

# MARSH CYBER ASSURANCE

CYBER RISK CONSULTING FOR COMMUNICATIONS, MEDIA,  
AND TECHNOLOGY COMPANIES



# CONTENTS

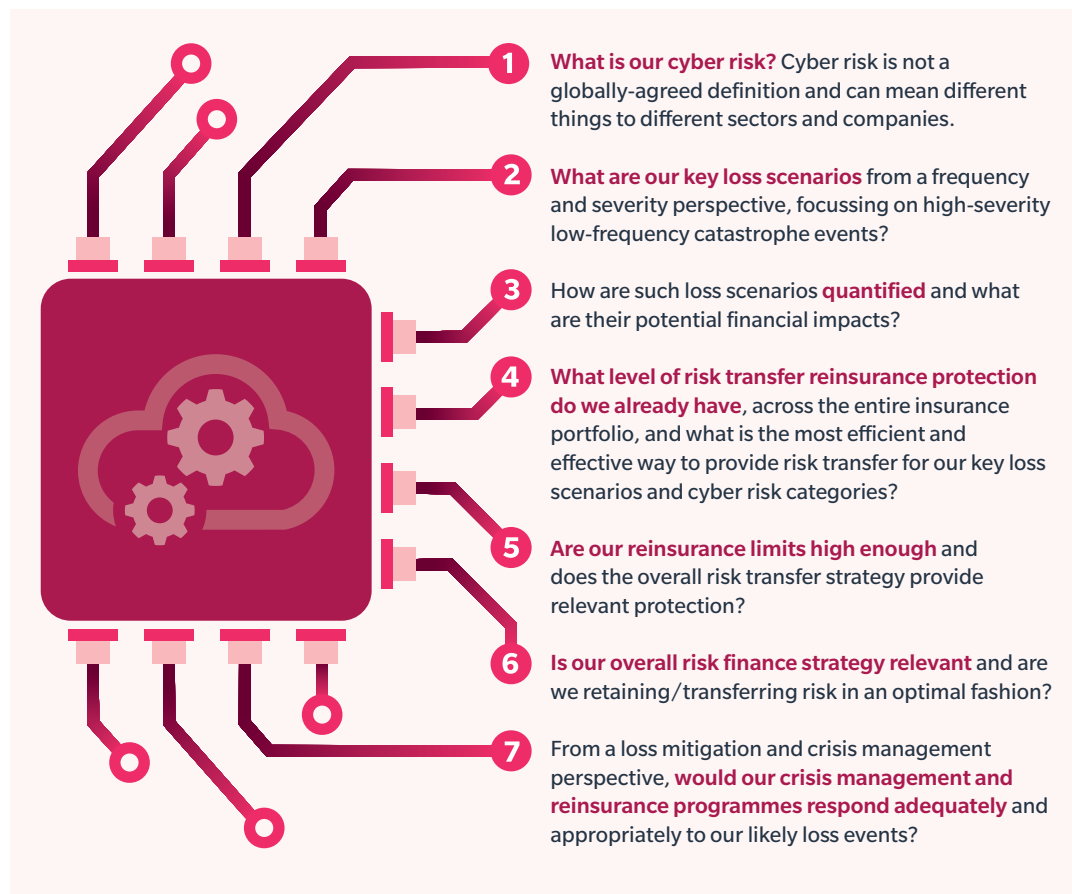
▶ Introduction	1
▶ CMT industry challenges	3
▶ What we do	5
▶ Value enhancement	6
▶ Case studies	7
▶ Conclusion	8
▶ Who we are	9

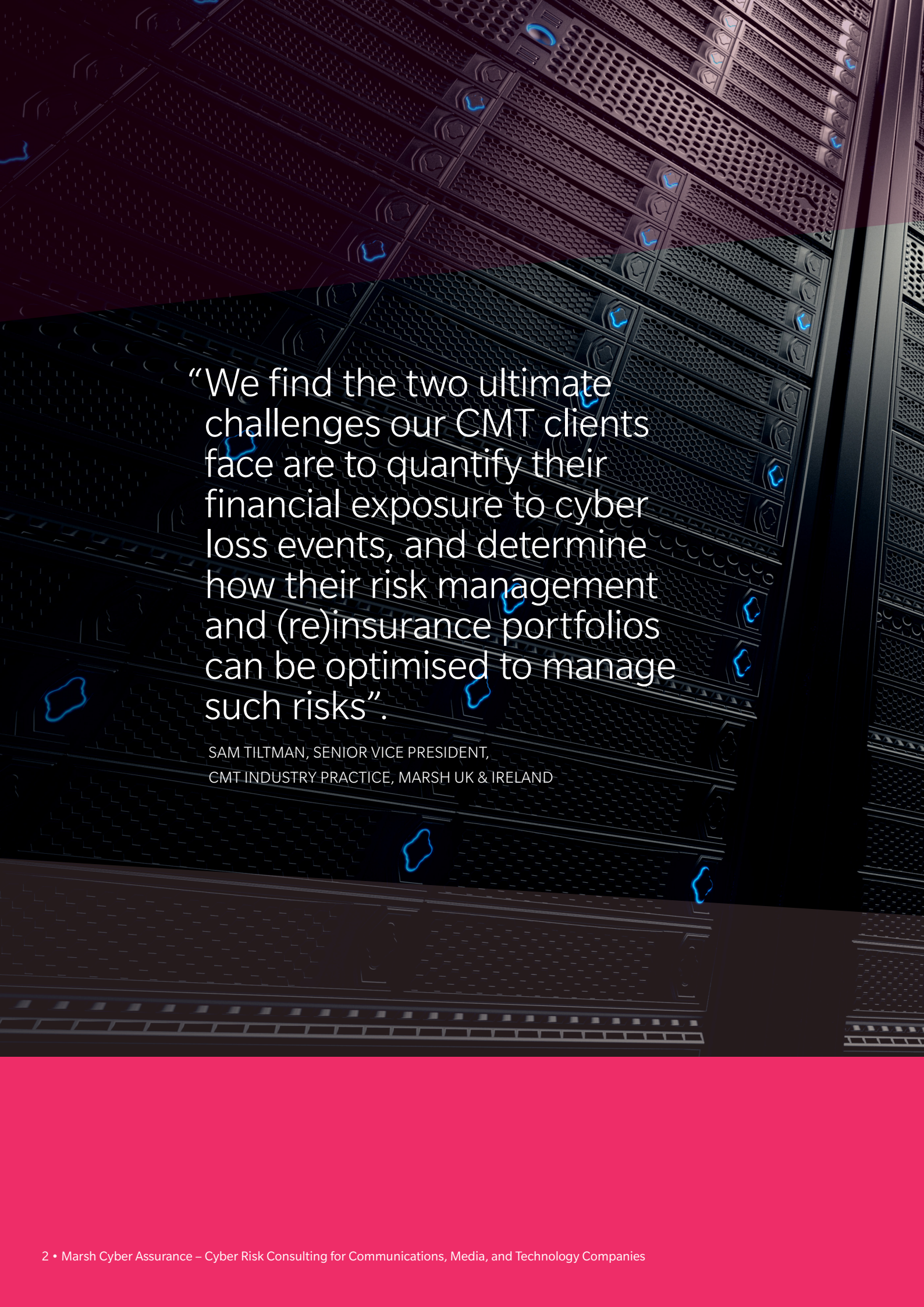
# MARSH CYBER ASSURANCE

## CYBER RISK CONSULTING FOR COMMUNICATIONS, MEDIA, AND TECHNOLOGY COMPANIES

Communications, media, and technology (CMT) industry companies are at the forefront of disruptive technologies and business models. As well as having well-established and significant intangible risk exposures, CMT companies provide products and services which inherently create, amplify, and attract cyber risks. Furthermore, they have their own industry-specific approaches to risk management and transfer (insurance) meaning they require advanced and specialised industry solutions.

For CMT companies, cyber risks are a significant component of their overall risk landscape. These challenges are typically encountered by our clients and raise the following questions:





“We find the two ultimate challenges our CMT clients face are to quantify their financial exposure to cyber loss events, and determine how their risk management and (re)insurance portfolios can be optimised to manage such risks”.

SAM TILTMAN, SENIOR VICE PRESIDENT,  
CMT INDUSTRY PRACTICE, MARSH UK & IRELAND



## CMT INDUSTRY CHALLENGE – WHAT IS OUR CYBER EXPOSURE? ARE WE NOT ALREADY COVERED?

### ISSUE

Cyber risk is not a consistently agreed global definition and can mean different things to different people. Further to this, cyber and intangible risks are “risk modifiers” which can exist across and modify other risk categories, for example, errors and omissions (E&O)/contractual risk, property damage and business interruption (PDBI), crime, management liability, kidnap, ransom and extortion, and general liability. This can make it challenging for companies to determine what level and extent of coverage they have for their cyber risks.

### SOLUTION

Through conducting a cyber risk assessment, we can define what your “cyber” risk is based upon your exposures and loss scenarios. The gap analysis component of the assessment and analysis risk transfer across all the categories of insurance (set against the loss scenarios and financial exposure) means a cross-class assessment of risk transfer is provided within a single analysis. This can enable you to:

1. Understand the level of risk transfer achieved.
2. Determine potential issues including overinsurance, coverage duplications between different policies and potential other insurance issues.
3. Identify gaps in risk transfer and ascertain optimal strategies in dealing with them.



## CMT INDUSTRY CHALLENGE – ARE WE BUYING HIGH ENOUGH LIMITS?

### ISSUE

Many CMT companies are already buying moderate to significant levels of cyber, or other, (re)insurance coverage, either within specialised CMT industry (re) insurance programmes (such as technology/media E&O, PDBI, general liability, and crime) or specific cyber (re)insurance programmes. However, many struggle to determine if their limits of indemnity and sublimits for specific loss scenarios are adequate versus the evolving exposures.

### SOLUTION

Through attaching financial exposures to loss scenarios (and hence helping our clients to quantify their cyber risks) the programme limits can be stress-tested from a loss and exposure perspective. Any deficiencies in limits, as well as coverage, are clearly defined within the Gap Analysis section of our consulting framework. We can recommend costed solutions to clearly outline how such gaps can be mitigated.



## CMT INDUSTRY CHALLENGE – DO WE NEED CYBER INSURANCE?

### ISSUE

Many CMT companies are procuring broad technology E&O/media liability/professional indemnity policies which can insure many aspects of cyber risk. They are currently considering the need for additional insurance and if indeed they need to procure cyber at all particularly pertaining to “first party” or “own costs” risks such as non-damage network/software interruption, notification costs, regulatory costs, and consumer redress costs, etc.

### SOLUTION

Through conducting a risk and exposure assessment, your current (re)insurance arrangements can be comprehensively stress tested from a:

1. Coverage (scope).
2. (Re)insurance envelope (deductible/retention and limit).
3. Crisis/claims response perspective. This process provides both clarification and validation of the current arrangements or identifies specific areas, and solutions, for improvement, ensuring the (re) insurance portfolio is relevant to the risks posed.



## CMT INDUSTRY CHALLENGE — SHOULD WE TRANSFER OUR NON-DAMAGE BUSINESS INTERRUPTION (NDBI) RISK?

### ISSUE

NDBI (software/network) is a key risk and challenge for CMT companies. Many elect to treat this as an operational risk and not one for transferring. However, many have challenges with quantifying the actual financial exposure to potential loss events, meaning the level and extent of financial impact is unknown. Furthermore, data is needed to either validate the current treatment (and retention) of such exposures, or to make decisions on which aspects, and to what extent, NDBI risk needs to be (re)insured.

### SOLUTION

Through conducting an exposure analysis and loss-scenario assessment, specific NDBI loss scenarios can be modelled from both a qualitative and quantitative perspective. The quantitative assessment can take into account:

1. The severity/frequency exposure.
2. Cost/revenue variation and seasonality.
3. Crisis management/disaster recovery.
4. Time exposure and broader loss mitigation strategies.

All of these modelled components can then be assembled to determine the overall NDBI exposure. From here the CMT company can then better appreciate their level and exposure to key loss scenarios and make informed decisions on how to manage them (risk treatment, risk mitigation, and potentially risk transfer options).

Importantly the claims and adjusting aspect of any (re) insurance response must also be carefully considered, including proofing the loss, providing appropriate evidence, and matching needs and demands for broader loss mitigation. Marsh Cyber Assurance can provide the data and insights to inform such a process.

“We link advisory directly into placement, delivering to our clients both rich insights into their cyber risk and effective insurance solutions.”

PETER JOHNSON – CYBER LEADER,  
MARSH UK & IRELAND



# WHAT WE DO

The Marsh Cyber Assurance consultancy framework for CMT companies is flexible, project-based, and can be tailored to suit your individual needs. At its most basic, the service framework consists of the following four main components (we are either engaged on a comprehensive basis or selectively across the following workstreams).

PROCESS STEP	LOSS-SCENARIO DEVELOPMENT	LOSS QUANTIFICATION	INSURANCE PORTFOLIO GAP ANALYSIS	GOING FORWARD – PROGRAMME DESIGN AND IMPLEMENTATION
<b>OVERVIEW</b>	Help you to define what cyber risk means for you by developing loss scenarios with relevant stakeholders.	How much would a cyber event cost and why? We quantify the financial exposures presented by the loss scenarios identified in the previous step.	Armed with insight into your major cyber risks and their likely impact, we can then look at how your existing (re)insurance policies would respond, and their limits relative to your financial requirements. We establish any gaps and can advise on extending or adding cover so that you have protection against losses that fall out of your risk tolerance.	Following on from the three previous steps we can determine and agree with you the optimal programme going forward together with a clear cost/benefit analysis for any insurance required to close gaps.
	Our robust loss-scenario methodology captures all loss scenarios, and their permutations, into our Loss Scenario Tool.	Our qualified accountants quantify the potential impact on your revenue via a NDBI review. Further to this, our actuaries can quantify your financial exposures, including: <ul style="list-style-type: none"> <li>• Data breach and data corruption events.</li> <li>• System outages.</li> </ul>	Our “horizontal” cross-class approach means we review (re)insurance policies horizontally against the pre-defined loss scenarios and respective financial exposures, stress testing both the extent of cover and potential (re) insurance response from a coverage perspective.	This can include options to enhance current insurance programmes or explore new/alternative solutions; based on the qualitative and quantitative data analysed from the previous three steps.
<b>DELIVERABLES</b>	Qualitative loss-scenario framework and mapping.	Loss quantification analysis.	(Re)insurance gap analysis.	Cost/benefit analysis and insurance programme options.
	Board-level report consolidating the above outputs and providing both a clear audit trail and business case for any programme optimisation options.			
<b>VALUE</b>	<ul style="list-style-type: none"> <li>• Identify and map cyber loss scenarios.</li> <li>• Bring together different teams to determine loss scenarios.</li> </ul>	<ul style="list-style-type: none"> <li>• Quantify financial exposure to your own cyber loss scenarios.</li> <li>• Attach a financial exposure to potential NDBI events.</li> </ul>	<ul style="list-style-type: none"> <li>• Support, challenge, and enhance (re)insurance strategy.</li> <li>• Understand what you are already covered for and to what extent.</li> <li>• Identify optimal techniques to transfer cyber risks.</li> </ul>	<ul style="list-style-type: none"> <li>• Optimised insurance portfolio approach to cyber risks.</li> </ul>

Projects can range from short one week projects that define risk, with the associated analyses, through to six to 12-week comprehensive assignments analysing risk on a global level and across different operating companies, divisions, and insurance markets. Our consultative approach means we design assignments to add value to the internal work and strategy of the respective risk management, security, and audit departments, focussing on quantifying the risk, testing the current risk finance arrangements, and more specifically stress testing the (re)insurance programmes to determine if they are relevant and fit-for-purpose.

# VALUE ENHANCEMENT

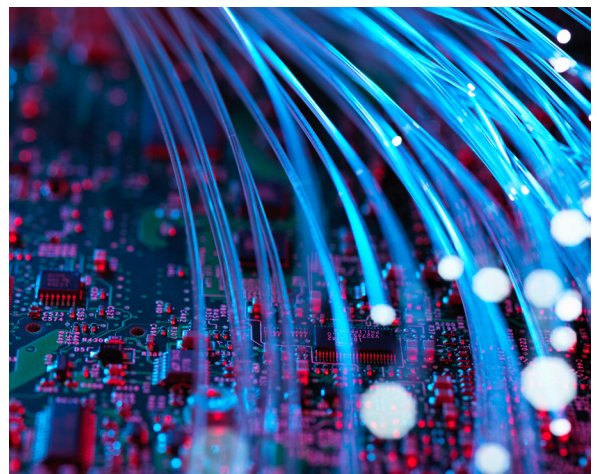
While procuring risk transfer solutions ((re)insurance) for cyber risks has been the main and well-established strategy for many CMT companies over the past few decades, the increasing severity of risks and loss events is challenging these traditional approaches. CMT companies themselves are providing products/ services which most likely are creating cyber risks for consumers and enterprise customers. With this in mind, Marsh has developed a structured approach to support CMT industry clients in responding to these key challenges.

The key value enhancement provided by our approach includes:

- Structured process – to comprehensively explore and develop highly specific CMT company loss scenarios.
- Industry experience – providing insights from working across the entire CMT industry spectrum means we have the knowledge and platform to support our clients in:
  - Developing an enhanced understanding of the nature and financial magnitude of their cyber risk profile.
  - Quantifying financial exposures to such loss scenarios.
  - Enabling them to codify risk categories, and help focus on higher-priority risks.
  - Benchmarking – loss and industry database to support internal working knowledge (including real-life industry loss events and theoretical loss scenarios, as well as the potential to conduct external threat benchmarking and non-invasive cyber reviews of critical suppliers).
- Developing a horizontal approach – we work horizontally across all insurance and risk categories meaning we both appreciate and develop solutions for cross-class risks. Our (re)insurance gap analyses are conducted by our claims experts who stress test insurance programmes from a claims perspective.
- Focusing on NDBI loss scenarios and quantifying the financial exposures – crucial for many CMT companies which rely on availability of services, networks, and data.
- Practical working experience:
  - An awareness and practical experience of how complex composite claims can occur across multiple (re) insurance programmes.
  - Understanding of the different (re)insurance possibilities available to CMT industry companies in transferring their cyber risks.
  - Actual working experience and knowledge of how cyber claims develop for CMT industry companies.

“The increasing severity of risks and loss events is challenging traditional approaches. Marsh’s approach supports CMT industry clients to respond to these key challenges.”

CARRICK LAMBERT – CMT INDUSTRY PRACTICE  
LEADER, MARSH UK & IRELAND





# CASE STUDIES



## ADDING VALUE TO THE COMMUNICATIONS SERVICES INDUSTRY SECTOR

### ISSUE

A diversified global telecommunications operator did not have any specific insurance protection for business interruption (BI) losses arising from non-damage (cyber) events. The client wanted to understand what may cause a NDBI incident within the context of cyber.

### MARSH SOLUTION

Marsh undertook a detailed study to deliver an opinion on actual and potential cyber risk scenarios including maximum foreseeable loss calculations for identified scenarios in its operations. Marsh also calculated the normal loss expectance for critical failure points by each scenario for each operation, taking into account pre/post loss controls and workarounds in place. Finally, the team reviewed to what extent a cyber BI insurance policy might reflect the client's risk profile and how future planned changes would impact the cyber risk and exposures faced by the client.

### THE RESULT

The client gained a detailed insight into the type of potential risk faced, where they would manifest, and how they would impact specific business units within the organisation. Additionally, the process ensured the insurance buying process was optimised for their renewal and the broking process supported, with opportunities for improving resilience.



## ADDING VALUE TO THE MEDIA INDUSTRY SECTOR

### ISSUE

A major broadcasting company needed guidance and support in (i) determining its cyber risk profile, (ii) identifying loss scenarios, and (iii) quantifying such exposures (from a frequency and severity perspective). Before the process began, there wasn't a consensus on what their cyber risk was, their potential financial exposure, and the extent of insurance protection already afforded (and if indeed this was appropriate).

### MARSH SOLUTION

Marsh undertook a detailed cyber risk assessment review which included workshops composed of people from across the client organisation. The main focus was to establish likely potential loss scenarios and model how they would play out; this work also undertook a risk maturity assessment and benchmarking using Marsh's comprehensive database. The project team also undertook a composite insurance programme analysis to determine the level of risk transfer achieved for the loss scenarios, as well as identifying issues and gaps in risk transfer.

### BENEFITS

An increased insight into cyber exposures and loss scenarios (categorised and mapped), quantified exposures (frequency and severity), hard data to support decision-making (on risk management and insurance activities), and improved governance/risk management. The process also acted as a great platform to bring together multiple different stakeholders to collaboratively determine their cyber loss scenarios.



## ADDING VALUE TO THE TECHNOLOGY INDUSTRY SECTOR

### ISSUE

A large European semiconductor client was concerned by their BI risk presented by cyber-type triggers such as hack-attack, extortion, and errors/omissions leading to an interruption in the supply chain.

### MARSH SOLUTION

The Marsh team identified a number of loss scenarios through working with key elements of the client's management and operations. This included issuing a survey to obtain information across multiple departments. The team then modelled the client's exposure based on the data records and BI events. This resulted in modelled financial exposures.

### THE RESULT

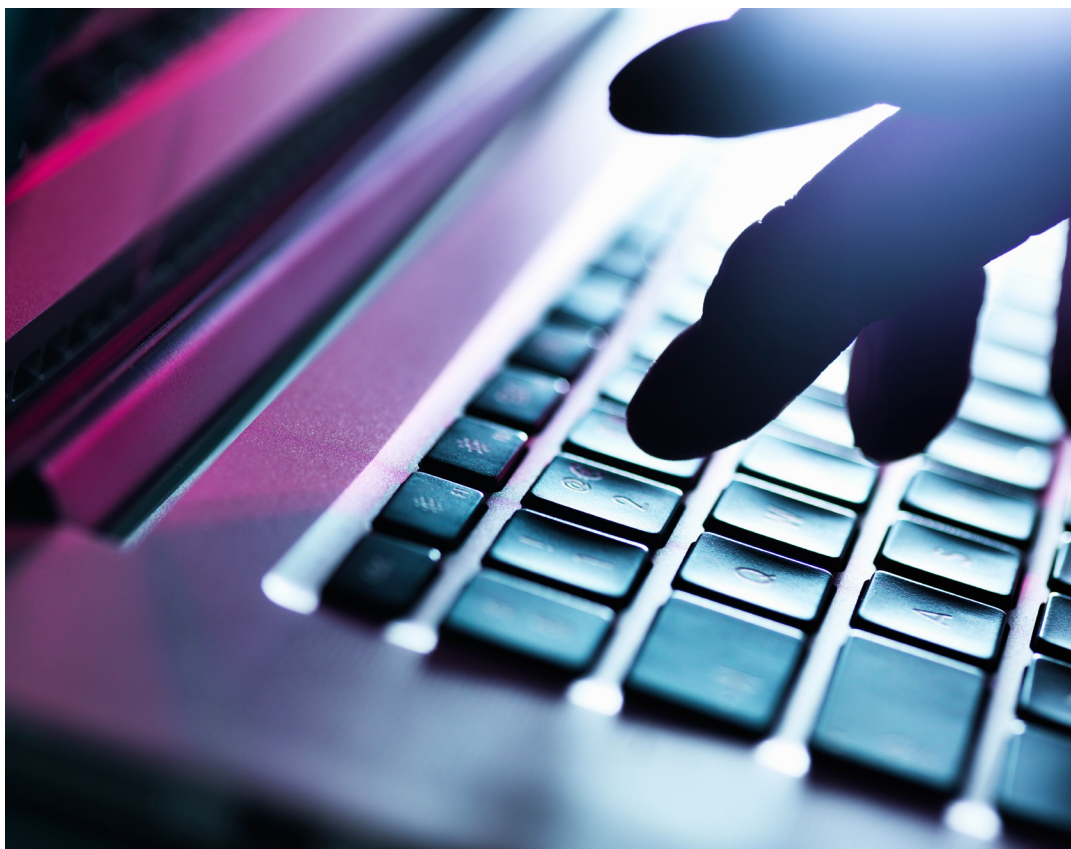
The client not only had detailed information to support their risk management processes, but were also able to make informed decisions on the type of cyber insurance they needed to procure, including limits, the extent of coverage, and deductible levels. A further benefit of running the project was that it obtained a significant amount of the data and information which was subsequently required by insurers to underwrite the risk.

# CONCLUSION

Marsh Cyber Assurance consulting services for CMT companies can enable you to:

- Identify and further develop your cyber loss scenarios.
- Benchmark your loss scenarios, external exposure to threats, and (re)insurance programmes.
- Quantify financial exposures to cyber loss scenarios, importantly including both data/network breach type events as well as non-damage BI scenarios.
- Have comprehensive information and insight which can enable you to:
  - Make better-informed decisions.
  - Stress test current risk management and (re) insurance programmes.
  - Further develop and tailor your risk management strategies.
  - Structure new/enhance (re)insurance solutions based on the data provided.

Importantly, the majority of our CMT clients have cutting-edge risk management and IT security functions, and work with us to assist them in bridging the gap across their different departments, ensuring their (re)insurance portfolio is aligned to their loss scenarios, risk management approach, and crisis management frameworks.



# WHO WE ARE

Marsh is a global leader in insurance broking and innovative risk management solutions. Our CMT Industry Practice is dedicated to helping you identify, quantify, manage, and mitigate your composite risks.

Most companies that operate in the CMT industry sectors are on the frontier of emerging risks, pushing boundaries with their business models and disrupting industries. This means they require tailored advice and customised solutions which go way beyond “standard”. Our flexible approach combined with our significant human and knowledge resources enables us to advise across the entire journey of risk services, or advise on specific projects, risk categories, or challenges.

Marsh Risk Consulting (MRC) helps organisations to manage their risk strategically, with bespoke solutions designed to meet not only risk management objectives, but also overall business goals. Using industry-leading data and analytics, we evaluate an organisation’s exposures and risk management programme gaps, helping decision makers to determine the return on investment and make informed decisions about programme adjustments and direction.

MRC is made up of a team of circa fifty professionally and technically qualified risk consultants who can help an organisation change and manage its risk profile in such a way that improves resiliency, reduces future claims, and minimises risk costs.



For more information on Marsh Cyber Assurance, please contact any of the following:

PETER JOHNSON  
Cyber Leader, UK & Ireland  
Marsh Risk Consulting  
+44 (0)20 7357 3527  
peter.a.johnson@marsh.com

SAM TILTMAN  
Head of Business Development, Communications, Media, and Technology  
Marsh UK & Ireland  
+44 (0)20 7357 3255  
sam.tiltman@marsh.com

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

Marsh Ltd is authorised and regulated by the Financial Conduct Authority.

Copyright © 2017 Marsh Ltd All rights reserved

GRAPHICS NO. 17-0784

