Affirmative vs. Silent Cyber: An Overview

Cyber liability is a young class of business, but it continues to experience rapid growth spurts, seemingly following each major global cyber breach or attack. As a peril, cyber risk can be defined as any risk emerging from the use of information and communication technology that compromises the confidentiality, integrity or availability of data, systems or services.

Cyber risk is characterized by interdependencies, potentially extreme events with a high uncertainty with respects to the data and modeling approaches. In the past, the focus was mostly on issues surrounding third-party liability; however, in 2017, WannaCry and Petya/NotPetya caused a shift in the cyber discussion to first-party liability, such as extortion, ransomware and business interruption. Losses from NotPetya, in particular, extended over the billion dollar mark in part as a result of the broadening of the original security and privacy policy language for first-party coverages, such as system failure and business interruption.

What is Affirmative Cyber?

Coverages for cyber perils contained within either Stand-Alone Network Security & Privacy policies or endorsements added to P&C policies covering costs associated with the impact of a data breach and network security failure/attack

Common Coverages

1st Party

Event management/ breach response – Forensics, public relations, call center, notification and credit monitoring services

Business/network interruption Extra expense and loss of business income

Cyber extortion/ ransomware – Forensics, investigation and ransom payments

Data restoration – Costs to replace, restore, recreate damaged or lost data

3rd Party

Privacy liability – Failure to prevent unauthorized access/disclosure of entrusted personally identifiable or confidential information (liability and defense costs, PCI fines and penalties)

Network security liability – Failure of system security to prevent or mitigate a computer attack (liability and defense costs)

Privacy regulatory defense costs – Privacy breach and related fines or penalties assessed by regulators

What is Non-Affirmative/Unintended/Silent Cyber?

Instances in which a P&C insurance policy (i.e. General Liability, D&O, Property, Marine, etc.) is triggered where:

1. Cyber perils are not explicitly included or excluded;
2. Exclusionary language, when included, is ambiguous;
3. Insuring agreements are satisfied, however the insurer did not price for or contemplate loss scenarios emanating from a cyber peril/threat

	Examples
Property Business interruption from non physical property damage	Ransomware attack caused computer systems to be inoperable causing business interruption
Errors and Omissions Liability Coverage for negligent acts in securing data	Law firm breached and client records are stolen. Due to professional standard of care, third party coverage applies
Directors and Officers Indemnification coverage for any legal action due to failure to have adequate protocols and procedures in place	Publicly traded company breached causing stock drop and a class action lawsuit follows
General Liability Bodily Injury, property damage liability and privacy	Cyber attack causes building's heating system to overheat causing an explosion. Bodily injury and property damage ensue

WannaCry and Petya/NotPetya also contributed to the current affirmative versus non-affirmative/"silent cyber" coverage debate, a lurking variable in the cyber risk discussion. "Silent cyber", also known as "unintended" or "non-affirmative" cyber, refers to the unknown or unquantified exposures originating from cyber perils that may trigger traditional property and liability insurance policies, which may not explicitly provide a cyber coverage grant, or from a cyber exclusion that is poorly worded or ambiguous. The systemic nature of the cyber risk means "silent cyber" is becoming endemic in virtually every type of insurance policy.

While initiatives have emerged across the industry to address non-affirmative cyber coverage, there is still a great degree of uncertainty as to the extent to which this type of coverage is unintentionally being written. This area of unknown leaves the industry vulnerable to a major accumulation of losses, which will only grow in today's market conditions. The dynamic nature of cyber risk and the rapid pace of technological innovation cannot be understated because the challenges they create are profound. Disruptive technologies are not only changing the way we do business but transforming the way we communicate, the way we make decisions and the way we see our place in the world.

From a reinsurer's perspective, providers would like to see more clarity of coverage in standard property/casualty lines with respects to cyber, with exclusions added where necessary. If cyber is defined as affirmative security, business interruption and privacy insurance then, in the current environment, sufficient reinsurance capacity is available. If the definition of cyber were expanded into non-affirmative cyber, where losses attributable to cyber could also impact traditional property and casualty lines of business, especially non-physical business interruption losses, we would see some reinsurers exit the space or, possibly, reduce their capacity. While there would be a premium charge for adding non-affirmative or unintended cyber, Guy Carpenter has provided client solutions to address this exposure. As the first dedicated cyber specialty reinsurance broking practice in the industry, Guy Carpenter leverages technical product expertise and best-in-class analytics to provide innovative first-to-market solutions.

"Silent cyber", also known as "unintended" or "non-affirmative" cyber, refers to the unknown or unquantified exposures originating from cyber perils that may trigger traditional property and liability insurance policies.

For more information and general enquiries please reach out to one of the Guy Carpenter contacts below:

Jeremy S Platt
Managing Director
New York
+1 917 937 3002
jeremy.s.platt@guycarp.com

Ralph Caravello
Managing Director
New York
+1 917 937 3043
ralph.m.caravello@guycarp.com

Eddy Vanbeneden
Managing Director
Brussels
+32 267 49811
eddy.vanbeneden@guycarp.com

Elizabeth Pullum
Senior Vice President
New York
+1 917 937 3420
elizabeth.pullum@guycarp.com

Chris Shafer
Assistant Vice President
New York
+1 917 937 3423
christopher.shafer@guycarp.com

Carolyn Morley
Managing Director
London
+ 44 207 357 2733
carolyn.morley@guycarp.com

Thomas Herde
Managing Director
London
+ 44 207 357 1511
thomas.herde@guycarp.com

Laura Boettcher
Vice President
San Francisco
+ 1 415 984 2860
laura.c.boettcher@guycarp.com

Siobhan O'Brien
Managing Director
London
+44 207 357 5593
siobhan.obrien@guycarp.com

Kirsten Eickstaedt
Managing Director
London
+44 207 357 5083
kirsten.eickstaedt@guycarp.com

Aris Papachronopoulos
Vice President
London
+44 207 357 1516
aris.papachronopoulos@guycarp.com

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with more than 2,300 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy, and people. With nearly 65,000 colleagues and annual revenue over $14 billion, through its market-leading companies including Marsh, Mercer and Oliver Wyman, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment. For more information, visit www.guycarp.com. Follow Guy Carpenter on Twitter @GuyCarpenter.