Defining Silent Cyber Risk

Also nicknamed “cyber as a hazard,” silent cyber risk takes one of two forms:

Unintended Coverage

- Most common meaning of “silent cyber”
- Policy language does not explicitly address cyber risk as a potential cause of loss
- Cyber coverage neither excluded, nor affirmatively granted
- Unanticipated events could create surprise aggregation of claims
- Example: property claims due to ransomware resulting in non-property damage business interruption

Unpriced Coverage

- Cyber risk implicitly accepted, but no premium is allocated or charged for the risk
- Cyberattack is not a covered cause of loss, but could trigger a covered peril / cause of loss
- No adjustment to premium for marginal increase in frequency / severity due to cyberattack risk
- Example: small cyber sublimits in crime policies with no premium allocation

Common Silent Cyber Issues Facing Risk Pools

Silent cyber poses challenges to risk pools on a number of fronts. Some of the main challenges are:

Identifying the exposure

- Non-cyber policies do not have a flag to identify cyber exposure
  - Possible unintended coverage
  - Cyber as a hazard triggering a covered peril
- Legacy policy systems make it burdensome to update and code policies

Recognizing the perils

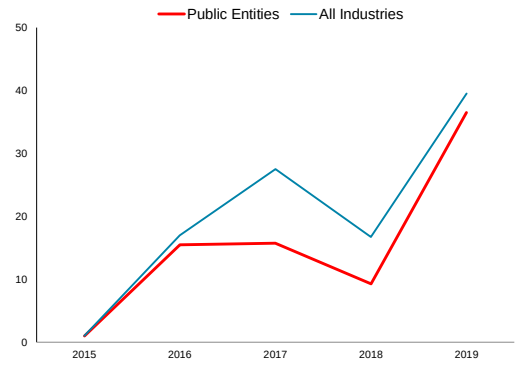
- Policy ambiguity can lead to member confusion and disconnect
- Changes in the threat landscape create new ways to exploit old policy wording
- New and emerging technologies, including connected devices (IoT), wireless sensor networks (WSN), and operational technology (OT)

Lack of coordination & strategy

- Dealing with silent cyber requires integration across various functions including insurance and reinsurance teams, product leaders, IT, actuarial, cat modeling, ERM and others
- This is challenging to traditional (re)insurance silos
- Some pools would prefer to ignore silent cyber or transfer the excess risk to reinsurers rather than solve for it

Ransomware Targeting Public Entities are on the Rise

Cyber ransomware rates by year
(Indexed 2015 = 1.0)



Notes: 2019 incidents through Q3; public admin includes public hospitals and public schools.

Source: Risk Based Security, analysis by Aon. Data as of 10/1/2019

- Through 2019, ransomware incidents affecting US public administration up nearly 400% since 2015 and the worst year recorded
  - Ransomware may have been underreported prior to 2017
- Although public administration ransomware rates kept pace with all other industries, ransomware affecting public administration accounted for nearly 50% of reported incidents in 2019.
  - Public administration reporting rates may be higher than private industry, which may partially explain this trend
- Rise in ransomware in 2019 largely attributed to a reemergence of Ransomware as a Service (RaaS)
  - Sophisticated organized crime also increasingly turning to ransomware
- Victims of ransomware generally appear to be targets of opportunity, although "copy-cat" attacks are prevalent
- Business interruption associated with ransomware increase to 16.2 days on average
- Claims have been made via property policies where cyber exclusions are weak or altogether "silent"

Example Silent Cyber Events – Historical and Potential

Historical Event

Merck loss (NotPetya - 2017)

Property Damage (Data) and consequential Business Interruption

Historical Event

Maersk loss (NotPetya - 2017)

Damage to data systems leading to inability to track and monitor cargo (business interruption)

Historical Event

German steel mill loss (2014)

Property damage emerging from cyber attack against smelting functionality

Potential Event

US blackout scenario

PD, Contingent BI, D&O and Fines and Penalties stemming from a mass blackout event

Potential Event

Dam failure

Flood loss from Dam Failure leading to widespread property losses

Potential Event

Offshore energy events

PD, Control of Well, Removal of Debris and Pollution stemming from an attack against multiple rigs

Potential Event

Transport network manipulation

PD, Business Interruption, Workers Comp, Life, D&O and GL cover for manipulation of train network

Potential Event

Cloud provider systems failure

Contingent business Interruption as a result of systems failure at a large cloud provider

Assessing, Quantifying & Transferring Non-affirmative Cyber Risk

The Aon process, methodology and expertise is one approach to identifying, quantifying and mitigating the exposure to non-affirmative cyber.