TOKIO MARINE
GROUP

# Tokio Marine Group Non-Affirmative Cyber Risk Assessment

STAYING AHEAD OF THE CURVE

# PREFACE

Networking in London with insurance industry peers over a coffee was somewhat commonplace before the global pandemic. Luckily for me, the idea of this industry paper came to me in such a setting prior to the pandemic, with a former colleague from Munich Re. That discussion was a microcosm of the approach I wanted to take i.e. how can multiple views come together and enhance the thought-leadership needed to tackle the non-affirmative cyber problem. The process most carriers go through to manage their exposure to non-affirmative cyber is to Identify, Track, Exclude, and Price the risk. The opportunity to price for non-affirmative risks (through affirmative endorsements and buy-backs in other lines of business) will increase, but first a stable platform and collective understanding must be the priority.

Our goal of strengthening the Tokio Marine Group risk management approach was achieved, but nothing can be taken for granted in the insurance market. Collectively we should do more to ensure there are no surprises in the advent of a claim by applying the appropriate exclusionary language. The approach we inevitably developed within Tokio Marine Group is reusable, adaptable, and laser-focused on offering our senior executives the confidence needed to continue to manage the risks.

**Daljitt Barn**
Global Head of Cyber Risk, Tokio Marine Holdings, Inc.

# CONTENTS

# EXECUTIVE SUMMARY

In summer 2020, Tokio Marine Group launched a project to elevate our non-affirmative cyber risk management and strategy, building on existing work done in 2016 and 2018. On this occasion, we decided to take an open and collaborative approach by inviting Munich Re and Gallagher Re as discussion partners. This paper is an outcome of that project, with the team aspiring to contribute to the industry by bringing forward a new concept to the ever-evolving market.

In this paper, we discuss market developments on non-affirmative cyber risk over the last few years, signposting a broad range of views from (re)insurers and market bodies to regulators and model vendors.

We then introduce Tokio Marine Group's non-affirmative cyber risk assessment framework. The framework is the core output and key outcome from the project which allows any (re) insurers to assess non-affirmative cyber risk exposures within their Property and Casualty insurance portfolios.

To help visualise our framework for market participants, we have applied the framework to the London Market exposure as an illustrative example.

Collaborating with a leading cyber (re)insurer and broker offered the project team insights into markets, products, regulatory frameworks, and legal considerations which accelerated and enhanced our framework development.

We will continue to keep a close watch on market developments in non-affirmative cyber, but our innovative approach, supported by Munich Re and Gallagher Re, has given Tokio Marine Group an elevated position in the market.

# DEVELOPMENTS IN THE MARKET

## MARKET INITIATIVES

Non-affirmative cyber initiatives in the (re)insurance market have ranged from the codified approach of the Lloyd's and UK market bodies, to bottom-up, (re)insurer-led approaches, as evidenced in the actions of some of the world's largest (re)insurance carriers. (Re)insurers are at different stages in their efforts to identify and manage non-affirmative exposure and adhere to their respective regulatory requirements. A diverse range of strategies have been employed, manifesting in projects of differing depth, breadth and outcomes. For this reason, it is worth highlighting the industry-wide benefit of transparency - as demonstrated in the publication of this paper.

EXHIBIT 1.1 MARKET & REGULATORY RESPONSES TO NON-AFFIRMATIVE CYBER

**2013**
- APRA highlights need for (re)insurers to understand their accumulation

**2015**
- Lloyd's introduces Cyber Realistic Disaster Scenarios (RDS)

**2016**
- PRA highlights challenges for (re)insurers to understand both their affirmative and non-affirmative cyber exposure

**2017**
- EIOPA & NAIC announce collaboration strategy with non-affirmative cyber on their agenda
- In a supervisory statement, PRA states that it expects firms to be able to "identify, quantify, and manage" cyber risk both affirmative & non-affirmative

**2018**
- Global P&C insurer announces non-affirmative strategy, namely revising its forms

**2019**
- Two more global P&C insurers announce plan to clarify cyber coverage
- Lloyd's Y5258 bulletin outlines mandate to affirm or exclude cyber from all contracts and sets out Phase I schedule
- EIOPA non-affirmative workshop
- PRA "Dear CEO" letter highlights that onus is on firms to meet their expectations per their 2017 statement
- IFoA publishes non-affirmative framework
- APCR issues memo on "Implicit Cyber"
- BaFin releases non-affirmative survey

**2020**
- Lloyd's Phase I (incl. Property); Y5277 bulletin outlines further timeline; Phase II (incl. A&H and Contingency)
- EIOPA publishes Cyber Underwriting Strategy
- MAS releases "Cyber Risk Surveillance" paper
- EIOPA & NAIC work on non-affirmative best practice
- BaFin prioritizes non-affirmative cyber

**2021**
- Tokio Marine begins coverage clarification for Commercial Lines in Japan
- Lloyd's Phase III (incl. Aviation and D&O) & Phase IV (incl. Marine and Casualty Treaty)
- NY DFS releases Cyber Insurance Framework

| | | |
|---|---|---|
| APCR | Prudential Supervision & Resolution Authority (France) | Asia-Pacific |
| APRA | Australian Prudential Regulation Authority (Australia) | Europe |
| BaFin | Federal Financial Supervisory Authority (Germany) | London / United Kingdom |
| EIOPA | The European Insurance & Occupational Pensions Authority (EU) | Markets |
| IFoA | Institute & Faculty of Actuaries (UK) | North America |
| MAS | Monetary Authority of Singapore | |
| NAIC | National Association of Insurance Commissioners (US) | |
| NY DFS | New York State Department of Financial Services (US) | |
| PRA | Prudential Regulation Authority (UK) | |

# EXCLUSIONS

In parallel to the developments outlined above, the timeline below outlines the release of new exclusionary language focused on non-affirmative cyber risk post-2014. As evidenced below, the cadence of new exclusion production has aligned with wider market and regulatory initiatives.

EXHIBIT 1.2 NON-AFFIRMATIVE CYBER EXCLUSIONS LANDSCAPE

**2014**
- ISO publishes first non-affirmative exclusions relating to data breach (incl. CG21 06 05 14)

**2019**
- IUA 09-81 (Cyber Loss Absolute Exclusion) and IUA 09-082 (Cyber Loss Limited Exclusion) published
- LMA releases Property and Marine Cyber clauses (incl. LMA5400 and LMA5402) in respect of Lloyd's Y5258

**2020**
- IUA releases Model Joint Excess of Loss Cyber clause (JX2020-007) and Model Marine Cargo Exclusion & Affirmation Endorsement (JC-2020-014)
- LMA releases clauses for Contingency Risks (incl. LMA5430), Motor Risks (incl. LMA5434), Casualty Reinsurance (incl. LMA5460) and Personal Accident Reinsurance (LMA5467) in respect of Lloyd's Y5277
- ISO releases Cyber Incident Exclusion Endorsement and Cyber Incident Exclusion with Ensuring Cause(s) of Loss Exceptions Endorsement

**2021**
- LMA releases clauses for D&O business (incl. LMA5471) in respect of Lloyd's Y5277
- ISO Auto Hacking Expense Endorsement for Commercial Auto slated for 2021

| | |
|---|---|
| LMA | Lloyd's Market Association |
| IUA | International Underwriting Association |
| ISO | Insurance Services Office |

# EXPOSURE MANAGEMENT

With the initiatives being led by market regulators and the new exclusion releases, cyber accumulation models have required continuous innovation to keep pace with the evolutionary nature of cyber threats. Updates also incorporate emerging data sources, driving greater model relevance. The ability of leading accumulation modelling vendors to meet this challenge for affirmative cyber events is still a work in progress.

Understanding non-affirmative cyber exposure presents additional challenges. Arguably every line of business contains some form of non-affirmative cyber risk. Additionally, as with other perils, each line of business requires different modelling approaches to determine exposure to cyber risk. The heterogeneous nature of non-affirmative cyber exposure across the insurance market also compounds this challenge, rendering standard accumulation scenarios less capable of presenting a complete picture of the risk.

EXHIBIT 1.3 COMPARING DIFFERENT VENDOR APPROACHES & CAPABILITIES

| How are accumulation vendors providing solutions for managing non-affirmative exposure? | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 | Vendor 5 |
|---|---|---|---|---|---|
| **Research & Development** Releasing research papers and/or supporting clients through consulting engagements | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Lloyd's Blackout Scenario** Vendor has blackout model or equivalent available as part of their accumulation offering | ✓ | ✓ | ✓ | ✓ | |
| **Additional Non-Affirmative Scenarios Available** Non-affirmative models and modelling parameters beyond Blackout are provided in core toolset | ✓ | ✓ | ✓ | | |
| **Non-Affirmative Coverages are Mapped** Model enables mapping of non-affirmative coverages for otherwise affirmative cyber scenarios | ✓ | ✓ | | ✓ | |

Given these challenges, some vendors have taken tentative steps towards quantifying non-affirmative cyber risk, with others focused on providing tools and solutions primarily for affirmative cyber exposures. Many vendors now offer an equivalent model for the Lloyd's Blackout Scenario and attempt to map non-affirmative coverages otherwise dedicated to affirmative cyber risk scenarios. Some vendors have even developed specific non-affirmative cyber models. As vendor approaches for quantifying non-affirmative scenarios are still developing, most existing models are currently deterministic in nature. This reduces complexity and arguably offers greater flexibility and transparency to clients looking to tailor models to their individual needs. Overall, these tools and models are best used in combination with other methods, such as the framework described in this paper, given the developing nature of the risk and wider understanding of non-affirmative cyber.

# NON-AFFIRMATIVE CYBER RISK ASSESSMENT FRAMEWORK

## BACKGROUND

Alongside the developments in the industry, Tokio Marine Group has taken steps to understand and control non-affirmative cyber risk as a prudent insurance group. Following on from the establishment of the Cyber Centre of Excellence (CCoE) in 2018, a central function to provide group-wide direction on cyber risk, we have accelerated our investment to manage underwritten cyber risk from both affirmative and non-affirmative exposures.

In summer 2020, Tokio Marine Group launched a project led by the CCoE to elevate our non-affirmative cyber risk management and strategy. The project team also invited industry leaders – Munich Re and Gallagher Re as discussion partners. As there are no well-established market standards in this area, the project aims to contribute to the industry by bringing forward a new approach.

## PROJECT OBJECTIVES

The key objectives of the project were as follows:

- Build a risk assessment framework to qualitatively capture non-affirmative cyber exposure within all major Property and Casualty (P&C) lines of business.
- Update quantitative risk assessment (scenario loss models) focusing on the material exposures identified by the qualitative risk assessment.
- Revisit the group's underwriting standard and strategy for non-affirmative cyber based on an improved understanding of the risk through these assessments.

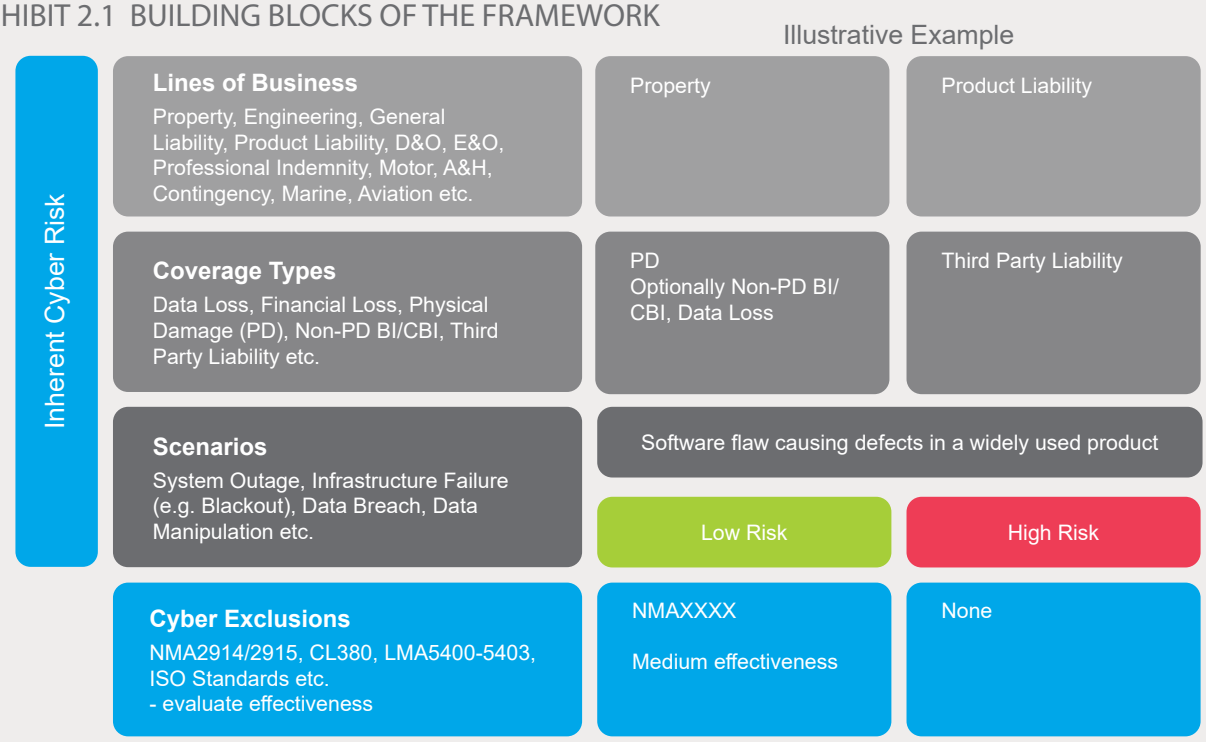

This approach was taken because the exposure base is large (in theory it is almost all the lines of business). It was not practical or efficient to build scenario loss models without knowing where high risk exposures lie within the portfolios i.e. our focus had to be materiality. Therefore, the approach we took had to be a mile wide, but a foot deep to ensure we achieved success.

# THE FRAMEWORK

The framework built by the team consists of two assessment criteria to evaluate the riskiness of the exposure:

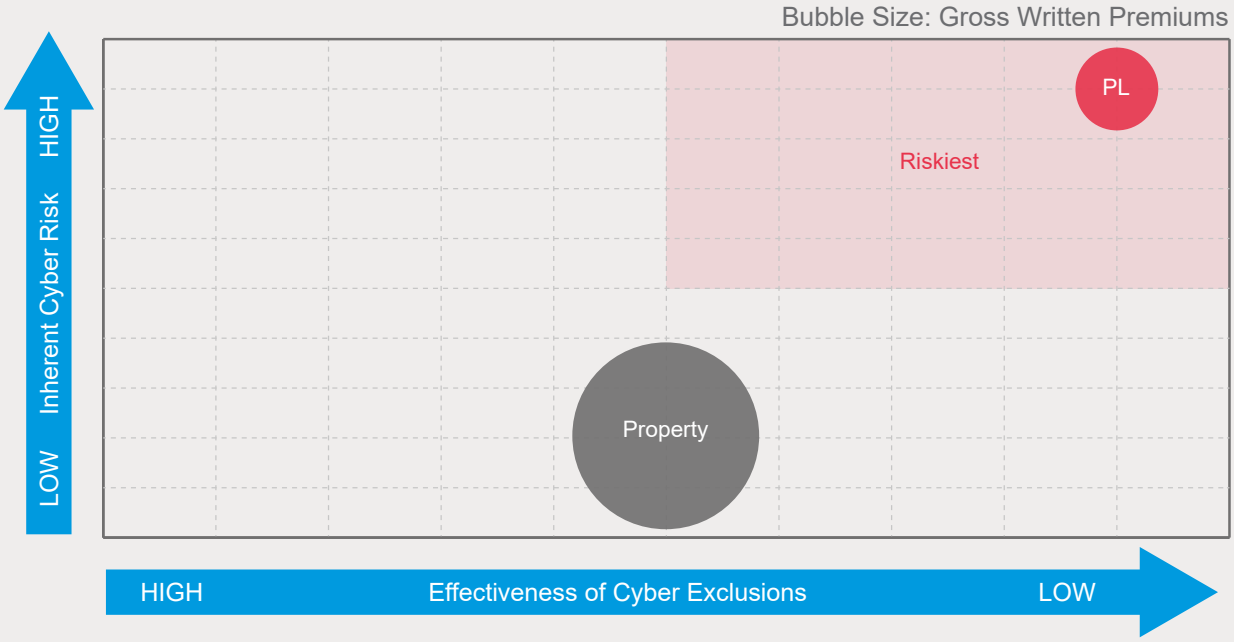
- Establish the inherent cyber risk within major lines of business by reviewing coverage types offered in the polices and applying a comprehensive set of generic cyber scenarios as-if there are no cyber exclusions attached to the polices.
- Evaluate the effectiveness of the cyber exclusions that are in place within these policies.

EXHIBIT 2.1 BUILDING BLOCKS OF THE FRAMEWORK




We then combine the two assessments together and draw a bubble chart which helps intuitively grasp the riskiness of the exposure. The bubble size can typically be a measure of exposure such as Gross Written Premiums. As is illustrated in the example below, Property has low inherent risk whereas Product Liability has high inherent risk under the software flaw scenario. By applying the effectiveness of the cyber exclusion, the output bubble chat demonstrates that Product Liability is in the top right quadrant i.e. riskiest area, which may need attention.

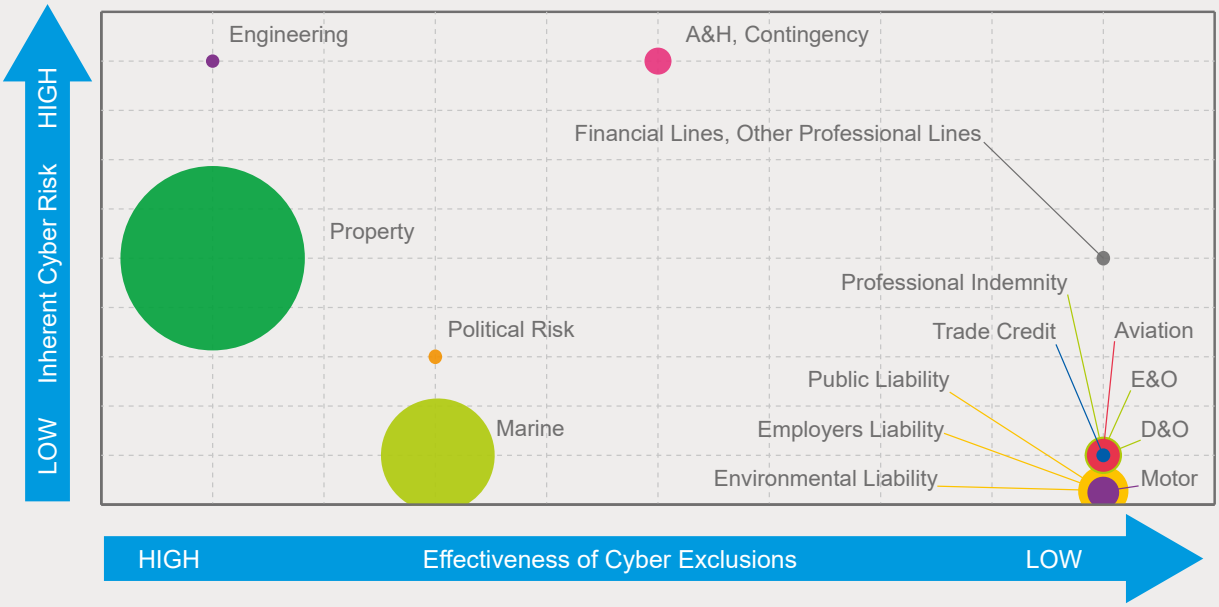
EXHIBIT 2.2 SOFTWARE FLAW SCENARIO



# ILLUSTRATIVE APPLICATION OF THE FRAMEWORK TO THE LONDON MARKET

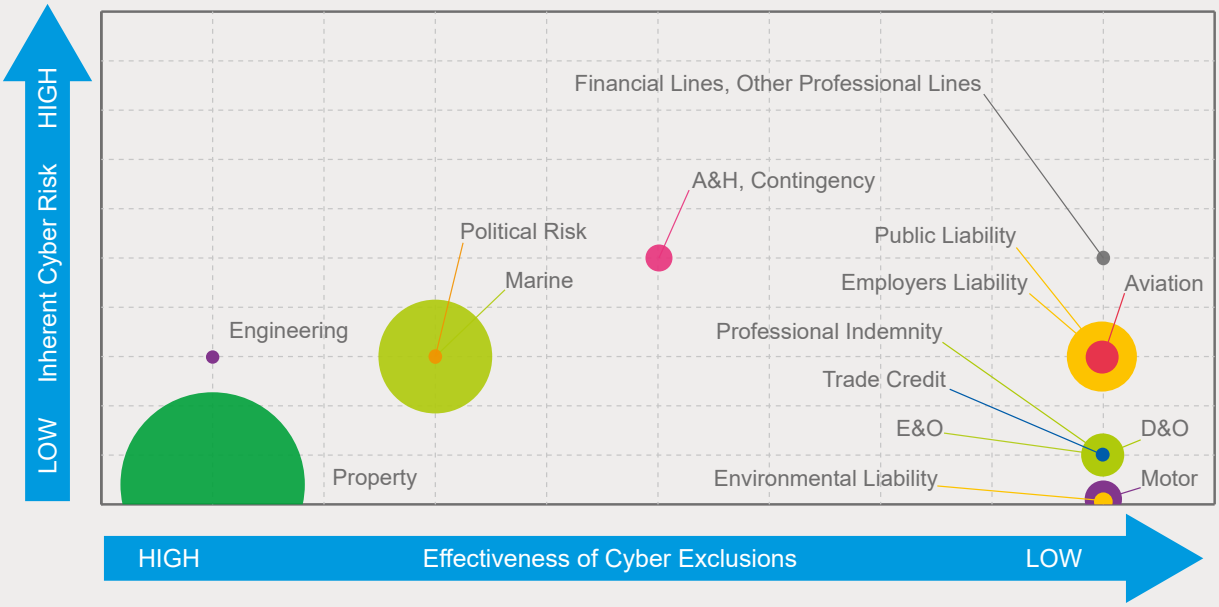
To demonstrate the value of the framework, an illustrative exercise was carried out to apply the framework to the London Market exposure. This was based on collective assumptions made by Tokio Marine, Munich Re, and Gallagher Re, so it does not represent either Lloyd's or IUA's view of risk. As assumptions were made at the end of 2020, results will change over time alongside the progress of the initiatives in the London Market. Some of the Casualty lines of business on the right-hand side of the charts (Low Effectiveness of Cyber Exclusions) should gradually move to the left (High Effectiveness of Cyber Exclusions), as exclusions are implemented for these classes across the market.

EXHIBIT 3.1 IT OUTAGE / MALWARE SCENARIO (Snapshot as of December 2020)



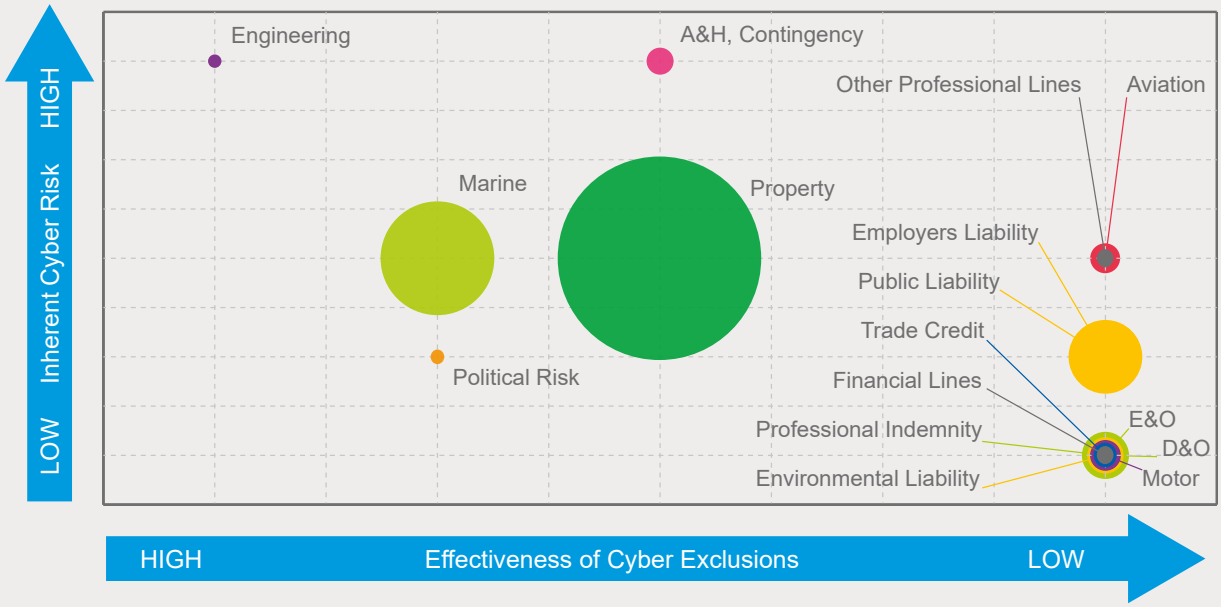

Accident and Health (A&H) and Contingency which includes Event Cancellation pose the highest potential for claims in an IT outage / data loss event. Property (including Machinery Breakdown) covers could also suffer especially if "data as property" cover is offered, but cyber exclusion initiatives in the London Market has resulted in coverage being minimised.

EXHIBIT 3.2 DATA BREACH SCENARIO (Snapshot as of December 2020)



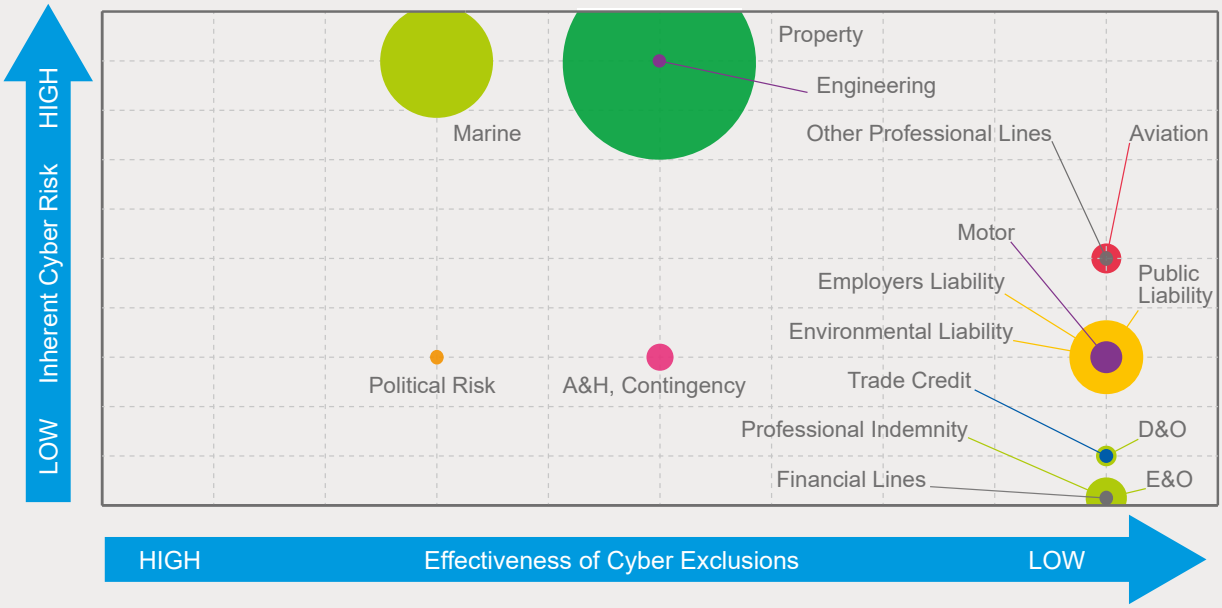
Liability classes all have potential to be triggered by claims when a data/privacy breach occurs, for example in the form of mental distress, or triggering regulatory notifications / negligence claims from affected counterparties, potentially leading to shareholder action (D&O). However, the link between an event occurring and a successful claim being made may not be as strong, leading to most exposures being found in the middle to the bottom right of the chart. It was uncommon to find cyber exclusions in Liability classes at the time of this exercise which will change from Lloyd's Phase III onwards.

EXHIBIT 3.3 BLACKOUT SCENARIO (Snapshot as of December 2020)




A blackout scenario has potential to trigger losses, especially under Contingency (including Event Cancellation) and Property covers with business interruption. In addition, the exclusions that apply for Property usually have some form of carve-back for physical damage, which result in increased coverage for blackouts with physical damage under Property policies.

EXHIBIT 3.4 CYBER-PHYSICAL SCENARIO (Snapshot as of December 2020)




Cyber-physical events (e.g. fire set off by hacking of industrial control systems) have potential to trigger claims under Property, Engineering and Marine Cargo. Due to partial physical damage carve-backs, there is more potential for successful claims due to such events. Other significant cyber-physical exposures include Aviation, where cyber exclusions are less common and can plausibly trigger claims under a cyber-physical scenario.

# REINSURANCE VIEWPOINTS OF NON-AFFIRMATIVE CYBER RISK

## MARKET LEADERS MUST CONTINUE TO LEAD, REGULATOR FOCUS TO INCREASE

To reiterate, in recent years, some of the largest global non-life insurers and notably, the London Market have made important progress towards identifying non-affirmative cyber risk across P&C lines, and providing a pathway to excluding it, then affirming it. Regulation has played a key role as a catalyst for action.

The key now is to use the momentum in local insurance markets across the globe. When taking a more global view, we observe that there is still much work to be done. To date, only a minority of local regulators are requesting reporting on non-affirmative cyber exposure.

## FRAMEWORKS AND SYSTEMATIC APPROACHES HELP IDENTIFY FOCUS AREAS

On such a broad topic, the questions facing P&C insurers conducting an investigation into their non-affirmative cyber exposures are often: "Where to start?", "What exactly do we mean by 'cyber risk'?", "Is this a huge risk, or rather a huge white spot, or both / neither?"

A systematic approach, that considers inherent cyber risk (elaborated through loss scenarios, coverages, exclusions and business volumes) helps to bring clarity to an insurer's extent of non-affirmative cyber exposure, and to answer their key questions. Such a process provides a helpful overview, from which actions can then be prioritised, to dive deeper and address the most critical areas.

## ACCUMULATION RISK AT THE CORE OF RISK ASSESSMENT

Global reinsurers are concerned about the ongoing sustainability of insurance markets. They strive to avoid unexpected or unmodelled accumulation exposure that pose existential threats to these markets. It is therefore of utmost importance to create a linkage between the practice areas of non-affirmative cyber investigations and accumulation risk management.

The cyber accumulation risk management function must look beyond the bounds of the stand-alone cyber products into traditional lines of business. Particular focus should be on scenarios where widespread economic disruption occurs. Insurance products exposed to first-party losses resulting from widespread cyber-induced disruption scenarios (e.g. failure of critical infrastructure, widespread malware, unavailability of cloud services), and especially those without a physical damage proviso, should be the focal point.

## LESSONS FROM THE PANDEMIC

The extent of "non-affirmative pandemic" exposure in the market has been revealed through significant losses suffered in particular within the Event Cancellation product in Contingency, and the recent UK Supreme Court ruling on business interruption coverages. The lessons could not be clearer here; a well-intended cyber exclusion may not be enough to avoid suffering unwanted systemic losses. When it comes to cyber, diligence and clarity in drafting policy wordings is similarly paramount across all P&C lines in order to avoid unintentionally covered losses in the yet to come "great cyber catastrophe".

A digital parallel to the government lockdowns seen globally in response to COVID-19 ("digital lockdown", whereby governments or industries shut down major IT services to prevent irreversible damage from the threat of ongoing massive cyber-attacks) is a scenario worth considering when testing both cyber and other P&C wordings.

## THE DEVIL IS IN THE DETAIL

Markets and companies who develop well-intended cyber exclusions must pay attention to avoid a too narrow approach to exclude cyber risk. There can always be new loss scenarios that occur which have not been thought of before they happen.

We already observe a trend whereby amendments to recently developed market exclusions (that aim to gain market acceptance and act as a common standard) are already being proposed in certain one-off deals and markets. The proliferation of amended clauses should be avoided. This introduces complexity in tracking the true cyber exposure within a portfolio and can increase risk of coverage gaps between primary and reinsurance wordings. Where market participants see flaws in commonly used clauses, these should be rectified at source with the relevant issuing market body to encourage clarity through standardisation.

## "MIND THE GAP": EXPLOITING OPPORTUNITIES

The "Phase 1" creation of cyber exclusions across all lines of business presents a "Phase 2" opportunity to then affirm coverage through intentional coverage design, risk assessment and pricing. The markets for these risks could either be taken up by the traditional cyber policies, or as properly tracked and coded gap coverages on the traditional P&C lines.

Some of the cyber market exclusions for traditional P&C lines developed thus far, go as far as excluding all malicious cyber acts and all non-malicious cyber incidents. When writing these back affirmatively, either in part or fully, particular care should be taken with respect to identifying cyber accumulation exposure granted intentionally outside of the cyber line of business. This presents a difficulty in capturing relevant exposure and incorporating the quirks of each line of business into existing cyber accumulation models (e.g. cyber accumulation exposed Event Cancellation insurance presents unique modelling challenges, due to the non-annual policy periods).

# CONCLUSION

Cyber risk is an evolving peril which poses both challenges and opportunities to the myriad of product options. A robust understanding of the risk is essential for a solid Enterprise Risk Management view. Exclusion or affirmation of cyber risk could be accompanied by some pain, but we believe it will eventually benefit both our customers and ourselves by providing clarity and narrowing any protection gaps.

The combination of hardening markets and momentum from market leaders and regulators on taking action on non-affirmative cyber presents a great opportunity for the P&C industry. Through the continuation of strong leadership, this can be carried forward across all local markets and lines of business.

As a leading global insurer, Tokio Marine Group aims to deliver safety and security to all our customers, act as a good corporate citizen and contribute to our societies. We strive to be a Good Company.

We hope this paper shines a light on the non-affirmative cyber topic, an ongoing industry-wide challenge. We hope it helps market participants to elevate their understanding of the risk, and serve their clients and societies globally and locally with higher confidence. We echo the sentiments of Munich Re and Gallagher Re: that market leaders must continue to innovate in this space – staying ahead of the curve!

## REFERENCES


- 2019 Supervisory Programme: Insurance Supervision, BaFin
- Communiqué de presse, 12 November 2019, ACPR
- Consultation Paper | CP39/16, PRA
- Cyber Risk For Insurers – Challenges And Opportunities, EIOPA
- Cyber Insurance Underwriting – Helping Boards Create Supervisory Confidence, Deloitte
- IFoA News Release, 18 October 2018, IFoA
- Insurance Insider Article, 2 April 2020, Insurance Insider
- Insurance Journal Article, 18 July 2014, Insurance Journal
- IUA Media Release, 5 June 2019, IUA
- Lloyd's Market Association Bulletin, LMA19-031-PD, LMA
- Lloyd's Market Association Bulletin, LMA20-040-DP, LMA
- Lloyd's Market Association Bulletin, LMA20-046-DP, LMA
- Lloyd's Market Association Bulletin, LMA20-047-DP, LMA
- Lloyd's Market Association Bulletin, LMA20-048-DP, LMA
- Lloyd's Market Association Bulletin, LMA21-002-TE, LMA
- Lloyd's Market Bulletin, Y5258, Lloyd's
- Lloyd's Market Bulletin, Y5277, Lloyd's
- London Company Market Statistic Report, IUA
- Visualize Article, 10 November 2020, Verisk

## CONTACT DETAILS

### TOKIO MARINE

**Taro Murakami**
Cyber Underwriting Strategist
Cyber Centre of Excellence
E :Taro.Murakami@tokiomarinekiln.com

**Ongnardo Andreas**
Cyber Actuary
Cyber Centre of Excellence
E: Ongnardo.Andreas@tokiomarinekiln.com

**Sona Kolcunova**
Cyber Risk Analyst
Cyber Centre of Excellence
E: Sona.Kolcunova@tokiomarinekiln.com

### MUNICH RE

**Rory Egan**
Senior Cyber Actuary
E: REgan@MunichRe.com

**Dr. Aiko Schilling**
Senior Underwriter - Cyber
E: ASchilling@MunichRe.com

**Karthi Indran**
Senior Underwriter – Property Treaty
E: KIndran@MunichRe.com

### GALLAGHER RE

**Jennifer Braney**
Consultancy
E: jennifer_braney@gallagherre.com

**Ed Pocock**
Senior Cyber Security Consultant
E: ed_pocock@gallagherre.com

**Jemima Hall**
Consultancy
E: jemima_hall@gallagherre.com

## ABOUT US

## ABOUT TOKIO MARINE

Tokio Marine Group consists of Tokio Marine Holdings and its subsidiaries and affiliates located worldwide, operating extensively in the non-life insurance business, life insurance business, and financial and general businesses. As the oldest and largest Japanese property/casualty insurer (established in 1879), Tokio Marine Group has been expanding its business globally from the domestic non-life insurance business to the life insurance business and the international insurance business. With a presence in 45 countries and expanding, Tokio Marine ranks as one of the world's most globally diversified and financially secure insurance groups.

## ABOUT MUNICH RE

Munich Re is one of the world's leading providers of reinsurance, primary insurance and insurance-related risk solutions. The group is globally active and operates in all lines of the insurance business. Since its foundation in 1880, Munich Re has been known for its unrivalled risk-related expertise and its sound financial position. Munich Re is a leading global provider of holistic cyber risk solutions including pre-incident and recovery services that go far beyond traditional insurance and reinsurance. It has built up significant cyber expertise, with more than 130 experts dedicated to cyber risk underwriting and related activities. It was awarded "Cyber Reinsurer of the Year" at the Advisen Cyber Risk Awards on four successive occasions between 2017 and 2020, for ongoing commitment to cyber through investment and entrepreneurialism, along with outstanding underwriting results. Munich Re continues to invest in cyber expertise and external partnerships with industry-leading technology companies in order to further support its clients with holistic cyber risk solutions.

## ABOUT GALLAGHER RE

Gallagher Re is the full service global reinsurance broking division of Gallagher, one of the world's largest insurance brokerage, risk management and consulting firms. Gallagher Re trades with 400+ clients and over 360 reinsurers, operating from global reinsurance hubs in London, Bermuda, Brazil, Chile, Miami and New York. The Gallagher Re cyber team is wholly committed to working proactively and collaboratively with both clients and markets throughout the cyber value chain. This includes the cyber consultancy practice – a "cyber centre of excellence for hire" – focused on harnessing cross-function expertise to help develop innovative solutions to specific client needs. As part of our cross-class work on cyber as a peril, consultancy services include: non-affirmative identification and quantification, framework building/validation, and (re)insurance product development.

## DISCLAIMER

Any reader of this document shall be hereby informed that whilst this document has been prepared with the utmost care on the basis of information and knowledge available at the time of drafting, all information therein are subject to uncertainty. Furthermore, this document is not intended to deal with all non-affirmative cyber topics that may exist, nor is it intended to be an exhaustive view on the topic "Silent Cyber". Considering this, Tokio Marine Group and all other authors of this document gives no guarantee as to the accuracy, completeness, timeliness and quality of the content of this document. Consequently, any use of this document including the recommendations contained therein shall be at the reader's own risk. Furthermore, Tokio Marine Group and all other authors do not accept any liability or responsibility for any loss which might be suffered as a result of any person relying on the information contained in this document.

Cover and back page image: VAlex/stock.adobe.com
Contents page image: rabbit75_fot/stock.adobe.com
Date of Issue: April 2021