GuyCarpenter

CYBER LANDSCAPE & ANALYTICS

Singapore Actuarial Society

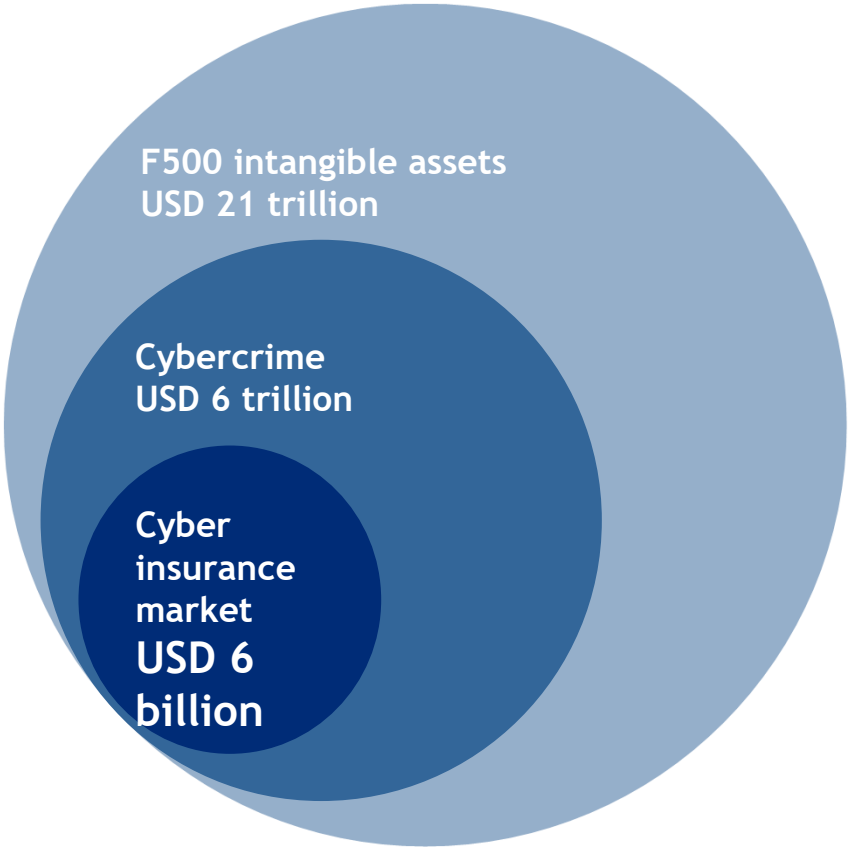
Next Generation Risk Webinar

September 24, 2021

Jess Fung, FCAS, MAAA, Managing Director, North American Cyber Analytics Lead
Ivan Lai, AVP, Center of Excellence

A business of Marsh McLennan

The Changing Nature of Risk



The global cyber insurance market was estimated at $4.85 billion in 2018 and is expected to hit at ***$28.60 billion*** *by 2026.*

Allied Market Research, 2020

The modelled U.S. industry 1-in-100 year cat loss from a cyber event is
USD14.6 billion

Looking Beyond the Clouds, 2019

"The direct loss ratio **rose immensely to 73%** in 2020 from the 47% of 2019".

Fitch, 2020

Intangibles ≠ Cyber exposure ≠ Cyber market

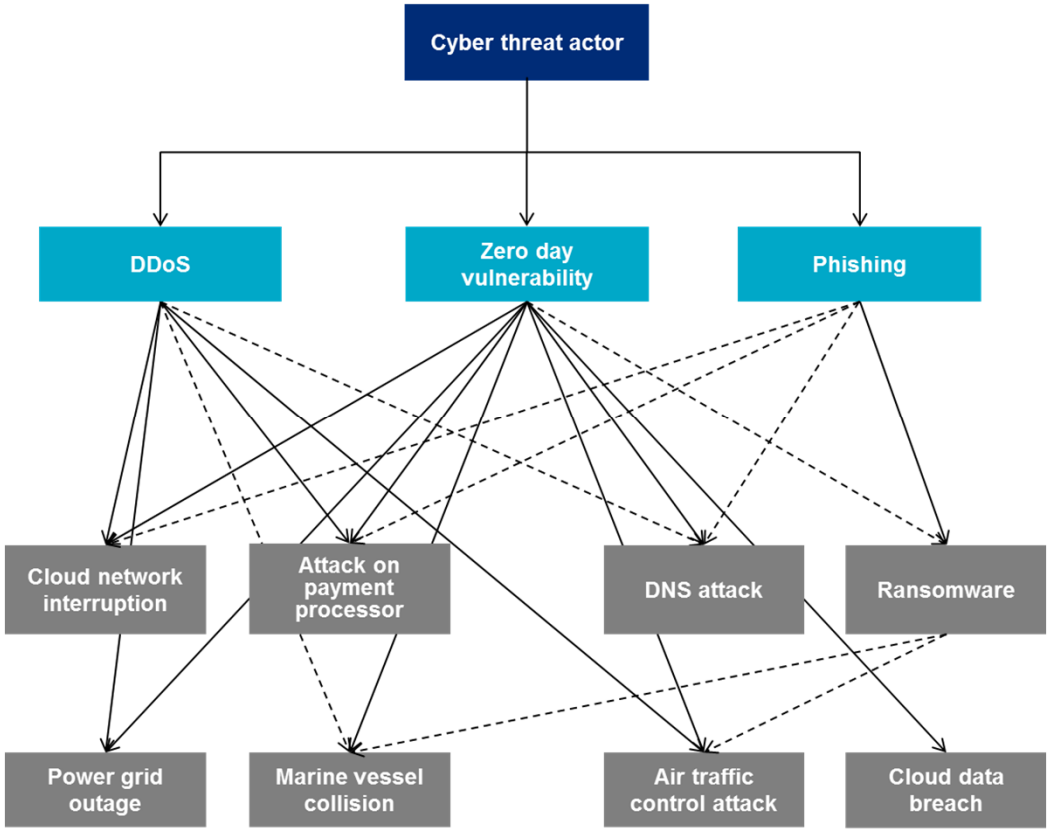
What Makes Cyber Risk Different?

Cyber Risk is a game played against an adversary

Cyber risk's past does not predict cyber risk's future

Cyber risk is extremely volatile

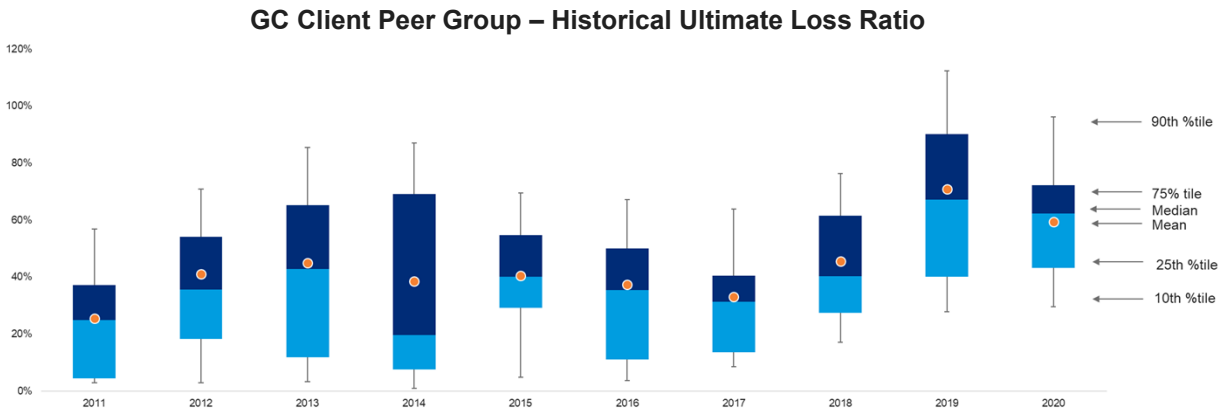
Cyber risk is interconnected and interdependent

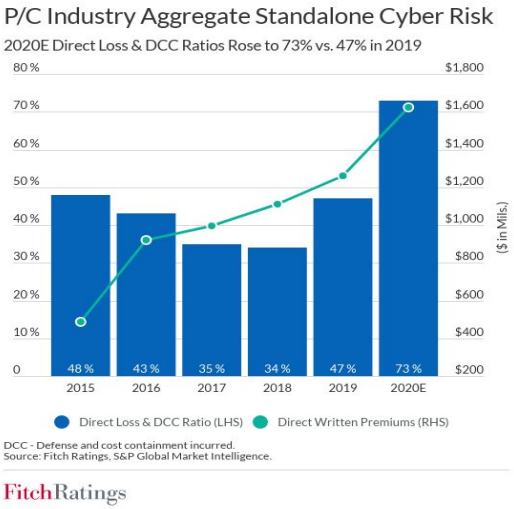


Rising Cyber Claims Signal Further Challenges to Insurance

Prompting Profitability Uncertainties Even for Established Portfolios

- According to the mid-year 2021 Fitch cyber report, the cyber industry direct LR rose to 73% in 2020 from 47% in 2019, which outpaced premium growth of 22%
- AMB reported LR of 67.8% in 2020 up from 44.8%; increased LR extended to 15 of 20 largest cyber insurers
- Across Guy Carpenter's client base, non-cat development increased 15-20% from 2019 to 2020 after previous deterioration of 12-15% in 2018 / 2019
- **This deterioration is reflective of broader global cyber market dynamics, driven by severity of ransomware claims**





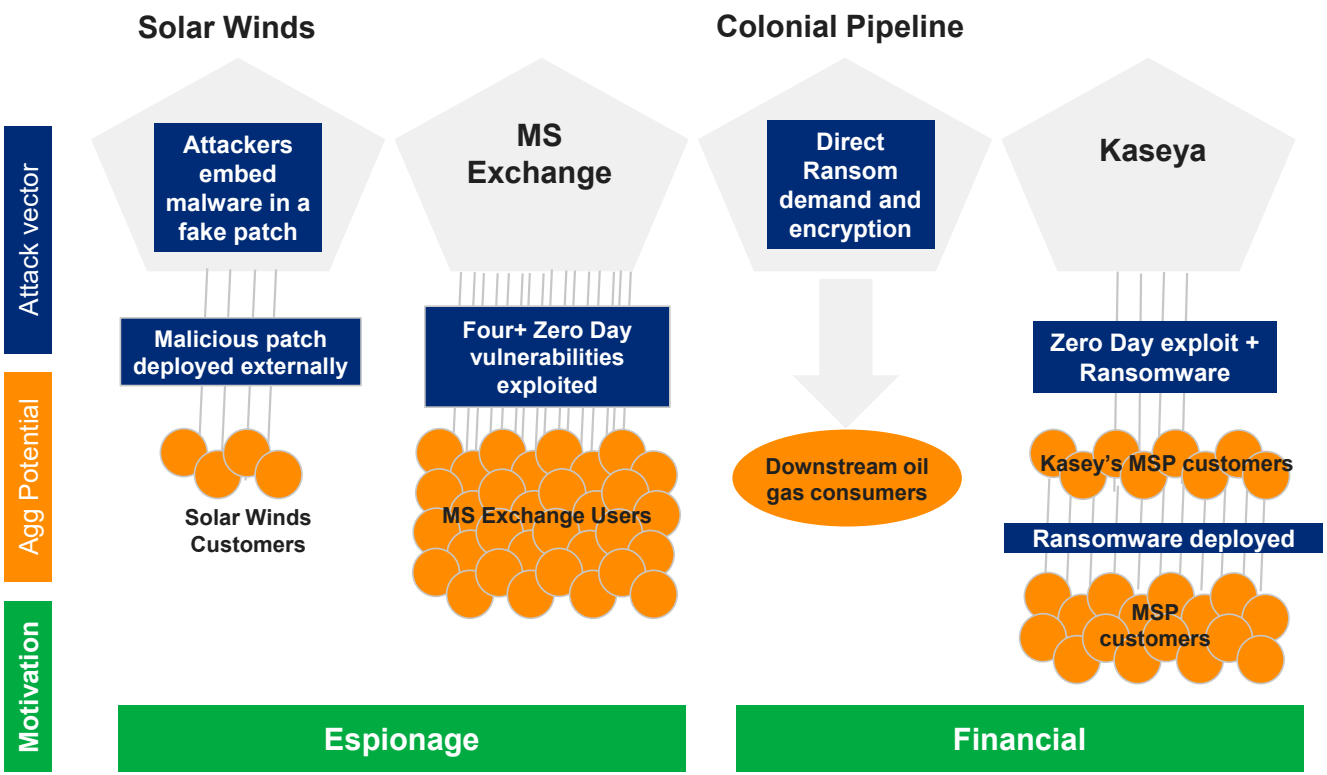
Insurers will have to achieve both significant premium rate increases and tighter coverage terms in order to stage a recovery in underwriting performance over the medium term

Results vary by year as shown in the chart due to carriers' underlying composition of business, limits & attachment points

Source: Guy Carpenter Analytics, Fitch Ratings & S&P Global Market Intelligence

Recent Events Highlight Insurable Exposure Aggregation Potential

Supply Chain Vulnerabilities in the Last 12 months



High profile cyber events are driving aggregation concerns amongst insurers, impacting rates, coverage and risk mitigation measures

- Guy Carpenter worked closely with CyberCube to develop a bespoke modeled view to understand the potential cascading effect of the SolarWinds breach and incorporate the scenario mapping into our modeling.
- Impact of events continue to build on each other. Kaseya was the first event observed combining elite technical sophistication with significant ransom demands.
- Additional zero day vulnerabilities stemming from SolarWinds and MS Exchange are still being identified.
- Headline events have prompted global response at the highest levels

Cyber Insurance Snapshot and Future Expectations

Pricing and Terms

Rates

Average premium increase in (US/UK)
1Q20: **5.6% / 11%**
2Q20: **7.2% / 18%**
3Q20: **10.6% / 13%**
4Q20: **17.2% / 17%**
1Q21: **35.1% / 29%**
2Q21: **59.5% / 51%**

Limits/ Coverage

Many carriers are reducing capacity exposed. Some carriers are scaling back ransomware-related coverages (or not offering coverage at all) for clients that don't have adequate controls.

Future Expectations

Anticipate increases to accelerate, likely **75% or greater** in Q3 and beyond. Risk specific terms dependent on risk profile & controls.

Claims

Frequency

Ransomware tactics are more accessible for bad actors. Short tail nature of losses is changing insurer profitability on an ongoing basis.

Severity

Ransom payments in the millions. Business interruption and data recovery loss. SolarWinds & MS Exchange attacks have increased carrier uncertainty around systemic nature of cyber risk.

Future Expectations

Ransomware attacks will continue to increase in sophistication; systemic risks concerns; privacy risk concerns.

Underwriting

Information Needs

Full application & responses to ransomware Q's. Underwriters focusing on supply chain exposures and CBI controls.

Carrier Flexibility

Ransomware responses required prior to quoting. Third party scans may lead to remediation requests. Adequate controls are required to obtain a quote.

Future Expectations

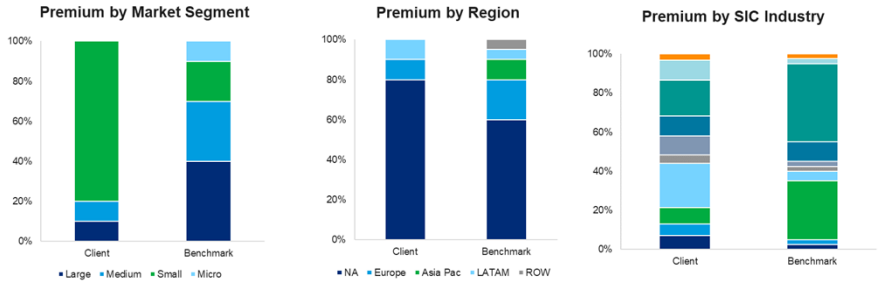
As technical acumen increases, underwriters will demand additional information to assess risk and may require certain cyber controls to quote.

Source: Marsh

Evolving Analytics For An Evolving Risk

Industry Thought Leadership Publications

Benchmark Peer Analysis



Cyber Stress Testing

Silent Cyber Event

Actual event: June 2017 WannaCry / NotPetya

Incident: Critical shipping and distribution downtime, ransom, data loss

Intent: widespread disruption

Stress Scenario

Primary Stressors: amplifying ransom demand + prolong disruption during holiday season

Cascading impact: ransom, data breach fines, forensics, legal fees, pipeline shutdown, global distribution delay, data loss, stock drop, reputational damage

Affirmative Cyber Event

Responsible parties: December 2020 SolarWinds

Incident: Targeted software supply-chain attack

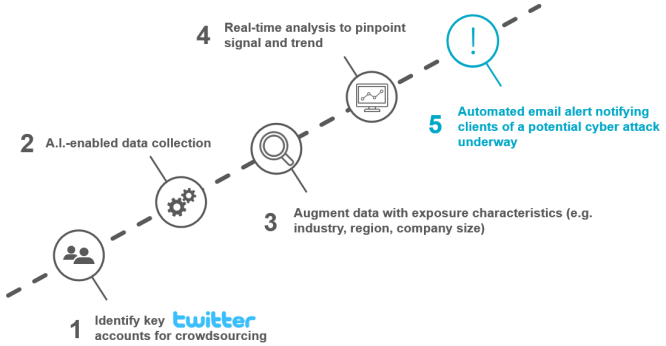
Intent: Espionage

Stress Scenario

Primary Stressors: financially motivated attack beyond espionage; extortion / ransomware on non-FI + fraudulent transactions for FI

Cascading impact: disproportionately higher impact on medium-to-large risks, downtime from top 10 telecom and vast majority of Fortune 500, data exfiltration, backdoors created for future exploits

AI-Powered Cyber Event Response



Assessing Cyber Exposure Through a Continuous Cycle

Internet of Things / Digitization

- Machines that can be fixed on their own
- Digital twins of systems, buildings, and cities
- Listening devices in stores
- Mobile phone voting for elections

Robotics

- AI-powered robots (e.g. microscopes) and nanobot technology
- Autonomous farming and agriculture

Biometrics

- Advanced prosthetics and wearable sensors
- Toys that monitor children's health and movement

Advanced Analytics/ Artificial Intelligence

- Environmental sensors for smart agriculture
- Human-like conversation platforms

Advanced Computing

- Quantum computers
- Blockchain-enabled identity verification

Source: Gartner, IoT Hype Report and Top 10 Strategy Technology Trends, Oliver Wyman analysis

Questions