MARSH

TECHNOLOGY INDUSTRY PRACTICE

Marsh Cyber Risk Management

Cyber Risk Consulting For Technology Companies

MARSH & McLENNAN COMPANIES

Contents

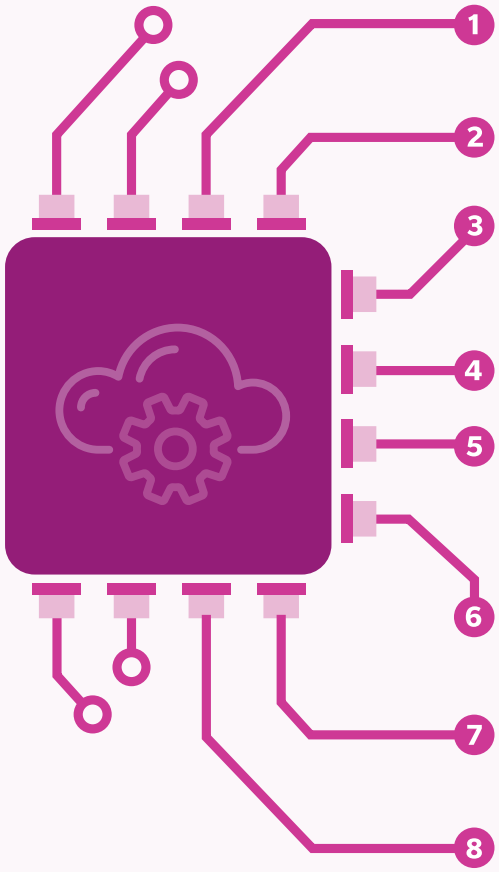
Marsh Cyber Risk Management	1
Technology Industry Challenges	3
What We Do	5
Value Enhancement	4
Case Studies	7
Conclusion	8
Who We Are	9

Marsh Cyber Risk Management

Cyber Risk Consulting for Technology Companies

Technology industry companies are at the forefront of disruptive technologies and business models. As well as having well-established and significant intangible risk exposures, technology 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 ((re)insurance), meaning they require advanced and specialised industry solutions.

For tech 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:



1. **What is our cyber risk?** Every organisation has different cyber exposures and the potential impact on an organisation is constantly evolving.
2. **How mature is our cyber security?** Does it match our cyber risk landscape?
3. **What are our key loss scenarios** from a frequency and severity perspective, and how do our existing controls mitigate them, focusing on high-severity low-frequency catastrophe events?
4. How are such loss scenarios **quantified** and what are their potential financial impacts?
5. **What level of risk transfer reinsurance protection do we already have,** across the entire insurance portfolio, and what is the most efficient and effective way to provide risk transfer for our key loss scenarios and cyber risk categories?
6. **Are our (re)insurance limits high enough** and does the overall risk transfer strategy provide relevant protection?
7. **Is our overall risk finance strategy relevant** and are we transferring, retaining and managing risk in an optimal fashion?
8. From a loss mitigation and crisis management perspective, **would our crisis management and (re)insurance programmes respond adequately** and appropriately to our likely loss events?

We find the two ultimate challenges our technology 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,
TECHNOLOGY INDUSTRY PRACTICE, MARSH UK & IRELAND

TECHNOLOGY INDUSTRY CHALLENGE

What Is Our Cyber Exposure?

ISSUE

Cyber risk has no consistently agreed definition and means different things to different sectors and companies. Every organisation has different cyber exposures and while there are commonalities in the exposures themselves, the potential impact on an organisation is constantly evolving. This can make it challenging for companies to determine what level and extent of risk management they have for their cyber risks, both in terms of coverage and existing cyber risk mitigation strategies.

SOLUTION

Through conducting a cyber risk assessment, we can define what your "cyber" risk is based upon your exposures and loss scenarios, mapping your existing risk mitigation controls to understand residual risks.

Quantification of your exposure provides greater clarity as to the potential impact of a cyber event, providing a business case for investment in cyber risk management. Having determined the level of controls already in place, our insurance analysis highlights your current level of risk transfer, gaps in your risk transfer and strategies to address the gaps (in both transfer and risk mitigation) and determine potential other insurance issues including over-insurance and coverage duplications between different policies.

The option to conduct a gap analysis across all categories of insurance (set against the loss scenarios and financial exposure) provides a comprehensive view of your coverage in relation to cyber and would highlight any gaps in cover introduced by the Lloyd's 'Silent Cyber' initiative.

TECHNOLOGY INDUSTRY CHALLENGE

Do We Need Cyber Insurance?

ISSUE

Many technology 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.

TECHNOLOGY INDUSTRY CHALLENGE

Are We Buying High Enough Limits?

ISSUE

Many technology companies are already buying moderate to significant levels of cyber, or other, (re)insurance coverage, either within specialised technology 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.

TECHNOLOGY INDUSTRY CHALLENGE

How Do We Evaluate the ROI of Cyber Security Spend?

ISSUE

Tech organisations typically have extensive information security measures in place. Evaluating the effectiveness of controls on your cyber exposure is challenging, as it requires a detailed understanding of the potential business impacts from cyber events and the ability to quantify financial exposures.

SOLUTION

Utilising our advanced cyber analytics platform, we can model your cyber exposures using detailed threat and controls information, with the following benefits:

1. Compare your management of cyber risk to industry peers.
2. Facilitates investment decision making based on reduction to overall exposures.
3. Demonstrates return on investment from risk spend.

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

JANO BERMUDES, HEAD OF CYBER RISK CONSULTING, TECHNOLOGY INDUSTRY PRACTICE, MARSH UK & IRELAND

What We Do

The Marsh Cyber Risk Management consultancy framework for Technology 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	Cyber Maturity Assessment	Loss-Scenario Development	Loss Quantification	(Re)insurance Portfolio Gap Analysis
OVERVIEW	Assess technical control maturity through Marsh assessment.	Help you to define what cyber risk means for you, in the context of your business, by developing loss scenarios, and working with a breadth of stakeholders to develop, validate, and score the identified risks.	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.
	Our maturity assessment is aligned to multiple leading cybersecurity frameworks to give you an overview of your current cybersecurity maturity.	Our loss scenario methodology captures a broad view of your cyber risks, detailing cause, consequence, and impact, while mapping these to your control landscape.	Our qualified actuaries quantify the potential cost of your cyber exposures to the business. Our forensic accounting teams can also model the potential impact of a Cyber Business Interruption event on your revenue.	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.
DELIVERABLES	Cybersecurity maturity scores against each of the NIST Cybersecurity Framework domains.	Comprehensive stand-alone risk register document, detailing cause, consequence, impact and controls, prioritised by risk score.	Loss quantification analysis of your cyber exposures, providing a breakdown of key cost drivers and impacts.	Insurance gap analysis document, detailing coverage probability rating for each business impact applicable to each scenario.
	Board-level report consolidating the output, and providing a clear audit trail, actionable recommendations and roadmap, and a business case for any improvement options.			
VALUE	These scores provide a starting point for loss scenario and quantification focus, as well as aiding in insurance placement.	Independent and objective view of key cyber loss scenarios. Involvement of teams across the organisation to understand and articulate the true impact of cyber event.	Understand financial exposures to bespoke loss events to inform insurance limits, and justify cybersecurity spend.	Ensure insurance programme keeps pace with evolving cyber risk profile and threat landscape. Understand the extent to which non-cyber policies cover the identified cyber risks. Identify optimal techniques to transfer cyber risks.
	Optimised cyber risk management programme, focussed on cost-effective and targeted improvements.			

Projects can range from short one week projects that define risk, with the associated analyses, through to extended 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 technology companies over the past few decades, the increasing severity of risks and loss events is challenging these traditional approaches. Technology 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 technology 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 technology company loss scenarios.
- **Industry experience –** providing insights from working across the entire technology 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 technology 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 technology industry companies in transferring their cyber risks.
  - Actual working experience and knowledge of how cyber claims develop for technology industry companies.
  - Extensive experience in cyber security strategy and transformation.
  - Previous incident response expertise of managing cyber events, for both insured and uninsured organisations.

> ***"The increasing severity of risks and loss events is challenging traditional approaches. Marsh's approach supports technology industry clients to respond to these key challenges."***
>
> **CARRICK LAMBERT, LEADER,**
> **TECHNOLOGY INDUSTRY PRACTICE, MARSH UK & IRELAND**

Case Studies

Adding Value To The Communications Services Industry Sector

BACKGROUND

The client – a multinational telecommunications and consumer electronics company – already had some level of cyber cover under its existing E&O policy, and was seeking to understand how well this cover aligned to its cyber risks, as well as whether a specialised cyber policy would be a valuable addition to its insurance portfolio. It asked Marsh to evaluate its existing cover and compare this to the cyber cover available.

MARSH SOLUTION

We started by analysing the cyber risks already being tracked by the client, and mapping these to the Marsh cyber risk taxonomy. After assigning business impacts to each cyber risk, we worked with our legally qualified Complex Claims team to determine a probability of coverage for each of the business impacts, for each risk, to create a coverage heat map for the existing E&O policy. We then worked with our specialist cyber brokers to map the cyber cover available for each of the business impacts to compare the two coverage options, and provided recommendations for moving forward.

IMPACT

A clear overview of the different coverage areas provided by cyber in addition to the existing E&O coverage was provided, alongside recommendations to enhance the existing coverage to mitigate coverage gaps identified. This enabled decision making by presenting the optimal risk transfer strategy based on the business impacts identified.

Adding Value To The Fintech Industry Sector

BACKGROUND

The client – a UK-based FinTech company providing payment automation services across a number of industries – was looking to better understand the breadth of its cyber risks, as a rapidly growing and complex business. It asked Marsh to assist in articulating its cyber loss scenarios, conduct a quantification exercise for an internal fraud scenario and unpick the insurance arrangements required across its complex cyber risk profile.

MARSH SOLUTION

We reviewed the client's targeted data and interviewed key stakeholders to better understand its core business activities and existing risk profile, identify the cyber loss scenarios the client faces and the potential gaps or unexplored avenues, and clearly articulated these to C-suite stakeholders. This involved developing and workshopping 17 cyber risks with the stakeholders, to articulate the impacts and controls associated with each scenario.

We also developed a bespoke scenario for quantification, collecting additional data to create inputs for a customer financial exposure model. Additionally, we used inputs from loss scenario development and the bespoke quantification exercise to produce financial exposure figures for a data breach scenario, in order to help the client understand its exposures to the large amounts of PII and PCI records it holds.

IMPACT

Mapping out and articulating the insurability of each business impact in each loss scenario – cyber, professional indemnity and commercial crime coverage – and linking to the renewal strategy, provided actionable recommendations on the client's insurance programme and risk management programmes. Our detailed approach ultimately allowed the client to understand how to comprehensively insure its cyber risk profile.

Adding Value To The Software Industry Sector

BACKGROUND

The client – a UK-based software provider, focused on assuring data security with uptime guarantees for critical public services – was looking to better understand the breadth of its cyber risks and whether its current insurance programme adequately covered its risk profile. Marsh were asked to assist in articulating its cyber loss scenarios, by interviewing key stakeholders across the business and analyse its existing insurance cover against its identified loss scenarios to identify any gaps.

MARSH SOLUTION

We reviewed the client's targeted data and interviewed key stakeholders to better understand its core business activities and existing risk profile, identified 16 cyber loss scenarios the client faced, with a particular focus on data security, and system interruption risks impacting critical public services, and clearly articulated these to C-suite stakeholders. Having validated the scenarios with the project sponsors and information security to ensure that all relevant details were present, we worked with our legally qualified Complex Claims experts to assess the level of insurance coverage under three carefully selected insurance policies, providing a probability of coverage rating for each business impact within each identified loss scenario. Following this, we worked with the broking and client servicing teams to provide actionable recommendations for the client to close any gaps in its insurance programme, and provided risk management recommendations to further enhance the client's control environment.

IMPACT

The review identified critical gaps in cover, due to the recent expansion of the company and subsequent evolution of the client's cyber risks profile, for which we provided actionable recommendations to close these gaps, both through insurance and risk management controls.

Conclusion

Marsh Advisory is well positioned to support you in managing your cyber risk. Our experienced team link cyber security expertise to knowledge of the insurance industry, providing a holistic approach to managing cyber risk. Our consulting solutions enable you to:

- Analyse and benchmark your cyber security maturity.
- Identify and further develop your cyber loss scenarios.
- Quantify financial exposures to cyber loss scenarios and map your exposures to control effectiveness.
- Prepare your response through planning and carrying out exercises.
- Have comprehensive information and insight which can enable you to:
  - Make better-informed decisions.
  - Respond to, and recover from, cyber events.
  - Stress test current risk management and (re) insurance programmes.
  - Further develop and tailor your risk management strategies.

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

Who We Are

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

Most companies that operate in the Technology 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 Advisory, Consulting Solutions 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.

Marsh Advisory, Consulting Solutions is made up of a team of 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 Risk Management, please contact any of the following:

JANO BERMUDES
Head of Cyber Risk Consulting,
UK & Ireland Marsh Advisory, Consulting Solutions
+44 (0) 20 7357 1456
jano.bermudes@marsh.com

SAM TILTMAN
Senior Vice President
Technology Industry Practice, Marsh UK & Ireland
+44 (0) 20 7357 3255
sam.tiltman@marsh.com

Insurance Brokers
Chartered