MARSH

TECHNOLOGY INDUSTRY PRACTICE

Business Interruption and Resilience for Technology Companies

MARSH & McLENNAN COMPANIES

Technology companies are at the forefront of change: recent technological advancements, as well as challenging economic conditions, are presenting numerous challenges for those stakeholders responsible for risk and insurance. Furthermore, the significantly worsening insurance market conditions are making risk transfer more difficult, restrictive and expensive. How can technology companies proactively prepare themselves for such risk exposures and related insurances and risk management strategies?

Introduction

Technology companies are seeing greater pressure on insurance pricing and market capacity for Business Interruption (BI) insurance cover. As insurers are remaining cautious in the levels of BI risk that they are underwriting, being able to accurately map, quantify and declare holistic BI exposures will go a long way to mitigating these challenges.

Furthermore, understanding the loss scenarios and financial impact of business interruption events is a key factor in the broader risk management process for technology companies. And having hard data combined with deep insights enables our clients to make informed risk management decisions.

Marsh Technology Industry Practice Sectors

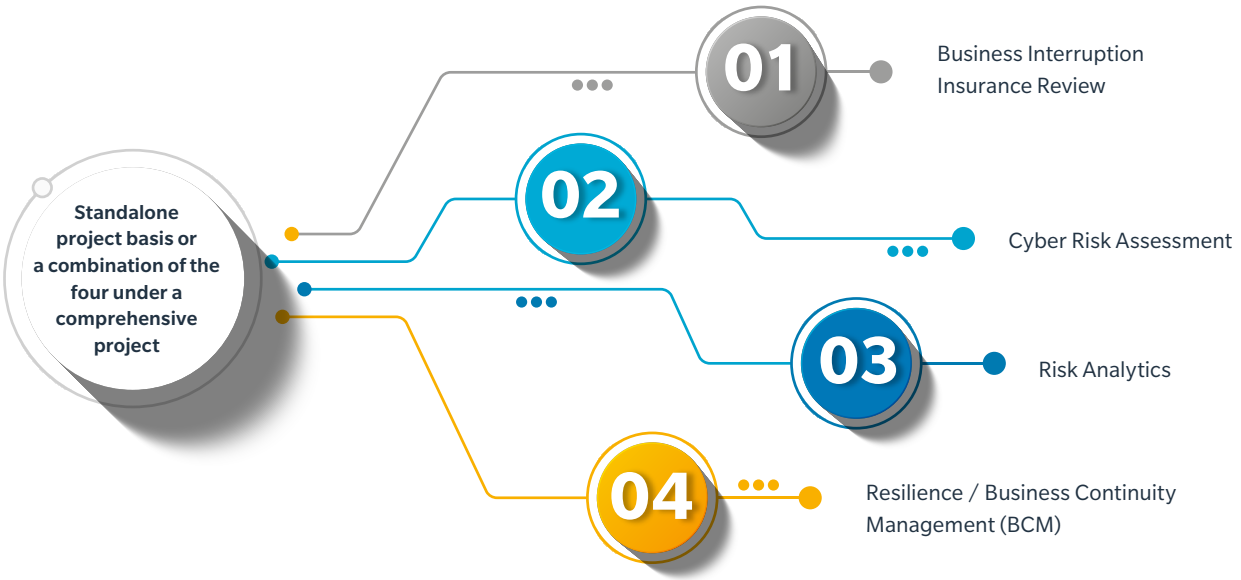
Challenges and Questions for Technology Companies

- Do we have BI exposure and to what extent do we need to transfer (insure) it?
- What is our quantified financial exposure to business interruption?
- Has our changing use of technology, and related infrastructure/services, evolved our BI risk exposures and required insurances?
- What is our own unique financial exposure to cyber non-damage business interruption (NDBI) type events?
- Is our business resilience and continuity management fit for purpose, taking into account recent economic and technological developments?

How Marsh is Helping Technology Companies

In order to help our clients respond to such challenges, we have developed a composite business interruption and resilience service composed of four work streams. These work streams can be deployed on a standalone project basis or together under a comprehensive project.

Ultimately, through our dedicated risk advisory division, we can provide outputs reviewing and quantifying your fundamental BI exposures; quantifying your insurable risk profile; and, if required, supporting with business resilience measures.



01

Business Interruption Insurance Review

Through our Business Interruption and forensic accounting expertise, a fundamental component of our collective BI risk advisory proposition is our Business Interruption Insurance Review.

Across all business sectors, the rate and extent of change, be it in processes, technology, or business to business relationships, can fundamentally affect a company's BI exposures. Insurance and risk financing arrangements can struggle to keep pace with business needs in such an environment, and unfortunately, for many organisations, this only becomes apparent when a major loss occurs.

A BI Insurance Review focuses on your BI exposures and involves a comprehensive identification and evaluation of an organisation's business interruption exposures (including estimated maximum loss calculations); both at owned premises and within the wider supply chain. We provide assessment of insurable exposures, key vulnerabilities and operational interdependencies, together with an understanding of how losses arise, the resultant business impact and the ensuing costs that can occur. Additionally, we validate the existing insurance programme and identify any major gaps in cover and can also take into account business continuity options (as detailed later).

The objective of a BI Insurance Review is to provide confidence in the insurance product and the best chance of recovering financial losses if the policy is tested by a major claim. We provide clients with a technical report addressing the adequacy of your current policy arrangements with recommendations for possible improvements. This includes strategic advice on the status of any existing business continuity management programme, ensuring a clear link between insurance and risk management.

Our core approach is to review the BI exposures of the key operating locations that could be subject to physical loss or damage, to ensure that such exposures are fully evaluated and mitigation measures are understood.

In particular, our (re)examination of the BI insurance programme design considers the appropriateness, correctness or best fit of the:

- **Current basis of BI insurance cover.**
- **BI Declared Values.**
- **BI Sums Insured.**
- **Indemnity periods.**
- **Intergroup dependency exposures.**
- **Supplier and Customer dependencies.**
- **Policy extensions taken out or available**.

The following factors are all key drivers for a BI Insurance Review:

1. Threat or reality of premium increases and restrictions on cover (both capacity and terms).
2. Corporate governance and new financial reporting legislation.
3. Pressure from the insurance market for companies to more closely analyse the BI risk and to put risk control measures in place.
4. Insurer demands for better underwriting information.
5. The need to understand the supply chain fully and identify single points of failure and critical assets.

02

Cyber Risk Assessment

Technology, systems and data are foundational components of organisations in the Technology space, leaving them particularly exposed to cyber risk.

Cyber events can be disruptive to operations but can also result in reputational damage, particularly for those organisations with public profiles based around technology and digital presence: adverse cyber events undermine customers' trust in your business. Understanding the impacts of non-tangible cyber events, such as breaches of personal data, loss of intellectual property and misrepresentation, is key to understanding your risk profile.

In a Marsh cyber risk assessment, our focus is your business, understanding how technology underpins core operations to determine where cyber events could result in brand, reputational, regulatory and financial implications.

We work with organisations through workshops and interviews/discussions with key internal stakeholders (i.e. the Chief Information Security Officer, IT, Security, Risk, etc.) to understand technology infrastructure, any existing controls in place and understand, develop and quantify cyber loss scenarios.

By viewing cyber risks through loss scenarios, rather than generic cybersecurity standards and frameworks, you can prioritise risk management based on the potential business impact. We can help you to understand, measure and manage your cyber risk.

03 Risk Analytics

Core Exposure Modelling and Risk Finance Optimisation

Through our team of actuaries and analysts, we can build predictive models that forecast an organisation's Property Damage (PD)/BI, NDBI and/or Cyber loss exposures – incorporating the outputs of a BI review, a Cyber risk assessment, or both.

Using our proprietary stochastic modelling software, we will project insurable PD/BI, NDBI and/or Cyber losses for the forthcoming policy period – presenting annual aggregate losses at multiple probabilities (e.g. average annual losses, 1 in 5 year losses, 1 in 200 year losses, etc.). We then overlay your current insurance programme and a range of alternative programme structures.

These outputs then enable us to:

- **Identify the optimal insurance programme structure or wider risk financing strategy.**
- **Present projected retained and transferred loss costs; with the former being useful for budgeting purposes and the latter helping target and challenge pricing in the insurance market.**
- **Quantify gross (i.e. without insurance) loss potential – effectively illustrating your PD/BI, NDBI and/or Cyber risk profile.**

For Cyber risk specifically, we can incorporate the results from a Cyber Risk Assessment and utilise our proprietary Marsh cyber quantification models to quantify the BI loss impact of a systems outage event. We have also developed a bespoke model for clients whose revenue stems from subscriptions, rather than discrete transactions.

When both a BI Review and Cyber Risk Assessment have been conducted, we can also overlay detailed information on key network segregations. We would then also be able to take into account aggregation risks across data centres and revenue loss from different revenue generating activities.

Catastrophe Exposure Modelling

Through a combination of additional proprietary modelling software (Sunstone™) and market-leading third-party underwriting software respectively, we can also quantify PD/BI losses emanating from terrorism and natural catastrophe exposures.

Modelled PD/BI losses for both are again presented on an annual aggregate basis at various probabilities, as well as on a per event basis. Terrorism PD/BI loss exposures can also be calculated on a Probable Maximum Loss (PML) basis.

For natural catastrophe exposures, losses are presented individually for: each of the main perils (i.e. earthquake, storm and flood); each country/region; and each of the most exposed sites.

Data quality is a key factor in catastrophe modelling, meaning we require detailed information on each asset to accurately project potential losses. This information includes (but is not limited to) items such as the following, for each asset/location:

- **Total Insurable Value (PD + BI).**
- **Construction type.**
- **Occupancy type (e.g. warehouse, factory, office, etc.)**
- **Year built.**
- **Number of stories.**

Outputs from both terrorism and natural catastrophe exposure modelling can be incorporated into wider work around Risk Finance Optimisation.

04

Resilience/ Business Continuity Management (BCM)

Ensuring resilience is crucial in the Technology sector, in order to maintain continuity of service and withstand disruption. The public nature of this industry means that increased scrutiny of crisis management is likely; therefore the implementation of mechanisms to enhance resilience and maintain stakeholder confidence is essential.

At Marsh, we approach resilience through an industry-specific lens, understanding the unique challenges that organisations in the Technology sector face. We follow a systematic methodology to evaluate an organisation's priorities and then help to implement appropriate mitigation measures in response to potential threats. Marsh follows a top-down approach to firstly ensure that the right governance structures are in place to respond, and then develop workable response arrangements to manage key risks. We understand that resilience is only possible when the right mechanisms are in place, so our continuity plans outline measures to ensure swift decision making clearly – defined roles, communications and escalation protocols, and stakeholder management. The result of which is an organisation with the capability to respond swiftly, mitigate losses and maintain stakeholder confidence.

Marsh is able to support organisations in enhancing their resilience through offerings including business continuity plan development, crisis response team training, review of existing arrangements and scenario exercise facilitation.

Collective Benefits of Marsh's Business Interruption and Resilience Service for Technology Companies

	Better Underwriting Information	Increased Negotiating Strength with Insurers	Tailored Coverage (Ts&Cs and/or Structure)	Stakeholder Assurance and Corporate Governance	Improved Event Recovery (Speed & Cost)	Improved Understanding of Exposures and Loss Volatility	Smoother Claims Settlement Process
BI Insurance Review							
Cyber Risk Assessment							
Risk Analytics							
Resilience /BCM							

Case Studies

Case Study 1 INTERNATIONAL MOBILE TELECOMS OPERATOR

THE PROBLEM

A multinational telecommunications client commissioned Marsh to review their Business Interruption (BI) exposures in four of their key mobile telecoms markets, in addition to prior reviews for four of their other markets.

Given the nature of the client's business and product/service offering, the relationship between a potential physical damage event and their BI exposures was highly complex and required specialist knowledge to review.

THE SOLUTION

We deployed our forensic accounting expertise to conduct meetings with key senior personnel from the client's businesses, within each country – including representatives from: Finance, Operations, Logistics and Procurement.

At a high level, this review comprised of five key elements:

1. Financial Analysis
2. Operations Analysis
3. BI Potential Maximum Loss Analysis
4. BI Insurance Comments and Recommendations
5. High level Business Continuity Management recommendations

More specifically, our review covered: key risks, population coverage, key markets and demographics, network infrastructure (including crisis and disaster recovery), revenues and churn, and strategic and financial planning (amongst many other factors); all with the objective of mapping current and future revenues and dependencies vs. risk.

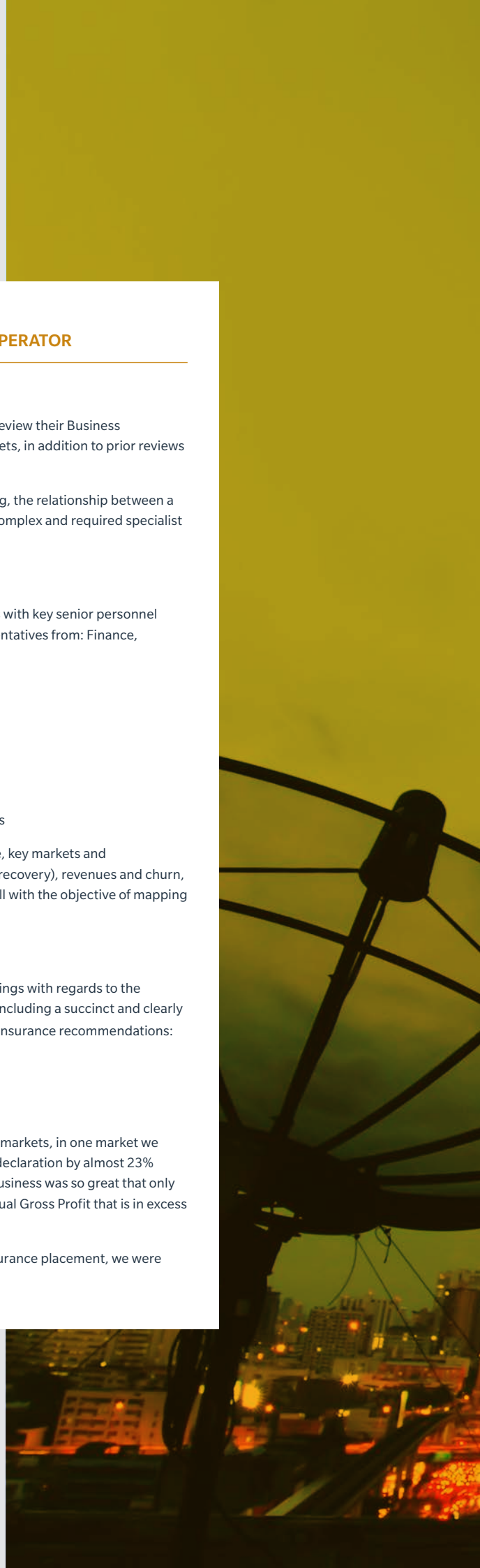
THE RESULT

Our BI specialists presented a holistic final report detailing their findings with regards to the client's BI exposures in contrast to the existing insurance coverage; including a succinct and clearly summarised table with three, colour-coded headings concerning BI insurance recommendations:

1. Maintain as existing (Green)
2. Review (Yellow)
3. Change (Red)

Amongst a broad range of recommendations across the client's four markets, in one market we recommended that the client reduce their Gross Profit sum insured declaration by almost 23% compared to prior year and in another, the level of resilience in the business was so great that only nominal Gross Profit was deemed to be at risk, in contrast to the annual Gross Profit that is in excess of USD1bn.

In addition, with the outputs of our review being so critical to the insurance placement, we were actually able to fully fund the project with an insurer bursary.



Case Study 2 DIVERSIFIED GLOBAL TELECOMS OPERATOR

THE PROBLEM

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 an NDBI incident within the context of cyber.

THE 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.

Case Study 3 DIVERSIFIED GLOBAL TELECOMS AND IT SERVICES COMPANY

THE PROBLEM

A large telecommunications company, with an extremely diverse technological offering was looking to understand their Business Interruption (BI) exposure for more than 12,000 buildings and sites. Prior to the work that Marsh conducted, there was limited knowledge as to the suitability of the breadth and depth of the BI insurance coverage that the company purchased.

THE SOLUTION

Our Claims Solutions team, comprised of forensic accountants and experts in quantifying interruption losses, worked to understand the location-specific implications of a multitude of events and the corresponding impact that this would have on the company's revenue, ranging from large commercial contracts to the bespoke services offered to multinational companies.

THE RESULT

By aggregating the information found on a location-specific basis, the team were able to provide key client stakeholders with a holistic view of the potential BI costs, allowing a better understanding of the risk profile throughout and hence helping to make well-informed decisions regarding insurance coverage, attachment points and limits.

Case Study 4 GLOBAL PROVIDER OF FINANCIAL MARKET DATA AND INFRASTRUCTURE

THE PROBLEM

After a challenging prior renewal, our client wanted to remarket their global Property Damage & Business Interruption (PD/BI) insurance programme with the objective of moving to another insurer at the coming renewal.

This was made difficult by a number of factors:

1. The client lacked holistic and accurate underwriting information (particularly PD and BI declarations).
2. The incumbent insurer delivered an in-house risk engineering survey programme and refused to release the reports to the client.
3. The client's BI exposures were difficult to quantify and map (partly due to the outsourcing of data centres).

THE SOLUTION

We deployed the breadth of our Marsh Advisory capabilities, as required, to support the client with the aforementioned issues – namely, our: forensic accountants; business interruption experts; property risk engineers; cyber risk consultants; and actuaries.

We focused a property risk survey programme on the client's six most material locations, spread across the US, Asia and Europe – capitalising on our own global footprint by accessing local Marsh expertise.

Since the client had limited physical damage-related BI exposures, our BI experts and forensic accountants worked very closely with our cyber risk consultants; to account for the sizeable exposures emanating from a systems outage or loss of a third-party data centre.

Finally, our actuaries were able to draw on the findings of the work outlined above (i.e. assessment of most material PD/BI, NDBI and Cyber exposures) to build predictive models quantifying the client's potential loss volatility going forwards, including exposures to natural catastrophes. This culminated in an efficiency analysis to identify the optimal risk financing strategy for the client, focusing on the structure of their insurance programme.

THE RESULT

Most notably, we determined that:

The client's largest cyber exposure (based on likelihood and impact scoring) was a scenario where a disruption to a supplier's network impacted the client's services.

A 1 in 200 year non-damage business interruption event could cost the client in excess of USD 110m in lost revenue and last at least 135 days.

The client's existing IT disaster recovery was extremely mature and less than 3% of the client's revenue was not subject to formal disaster recovery.

The client's existing limit of liability for PD/BI was larger than required for the indemnity period, versus their PD/BI Estimated Maximum Loss. We recommended that they reduce this limit by 75%. We also recommended that the client amend the basis of their BI cover from Gross Earnings/Gross Profit to Gross Revenue.

The client's existing sub-limits of indemnity for PD/BI losses as a result of natural catastrophes would be sufficient versus modelled losses up to a 1 in 10,000 year return period.

The client's existing insurance programme reduced their Economic Cost of Risk (ECOR)* by almost USD 17m, versus without insurance.

*ECOR = Annual average retained losses + Insurance Premium (and taxes) + The implied cost of funding unexpected and/or uninsured losses with own capital.

Case Study 5 FINTECH

THE PROBLEM

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

THE SOLUTION

We reviewed the client's targeted data and interviewed key stakeholders to better understand their 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 their exposures to the large amounts of PII and PCI records they hold.

THE RESULT

Mapping out and articulating the insurability of each business impact in each loss scenario 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 their cyber risk profile, and make informed decisions.

Case Study 6 FINANCIAL MARKET INFRASTRUCTURE AND INFORMATION SERVICES PROVIDER

THE PROBLEM

Marsh engaged with a large international financial infrastructure and information services organisation to help lead their crisis management response to the Coronavirus outbreak. The organisation was seeking expertise to guide their response and additional team capacity to help coordinate their sites across the world.

THE SOLUTION

Marsh provided the following support:

- Leading the Crisis Management Team – facilitating crisis team meetings by providing direction, focusing on key risks, maintaining response structure and facilitating decision making using experience and expertise.
- Building and implementing response and recovery procedures – conducting scenario planning and preparing step-by-step procedures to respond to key scenarios.
- Monitoring continuity measures – managing information flows and reports from international Group sites to provide a clear view of the situation to leadership.
- Reporting to, and updating, the Board – preparing and delivering Board reports to obtain strategic direction for the response.
- Providing ad-hoc subject matter expert guidance – sharing lessons learned from previous live response experience and providing benchmarking insights and industry expertise as required.

THE RESULT

Marsh successfully kept the organisation ahead of the curve in their response – on average 10 days ahead of Government activity – which meant that the response was seamless and timely. Marsh continues to support the team by modelling their recovery and preparing robust recovery procedures for the most likely scenarios.

Technology Industry Practice

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 Technology 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.

For more information on Business Interruption and Resilience for Technology Companies, please contact your local representative.

BRAD SAUNDERS
Industry Risk Leader
Marsh Advisory
Marsh UK & Ireland
+44 (0) 20 7357 1423
bradley.saunders@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

This is a marketing communication.

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.

Statements concerning legal, tax or accounting matters should be understood to be general observations based solely on our experience as insurance brokers and risk consultants and should not be relied upon as legal, tax or accounting advice, which we are not authorised to provide.

Marsh Ltd is authorised and regulated by the Financial C onduct Authority for General Insurance Distribution and Credit Broking (Firm Reference No. 307511).

Copyright © 2020 All rights reserved. July 2020 53946598.