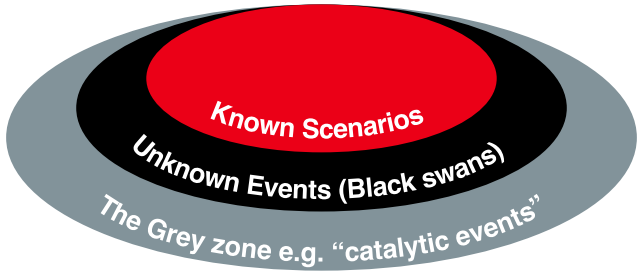
Defining a Cyber Event

Building Blocks of a definition & key questions

All perils vs Named perils

- **All perils**
  - Challenge: How to distinguish between event and non-event (i.e. attritional and large non-cat claims), e.g.
    - — Include losses from same “originating cause” (e.g. same vulnerability, delivery mechanism, point of failure)
    - — Exclude attacks targeted at individual insureds
    - — Exclude “campaigns” e.g. Ransomware as a service, ransomware gangs using same TTPs repeatedly
    - — Implicitly, “black swans” are covered
- **Named perils**
  - Known scenarios / perils only e.g.
    - — widespread malware
    - — service provider outages
    - — hardware or other “single point of failure” events
  - Black swans are excluded

Spectrum of events considered in Event Definitions



“Temporal” aka time constraint

How will an event’s losses be aggregated over time?

- Time frame for claim notifications stemming from the event to be aggregated as an “event”
- Cyber incident responders suggest activity following a major event peaks in the first 6-8 weeks
- Would a 60-day loss notification window therefore be long enough to capture most losses?
- Start at date of first notification, or date of discovery?
- How to deal with “straggler” notifications, complex loss adjustments, latent losses e.g. 3rd party liability

Defining a Cyber Event

Grey areas to be explored

Grey zone #1 : Mass vulnerabilities

Vulnerabilities with mass exploitation potential e.g. Log4J, MOVEit. How to deal with these?

- A vulnerability does not (necessarily) = an event
- Different malware strains may be developed by different threat actors, based on a single vulnerability.
  - Some may be used to carry out targeted attacks (might not be classed as an event), others may be used to carry out widespread events or ones aimed at a point of failure (clearly an event)
- There may be a short-term spike in separate targeted attacks until patch is available and applied
  - Are these claims grouped as one event?

One event definition includes all of the above within an “all perils” wording, in which these are described as “Catalytic Cyber Events”

Grey zone #2: Partially automated attacks

E.g. Microsoft Exchange aka ProxyLogon

- Millions of backdoors (Webshells) automatically installed = non-targeted widespread attack (sounds like an event!), however financial loss only occurs after additional individually targeted cyber acts per victim: use backdoors later to look for sensitive data and carry out further attack (e.g. data exfiltration, ransomware)
- Can insurers (or their IT forensic service providers) even determine this in a short time-frame – IT forensic analysis required to understand nature of how each loss occurred