interconnected and thus interdependent, with transmission operators working together to communicate, coordinate and move power across the country. However, the electrical grid in the US is constructed in three separate regions: Western, Eastern, and Texas. The blackout does not cascade into the Western or Texan grid Interconnection systems due to the physical structure of the United States electrical grid system, as the three grid interconnects are disconnected from each other with only limited shared connections for power transfers. While this attack is limited to the Eastern Interconnect region, this region is by far the largest, encompassing major infrastructure sectors vital for economic activity across the country. An outage of this scope (three days for 50% restoration and three weeks for full restoration) is extreme but not unrealistic, especially when considering the duration of electricity outages caused by major natural disasters (such as Superstorm Sandy) and the vast geographical region being impacted in the event.

The historical parallels of the Ukrainian grid attacks in 2015 and 2016 serve as an indicator that with an organized and well-funded group behind the attack, the initial malware can go undetected for months, even after being deployed to explore the utility’s industrial controls.Past evidence from targeted campaigns against electricity infrastructure (in Ukraine and elsewhere) indicate that attackers can enter operator systems via initial access methods such as credential-stealing, phishing, drive-by download, social engineering, etc. From there, attackers can use tools to scan, map, and find vulnerabilities within the network of interest to target. This level of access allows the disruptions to cascade further across grid infrastructure, causing disruptive and confusing communication between equipment and operators.

The return period of this scenario is estimated to be between 1 in 150 and 1 in 200 years.

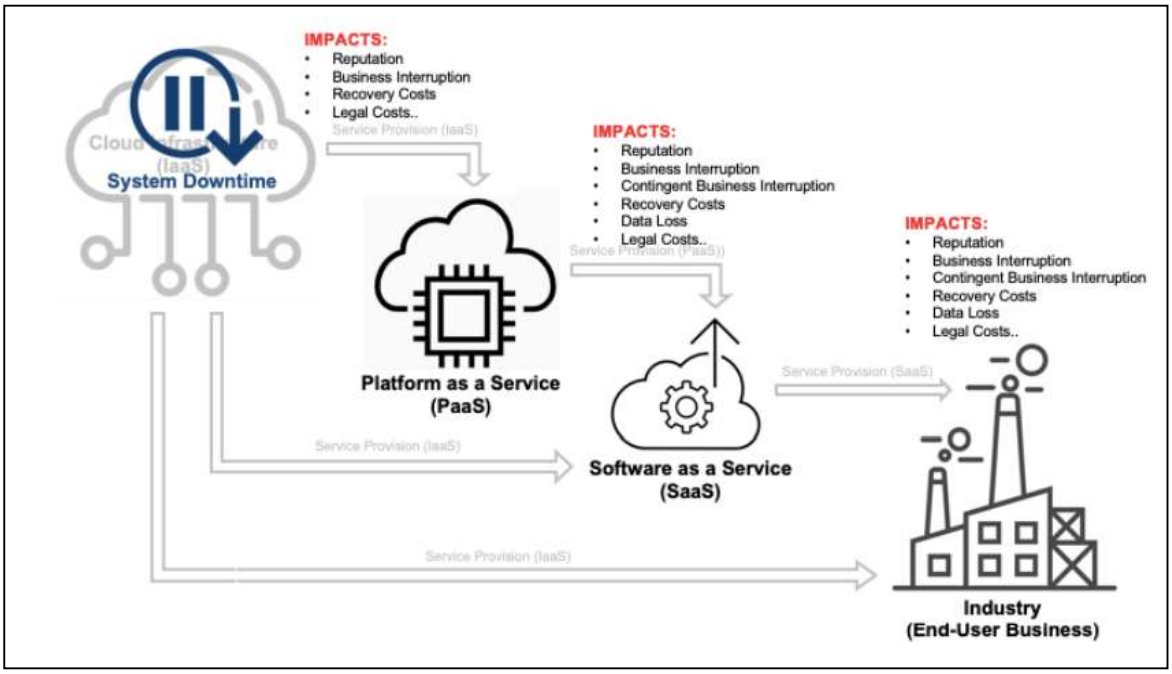
The key compounding assumptions that contribute to this estimated likelihood are:

- 36 States plus Washington D.C. impacted – This considers that every US state in the Eastern Interconnect is impacted, so is at the extreme end for this scenario. This could however be amplified if the attack region extended into Canada, to round out the full extent of the Eastern Interconnect’s reach. Doing so would increase the economic loss, while only moderately increasing the estimated return period. However, the US region was chosen to focus on the market exposure concentration.
- 16-hour cascading outage – This preliminary cascading outage duration was chosen as a moderate duration and not extreme for an outage given precedent of past cascading outages that can occur before remediation efforts take effect. This outage period could be extended to 24 hours, but this lessens the likelihood as utility workers, system operators, and other responders would have been assembled and deployed to actively try to mitigate the cascade in this event, and this would require additional outside factors (dangerous weather conditions etc.) to compound the effect.
- 21-days of restoration – This total downtime reflects the more extreme period of recovery for the grid after considering past cascading outages, blackouts, and electricity disruptions in the US. Increasing this assumption would significantly exacerbate the return period for this scenario.
- 50% power restoration after 3 days – This 3-day restoration period whereby 50% of power is restored is utilized based on past extreme events in the US previously cited. The initial and partial restoration for electricity availability is most rapid in the first few days, and then declines as more nuanced recovery efforts take place.

17.3 Cloud Cascade

17.3.1 Event Description

A major cloud service provider (CSP) suffers total system down-time in multiple datacentres located in the USA. The outage lasts for 48 hours and impacts all hosted services, cascading across infrastructure, platforms and software. Businesses around the world suffer business interruption and data loss, among other impacts. Investigation shows that the outage was triggered by misconfigured cluster management software and exacerbated by malicious code.



A ‘cascading cloud failure’ showing the effect of infrastructure failure on dependent services

17.3.2 Detailed narrative

On 20th December, a major cloud service provider (CSP) operating in multiple US regions experiences system down-time and elevated packet loss (as a result of network congestion) for a duration of 48 hours. Cloud platform and application services from various providers and dependent on the cloud service providers’ US network are also impacted. Customers experience increased latency, intermittent errors, and connectivity loss to instances in multiple datacentres across the western, central and eastern regions of the US. These locations account for 70% of the CSP customers’ global workloads and cloud applications. Core infrastructure services (IaaS) are affected until mitigation is completed for each region (representing up to a 2-day outage in some cases). Cloud platform services (PaaS) and cloud software services (SaaS) from several major providers that rely on the impacted cloud infrastructure experience significant disruption. End users experience data loss and business interruption. Business impacts are felt particularly heavily by online retailers due to the proximity of the outage to the Christmas holiday period.

17.3.3 Threat Actor

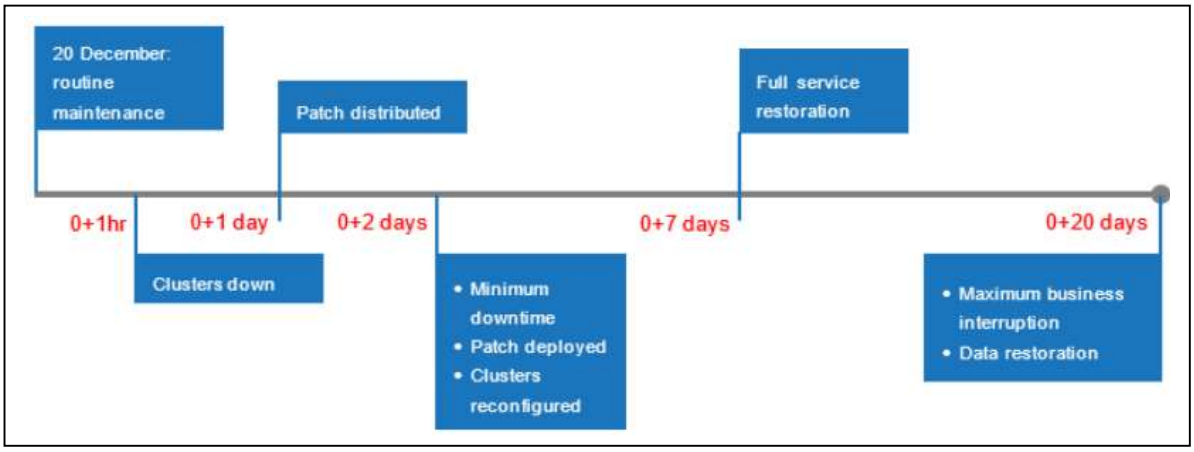
The malicious code design and delivery necessary for this scenario is not highly sophisticated. It is aligned to the capability and motives of several categories of threat actor, including organised criminal groups, hacktivists, insiders and nation states. These actors often operate in combination, and we assess that this scenario would most likely be executed by sophisticated hackers in combination with malicious and non-malicious insiders.

17.3.4 Threat Vector

The outage is caused by a coincidence of malicious code and human error in the Cluster Management System (CMS). • Malicious code. This could plausibly enter the CMS via a number of routes; one particularly common route is via a 'software supply chain' attack. The malicious code has the effect of increasing the severity of the event by causing 'ungraceful' shutdown of the CSP clusters. It is also a key factor in extending the outage to 48 hours, owing to the need for investigation and remediation. • Misconfigured CMS. The outage spreads across multiple datacentres because of human error in the coding of the CMS management of maintenance tasks. This causes the CMS to effectively 'transmit' the shutdown across datacentres during scheduled maintenance.

17.3.5 Duration of event

The timeline of the event is shown below:



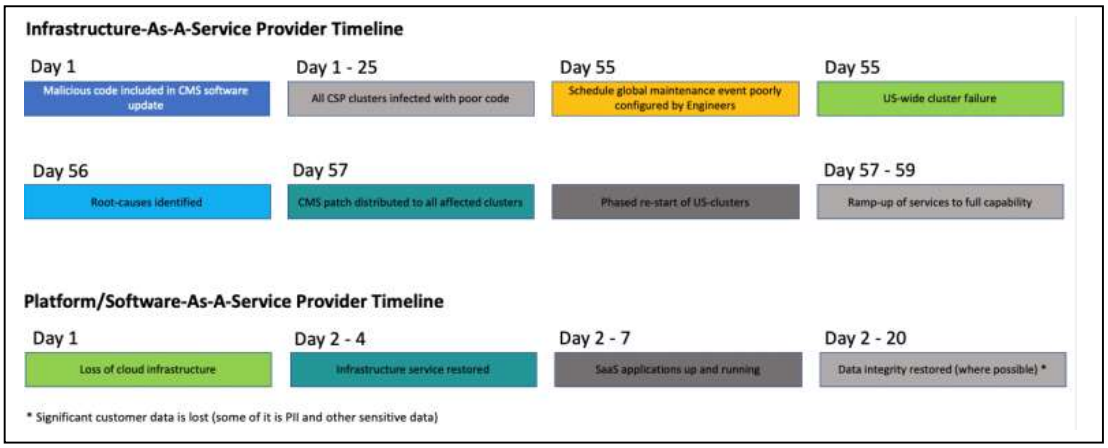
Investigation shows that the outage was caused by a combination of malicious code and human error affecting the CSP CMS. This had the effect of transmitting the outage across multiple datacentres during scheduled maintenance.

Initial Impact: the outage of 48 hours is an extreme event. By comparison, the 2019 Google Cloud outage lasted 4 hours. The severity of this scenario derives from the addition of a hostile actor: well-written, malicious code can severely disrupt online systems and confuse those struggling to find a root-cause, leading to long outages.

Effect on customers: despite the CSP restoring systems within 48 hours, some companies experience up to 20 days of disruption as their application and platform providers are unable to provide service and they suffer data corruptions caused by "ungraceful" system shutdowns and abrupt application failure.

- The root-cause (cloud infrastructure failure) has precedents (as cited earlier), and cloud independence and dependence research confirms that this scenario is realistic.
- Ungraceful system shutdown has often been seen to corrupt data. The nature of a Cluster Management Software failure through malicious attack would mean that many systems (both within the CSP's data centres and as part of SaaS providers estates) could fail "ungracefully". Systems unexpectedly shutting down can corrupt data where live transactions are occurring at the point of shutdown; this is sometimes referred to as a "dirty shutdown".
- Another source of potential data loss/corruption would be the sudden failure of SaaS applications due to catastrophic loss of cloud infrastructure. SaaS application failure of this kind has been seen in the past.

Cascading timeline: infrastructure – platform/software: the scenario models both the impact of 48 hours of downtime from a major CSP and the "knock-on" effect of this to SaaS and Platform (PaaS) providers and their clients. A web of interdependencies now exists between various CSPs and application (SaaS) providers as well as between end-user organisations and the applications that they rely on. The following graphic shows the length of occurrence in each of these contexts. The actual "downtime" experienced by customers starts on day 55 here:



Speed of response: the impact to businesses in the cloud value chain varies according to their speed of response. The assumptions for the major categories of businesses impacted are detailed below.

- CSP: responds quickly but struggles to find a root-cause within 24-hours as network latency issues hamper engineers' ability to query systems. In addition, malicious code within CMS is not expected and so some time passes before the malicious code is recognised and resolved with a global rollout of "clean" CMS code. Rollout of new code, configurations and subsequent restoration of all systems takes a further 24 hrs. This adds up to 48 hrs in total downtime. Key response actions required are to:
  - rollback system configurations to "clean" version of CMS code
  - reconfigure CMS clusters to working state
  - restore backups, where necessary
  - bring systems online, with consideration for interdependencies
  - ensure data integrity

- SaaS/PaaS provider: variance in response times and impacts, based on overall reliance on the CSP and on ability to restore services once CSP infrastructure is back online. Range of between 48 hours and 7 days of disruption. Key response actions required are to:
  - restore backups, where necessary
  - bring systems online, with consideration for interdependencies
  - ensure data integrity

- End-user businesses: variance in response times and impacts, based on overall reliance on the SaaS and on ability to restore data once SaaS application are back online. Range of between 48 hours and 20 days of disruption. Key response actions required are to:
  - restore backups, where necessary
  - bring systems online, with consideration for interdependencies
  - ensure data integrity

17.3.6 Precedents

The scenario has similarity to an event that affected Google Cloud in 2019. Google's willingness to share the detail of the event provides the basis for lessons to be learned and for improved risk management around the world.

17.3.7 Plausibility

The cloud cascade scenario is based, at its core, on a well-documented outage at Google in 2019. That outage was important in the context of building a narrative here for several reasons. Firstly, the outage proved categorically that a major cloud services provider can experience a systematic issue which takes down multiple data centres as part of one outage event. Secondly, the outage showed that, as is often the case in such instances, multiple failures can combine to amplify the impact of an outage (in Google's case, the failures were associated with human error combined with a software bug). It is very often not one issue that serves to cause an IT failure but several combining factors. Thirdly, the Google event demonstrated a common configuration factor that, when mis-configured, could cause major disruption, again across multiple sites. This was the Cluster Management Software referenced in our narrative.

This scenario is brought into the realm of 'disaster' by further exacerbating certain underpinning elements. In particular, the project team introduced a piece of malicious code into the narrative that deliberately causes the CMS software to shut systems down in an ungraceful fashion. This is important to the narrative for two reasons:

- Firstly, a piece of malicious code (introduced here through a software supply chain attack) would be unexpected by the cloud service provider and consequently harder to trace.
- Secondly, the deliberate "crashing" of systems and applications by the actor would cause more damage to data than if the CMS software were to shut systems down in a proper fashion.

The deliberate and malicious crashing of hundreds of systems would most likely lead to extended disruptions to the cloud eco-system, not least because these ungraceful shutdowns have been seen in the past to severely corrupt data and application configuration files, causing extended downtime and data loss. An additional justification to the 48 hours of downtime experienced by the cloud service provider in this scenario comes, once again, from documentation associated with the 2019 Google outage and several other outages experienced by cloud service providers. This is related to the network packet loss and bandwidth issues that tend to be experienced by the cloud provider when major systems fail. Significant extra demand on internal networks (caused largely by increased customer demand on certain locations) means that system operators find it very difficult to communicate with one another and to diagnose problems due to slow network and systems access.

The return period of this scenario is estimated to be between 1 in 100 and 1 in 125 years.

The key compounding assumptions of the scenario that contribute to this estimated likelihood are:

- CSP 48-hour downtime – The designated 48 hours is reasonable based on both precedent and expert judgment of response time. This downtime could be amplified to 7 days based on additional extenuating circumstances such as availability and other disruptions to staff trying to fix the issue, however, that would dramatically decrease the likelihood of the overall event.
- SaaS Provider 7-day downtime – This downtime is at the more extreme end for a SaaS provider as it ensures data integrity while restoring its systems on its infrastructure dependency. Extending this downtime would dramatically increase the return period, given lack of past precedent.
- End-User 20-day downtime – This downtime is dependent upon the range of downtime for the SaaS provider that an end-user is relying upon, and the end-user's dependency on that provider. This range considers a wide range of SaaS providers, but not an exhaustive list, and reflects the above return period. This downtime could be extended, but in order to reach a 30-day range or longer, it would pull this scenario beyond the targeted return period given the other assumptions about the outage and ability for a given company to respond.
- US Data Centres IaaS Geography – The specific regions chosen in the US are representative of the current status of data centre proximity and configuration for Infrastructure as a Service providers and demonstrates the inherent ability to impact US data centre regions for a given IaaS, and no other geographies.

17.4 Ransomware Contagion

17.4.1 Event Description

At 08:00 GMT a ransomware payload triggers. It has exploited a vulnerability in an operating system (OS) to infect the IT network of a major global corporation. The Ransomware encrypts files and presents users with a ransom demand. The OS has a dominant market share, and over the next 3 days the ransomware spreads all around the world. On average, victims experience 7 days of system downtime.

The OS provider issues a patch to the vulnerability, but the ransomware is already affecting companies around the world. Organisations in every sector are unable to access critical files and many victims pay the ransom. However, due to faults and errors in the decryption code, most victims are unable to restore their systems even after ransom is paid. Victims suffer business interruption and costs including data restoration and hardware replacement.

17.4.2 Threat Actor

An attack of this nature would require significant planning, funding and engineering effort. Nevertheless, access to the necessary capabilities is becoming easier, and several threat actor groups have the necessary capability and motive. Recent surveys have suggested that cyber-attacks aimed at destruction or disruption – as opposed to financial gain – are an increasing threat.

It is also plausible that more than one actor could be involved. Combinations of state actors and criminal gangs, activists and malicious insiders are common and any combination of these could be responsible for an attack of this nature. It is most likely that this scenario would be orchestrated by an actor linked to a Nation State (such as the Lazarus Group) but with the possible involvement of criminals or insiders.

17.4.3 Threat vector

The malware propagates in a similar way to that seen in the NotPetya and WannaCry attacks: it is designed to exploit a ‘zero-day’ vulnerability in an OS, and even though a patch is issued, variable patching practices means that the malware is able to penetrate many of the systems it finds.

The WannaCry ransomware was curtailed by the discovery of a ‘kill switch’ (this was a web address that the malware would check automatically; when a researcher discovered the address and registered the domain as his, the malware stopped further activity). This feature is assessed to be an anomaly that would not be repeated by sophisticated threat actors. WannaCry also contained errors which allowed some files to be recovered even without a decryption key.

17.4.4 Duration of event

Initial Impact: NotPetya and WannaCry demonstrated the potency of destructive, self-replicating malware and the effects it can have on a broad array of companies relying on a particular Operating System.

The scenario uses historical attacks as a baseline and gives them greater potency through the application of other, feasible technique attributes (such as use of a ‘zero-day’ vulnerability and the use of well-structured code). In the scenario, the malware proliferates rapidly with an initial infection phase of 8 hours. The dominant market share of the OS allows the malware to reach almost every country in the world, mirroring the impact of WannaCry, which reached over 150 countries in the first stage of infection. The malware then continues to spread at slower pace over 3 days. System downtime: in the scenario, victims experience an average 7 days of system downtime. This is a conservative average estimate based on more common historical examples.

17.4.5 Precedents

The scenario is similar to the WannaCry ransomware and NotPetya malware attacks of 2017. The threats and vulnerabilities described are also based on current intelligence and actual events.

17.4.6 Plausibility

The ransomware scenario is based on the WannaCry and NotPetya events which shook the world in 2017. While this scenario is based on these precedents, it is brought into the realm of ‘disaster’ by further

exacerbating certain elements of each. For instance, WannaCry would have been more disastrous if the malware code was more carefully developed. In actuality the attack failed, in many cases, to successfully collect ransoms and the code was susceptible to a “kill-switch”, discovered by an amateur hacker in the UK who successfully disabled it with a simple internet domain registration. This scenario assumes a high degree of maturity in the software coding and testing procedures associated.

Additionally, the ransomware scenario specifies the use of a zero-day vulnerability which, by its very nature, means a patch does not exist when criminals first leverage the vulnerability. This means that the attackers are able to take advantage of a window of opportunity and hone their attack methods as well as exploit the fact that (even in the event that the OS provider has discovered and patched the new vulnerability at the point of outbreak) many systems will remain unpatched during the timeline of the attack. This typically leads to high infection rates (as seen in this scenario) and was illustrated during the WannaCry outbreak where the zero-day vulnerability used by criminals had been patched by Microsoft for several months but many systems were not updated with the patches provided.

The average downtime of 7 days for any given company is plausible as an average assumption, but much longer periods of interruption have been experienced by individual companies, including as a result of the NotPetya attack.

The return period of this scenario is estimated to be between 1 in 75 and 1 in 100 years.

The key compounding assumptions of the scenario that contribute to this estimated likelihood are:

- 8 Hour Initial Infection – This infection rate reflects the speed by which malware of this sophistication can infect organizations and is demonstrated via past precedent. This initial infection rate is unlikely to be shortened, as evidenced by attacks seen thus far.
- Spread over 3 days – This period reflects the rapid mobilization of the malware and how quickly it can reach companies globally. This period could be extended to 4 or 5 days, however at that point awareness increases and so the impact of the malware begins to diminish.
- Flaws in Decryption Code –This assumption could be modified to suggest that the decryption code works. This would, however, alter the average downtime companies experience globally and the overall industry losses, as companies would be able to more rapidly recover their systems, thus reducing the return period.
- Global Malware – This assumption was chosen based on expanding upon past precedent. Decreasing the footprint to a much more focused and concentrated area would shorten the expected return period. However, changes to the footprint (such as stating that this will only impact North America and Europe) would not produce a realistic outcome. This overall assumption is demonstrative of the overall impacts seen globally by vulnerabilities in ubiquitous operating systems.

Scenarios subject to de minimis reporting

18 Marine scenarios

Managing agents should return a marine loss scenario for both of the following incidents. In both scenarios, excess layers of liability, hull and cargo should be included, based on maximum Aggregate exposures.

Please note that for both scenarios, liability costs exceed the coverage afforded by the International Group Programme. Please consider any other covers in force at 1st January 2023 that may be impacted, both Marine and Non-Marine, e.g. Personal Accident and D&O.

18.1 Scenario 1 - Marine Collision in US waters

A cruise vessel carrying 2,000 passengers and 800 staff and crew is involved in a high energy collision with a fully laden tanker of greater than 50,000 DWT with 20 crew.

The incident involves the tanker sinking and spilling its cargo; there are injuries and loss of lives aboard both vessels.

Assume 30% tanker owner/70% cruise vessel apportionment of negligence, and that the collision occurs in US waters.

Assume that the cost of pollution clean-up and compensation fund amounts to USD2bn. This would result in claims against the International Group of P&I Associations' General Excess of Loss Reinsurance Programme, and any other covers that might be in force.

Assume an additional compensation to all passengers and crew for death, injury or other costs of USD1.15bn and removal of wreck for the Tanker of USD100m. The cruise ship is severely damaged but is towed back to a safe harbour (repair estimate USD50m and USD10m for salvage operations).

18.2 Scenario 2 - Major Cruise Vessel Incident

A US owned cruise vessel carrying 4,000 passengers and 1,500 staff and crew is sunk with attendant loss of life, bodily injury, trauma and loss of possessions.

Assume a final settlement of USD3.2bn for all deaths, injuries and other associated costs. In addition, assume an additional Protection and Indemnity loss of USD1.15bn to cover removal of wreck and USD75m for Pollution.

19 Loss of major complex

Assume a total loss to all platforms and bridge links of a major complex.

Include property damage, removal of wreckage, liabilities, loss of production income and capping of well.

Managing agents should use the commentary facility in form 990 (supplementary scenario information) to name the complex and to provide details of modelling assumptions. Should a mobile drilling rig present potential material exposure to a syndicate, managing agents may wish to report this under the Alternative A or B scenario.

20 Aviation collision

Assume a collision between two aircraft over a major city, anywhere in the world, using the syndicate's two highest airline exposures. Assume a total liability loss of up to USD4bn: comprising up to USD2bn per airline and any balance up to USD1bn from a major product manufacturer's product liability policy(ies) and/or an air traffic control liability policy(ies), where applicable.

Consideration should be given to other exposures on the ground.

Assumptions should be stated clearly using the event commentary facility in form 990.

Managing agents should include the following information in their return;

1) the city over which the collision occurs;
2) the airlines involved in the collision;
3) the airlines policy limits and syndicate's line and exposure per policy;
4) maximum hull value per aircraft involved
5) maximum liability per aircraft involved
6) name of each product manufacturer and the applicable policy limits;
7) name of the air traffic control authority and the applicable policy limit.

21 Satellite risks

Managing agents should return satellite loss information relating to the single largest loss from the following events, if this figure produces a loss in excess of the de-minimis reporting level.

Managing agents should also consider any other lines of business that would be affected by the following events and in particular exposure under any live satellite third party liability policies that may accumulate.

21.1 Space weather – Solar energetic particle event

21.1.1 Event description

A solar energetic particle event such as a solar flare or coronal mass ejection produces a vast outpouring of protons, electrons and other charged particles which will cause permanent damage to semiconductor devices. This scenario specifically considers the effect of such events on the solar cells of a satellite. A certain number of solar energetic particle events are allowed for in the design of every satellite, but an anomalously large event, such as the Carrington event of 1859, could result in a significant number of satellites simultaneously incurring a reduction in operational capability due to the degradation of the satellite power source.

Satellite age and construction will also determine how an event will affect a particular satellite. However, a single large event (or a number of smaller events in close succession) has the potential to affect all geosynchronous satellites and could result in a loss of power on a majority of satellites.

21.1.2 Loss estimation

For the purposes of this RDS, it should be assumed that either a single anomalous event or a number of events in quick succession results in a loss of power to all satellites in geosynchronous orbit. All live exposures in this orbit will be affected by the proton flare. Managing agents should assume a 5% insurance loss to all affected policies.

The loss under this RDS will therefore be the sum of the following calculation for all live policies covering geosynchronous satellites:

(Insured Satellite Value) x (Loss to Policy)

Therefore, if a syndicate's share of two geosynchronous satellites is USD 10m on the first and USD 8m on a second, the loss to the syndicate would be calculated as:

(USD 10,000,000 + USD 8,000,000) x 5% = USD 900,000

Managing agents should note that under this RDS, "Total Loss Only" policies, component specific policies and policies not covering power losses will not be triggered.

Frequency: the frequency of this type of scenario is considered to be 1-in-100 years.

21.2 Space weather – Design deficiency

In 1994 two satellites of the same type were severely affected by a large space weather event, subsequently attributed to a design deficiency which made the satellites abnormally sensitive to this particular phenomenon. One of the satellites was ultimately a total loss. In 2010 a similar space weather event led to control of a satellite being lost for a period of eight months before the satellite was recovered.

21.2.1 Event description

For the purposes of this scenario, it should be assumed that a design deficiency leaves a particular geosynchronous satellite type vulnerable to space weather events. Such a deficiency should be assumed to leave the satellite, or component part thereof, prone to the effects of deep di-electric charging, surface charging, electrostatic discharge, total radiation dose or other similar effect which could be triggered by a large solar energetic particle event or related disturbances in the Earth's geomagnetic field. In a disaster scenario it is assumed that an anomalously large space weather event results in four satellites of the same type being declared total losses.

21.2.2 Loss estimation

To calculate the loss under this RDS, managing agents should consider all live policies covering geosynchronous satellites. The four largest lines for each satellite type (from the types listed below) should be summed and the largest of these figures reported as the Space Weather Design Deficiency RDS figure.

The following specific satellite types should be considered individually:

- Airbus Eurostar 3000 and Eurostar NEO (all variants)
- Antrix / ISRO I-2k and I-3k (all variants)
- Boeing Space Systems 702 (all variants)
- CAST DFH-4 and DFH-5 (all variants)
- ISS Reshetnev Express 1000 and Express 2000 (all variants)
- Lockheed Martin A2100 (all variants)
- Mitsubishi Electric DS2000 (all variants)
- Maxar LS500 and LS1300 (all variants)
- Northrup Grumman Star 2 and Star 3 (all variants)
- Thales Alenia Space Spacebus 4000 and Spacebus NEO (all variants)

Frequency: the frequency of this type of scenario is considered to be 1-in-50 years.

21.3 Generic defect

Supply chain consolidation means that many satellite prime manufacturers purchase subsystem units and component parts from small numbers of suppliers. Traveling wave tube amplifiers, reaction wheels, command receivers, solar cells and batteries are typically available from only two suppliers.

21.3.1 Event description

A generic defect that develops in one of these supplied parts has the potential to affect a number of different satellites. For any satellite commencing coverage in good health with all redundant units and margin intact it is considered that a total loss would be unlikely and a worst case loss of 50% is assumed. The likelihood of such a loss is considered to be directly related to the remaining coverage period of the insurance policy. From past experience with generic defects, it is considered safe to assume that after satellites have been in orbit for five years they have passed the point at which a generic defect is likely to occur. Based on the current build rates of the major manufacturers it is reasonable to assume that a generic defect could affect a maximum of ten satellites.

21.3.2 Loss estimation

For all live policies covering each of the satellite types listed under section 21.2.2 and which have not surpassed the fifth anniversary of their launch date, managing agents should calculate a generic defect loss as follows and sum the ten largest resultant figures:

(Insured Satellite Value) x (Risk Period Factor) x (50% Loss)

The Risk Period Factor should be calculated from the following table:

Period Remaining on Policy	Risk Period Factor
Greater than 24 Months	100%
18 Months – 24 Months	80%
12 Months – 18 Months	60%
6 Months – 12 Months	40%
Less than 6 Months	20%

Table 35

Frequency: the frequency of this type of scenario is considered to be 1-in-20 years.

21.4 Space debris

Space debris poses an increasing threat to satellite assets in all orbits. The only collisions to have occurred to date were in low Earth orbit [LEO].

A satellite break up or collision in LEO results in the generation of a cloud of debris that progresses, over time, both around the orbit and above and below the orbit. The debris cloud then poses an increased threat for other satellites in LEO. Experience from the Iridium 33 / Cosmos 2252 collision of 2009 illustrated that debris from such a collision could reach up to +/- 200 km from the altitude at which the collision took place. Following a collision, the growth of the debris cloud and the likelihood of further collisions is considered to be directly related to remaining policy period of the insurance coverage provided.

21.4.1 Event description

Considering insured assets in LEO, two groups can be considered. It is considered unlikely that a single event within one of these groups would result in a debris cloud expanding sufficiently to affect the other group. The two groups are as follows:

Group 1: Satellites with orbits in the range of altitudes between 400km and 800km (i.e. +/- 200km of 600km). This group encompasses the majority of imaging satellites as well as a number of communication constellations, including the Iridium Next and Orbcomm. All insured satellites known to orbit within this altitude range should be included in the RDS calculation.

Group 2: Satellites with orbits in the range of altitudes between 1200km and 1600km (i.e. +/- 200km of 1400km). This group encompasses some communication constellations, including Globalstar and Starlink. All insured satellites known to orbit within this altitude should also be included in the RDS calculation.

21.4.2 Loss estimation

For each of these two groups managing agents should sum the result of the following calculation for all satellites on live policies and report the larger of the two figures as the Space Debris RDS:

(Insured Satellite Value) x (Risk Period Factor) x (100% Loss)

Risk Period Factor is the same as shown in the table in section 21.3.2 above.

Frequency: the frequency of this type of scenario is considered to be 1-in-15 years.

22 Liability risks

Managing agents should report two internally modelled liability loss scenarios for each syndicate, subject to the *de minimis* criteria. Where exposed to both professional and non-professional lines liability scenarios, one of each type should be reported.

22.1 Professional lines

The following example scenarios are provided to help guide managing agents in considering the type, scale and impact of their internally modelled scenarios.

22.1.1 Mis-selling of a financial product

Any systemic loss arising from the mis-selling of a financial product including the distribution of said financial product through the appropriate channels. This could comprise two distinct sources of liability attributable to: 1) product and 2) distribution channel. Regulatory investigation might be a trigger to this type of systemic loss but would not of itself be the systemic loss.

22.1.2 Failure/Collapse of a Major Corporation

The failure or collapse of a major corporation listed on one or more Global Stock Exchanges.

22.1.3 Failure of a Merger

The failure or collapse of a merger involving one or major corporations listed on any Global Stock Exchange.

22.1.4 Failure of a Construction Project

The failure of a construction project involving all of the syndicate's casualty risk codes (for example, non-marine liability, architects, surveyors and engineers, etc.).

As an example, from the past, the London 2012 Olympics represented a major exposure in terms of potential failure of a large construction project. Problems had affected construction for the Greek Olympics; during 2008 – 2011 it would have been reasonable to assume that a similar scenario could arise for the London Games.

22.1.5 Recession-Related Losses

A managing agent may identify that its syndicate is exposed to a dramatic fall in the housing market, associated with high negative equity, mortgage shortfalls and defaults. It could model syndicate exposures by utilising casualty risk codes, including: Independent Financial Advisors (IFAs), Solicitors, Surveyors, Lenders, Accountants.

Modelled exposures should also consider a rising unemployment rate thus potentially increasing the exposures to Employment Practices Liability underwritten as a standalone product or as part of Directors & Officers Liability policies.

22.2 Non-Professional lines

The following example scenarios are provided to help guide managing agents in considering the type, scale and impact of their internally modelled scenarios:

22.2.1 Industrial/Transport Incident

A managing agent may identify that it has a high potential syndicate exposure to an extreme loss arising from a release of chlorine at an industrial site or from a train travelling through a major city.

The managing agent would develop a physical model of the incident, with assumptions for the area and populations affected, and the effects of the chlorine gas itself. The model should identify the various organisations that would be held liable, including joint ventures and professional advisors that the syndicate covers.

22.2.2 Multiple Public/Products Losses

An agent managing a syndicate with multiple peak exposures may determine that it would be severely impacted by catastrophe losses affecting a multiple number of contracts. Such a scenario would capture the cumulative effect of a number of vertical spikes and the impact on the syndicate's reinsurance programme.

An example of a loss scenario involving multiple products losses arising out of a common cause would be defective hip replacements which could generate a high frequency of relatively large individual payments via a series of class actions.

22.3 Back year deterioration

These scenarios focus on losses arising from events occurring in 2023, and therefore do not attempt to quantify potential exposures from back year deterioration. The issue of reserving adequacy is subject to monitoring and review by colleagues within the Lloyd's Corporation.

23 Political risks

Managing agents should return Political Risks scenarios that generate losses above the *de minimis* reporting level for the events in the 2023 RDS Political Risk Scenario Specification document.

Lloyd's in conjunction with the LMA Political Risks Panel have agreed that Political Violence (PV) damage factors should only be considered when written in conjunction with exposures under risk codes PR, CF or CR.