

# DATA BREACH: MITIGATE YOUR RISK

# RECENT EVENTS AND STATISTICS

- Recent BA attack by Magecart (Romanian/Lithuanian gang) – talk of multi-million £ fine.
  - Did they attack before (previous issue) and leave a back door to exploit later?
  - Also attacked Ticketmaster - RiskIQ.com – 11/9/18
- Dixons/Carphone Warehouse was biggest (known) breach in UK history
  - 5.9 million customer card details.
  - 1.2 million personal records.
  - £400k fine (saved from bigger GDPR fine by timing) - Source: BBC news 31/8/18
- 30% of UK companies have sacked employees for data-breach negligence.

## FACTS AND FIGURES – H1 2018

- H1 of 2018 saw a 133 percent increase in stolen, lost or compromised records over H1 2017.
- Social media incidents account for over 56 percent of records breached.
- 65 percent of data breach incidents involved identity theft.
- **Break Down of the 2018 Breach Level Index Stats:**
  - 18,525,816 records compromised every day.
  - 6,761,922,840 per annum.
  - 771,909 records compromised every hour.
  - 12,865 records compromised every minute.
  - 214 records compromised every second.

**Encryption was used in only 2.2% of cases!!**

# GDPR: THE INSURANCE POSITION

# GDPR AND ITS IMPACT ON INSURANCE POLICY WORDINGS

- Cover for breaches of data protection legislation is not a new concept.
- You may have cover for certain exposures under some of your existing insurance policies, e.g. public and products liability, employers liability, legal expenses, professional indemnity, and privacy liability.
- Speak to your broker for assistance in establishing your position.

# CYBER INSURANCE SUMMARY

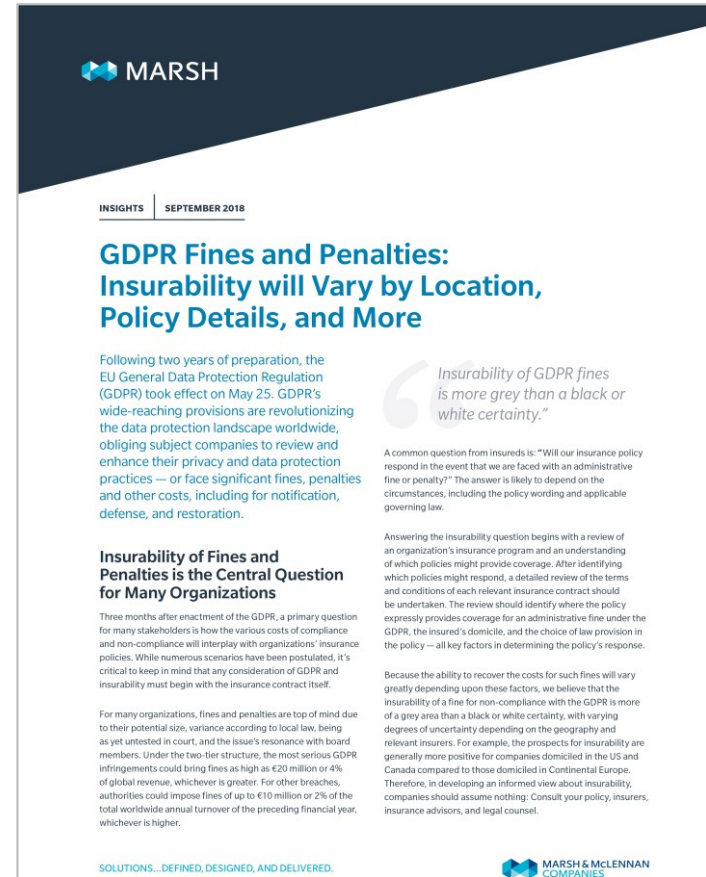
- Cover for your liability to third parties, defence costs, regulatory fines, in respect of:
  - A data breach
  - Breach of data protection legislation
  - Breach of confidentiality agreements
  - Network hijacking, including virus transmission
- Content injury cover in connection with your publishing and broadcasting activities, and your website content and functionality
- Cover for payment card industry (PCI) data security fines and assessments
- Cover for loss of income and increased costs of working resulting from network interruption caused by a security failure, system failure or operational error (including failure of your outsourced service providers)
- Cover for the costs of recovering, reconstruction, reloading or replacing digital assets which have been impaired due to a security failure, system failure or operational error (including failure of your outsourced service providers)
- Cover for the payment of cyber extortion losses and expenses
- Associated crisis response costs including IT forensic costs, legal expenses, notification expenses, customer call centre costs, identity theft remediation services and public relations costs

# GDPR: ARE FINES AND PENALTIES INSURABLE?

## Continental Europe and United Kingdom

*“The insurability of GDPR fines and penalties may not have uniform application in the EU. GDPR itself is silent on the issue. A key consideration is whether the relevant regulator has stipulated that its fine cannot be recovered from any third party. Within the UK, the Financial Conduct Authority has expressly prohibited the insurability of fines imposed by it on FCA regulated firms. To date, we do not know the position of the UK Information Commissioner’s Office on the recoverability of an administrative fine levied for non-compliance with the GDPR.”*

Decisions of insurability are likely to be clarified in the first instance as a matter of case law in each country.



**MARSH**

INSIGHTS | SEPTEMBER 2018

### GDPR Fines and Penalties: Insurability will Vary by Location, Policy Details, and More

Following two years of preparation, the EU General Data Protection Regulation (GDPR) took effect on May 25. GDPR's wide-reaching provisions are revolutionizing the data protection landscape worldwide, obliging subject companies to review and enhance their privacy and data protection practices — or face significant fines, penalties and other costs, including for notification, defense, and restoration.

**Insurability of Fines and Penalties is the Central Question for Many Organizations**

Three months after enactment of the GDPR, a primary question for many stakeholders is how the various costs of compliance and non-compliance will interplay with organizations' insurance policies. While numerous scenarios have been postulated, it's critical to keep in mind that any consideration of GDPR and insurability must begin with the insurance contract itself.

For many organizations, fines and penalties are top of mind due to their potential size, variance according to local law, being as yet untested in court, and the issue's resonance with board members. Under the two-tier structure, the most serious GDPR infringements could bring fines as high as €20 million or 4% of global revenue, whichever is greater. For other breaches, authorities could impose fines of up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

*Insurability of GDPR fines is more grey than a black or white certainty.*

A common question from insureds is: "Will our insurance policy respond in the event that we are faced with an administrative fine or penalty?" The answer is likely to depend on the circumstances, including the policy wording and applicable governing law.

Answering the insurability question begins with a review of an organization's insurance program and an understanding of which policies might provide coverage. After identifying which policies might respond, a detailed review of the terms and conditions of each relevant insurance contract should be undertaken. The review should identify where the policy expressly provides coverage for an administrative fine under the GDPR, the insured's domicile, and the choice of law provision in the policy — all key factors in determining the policy's response.

Because the ability to recover the costs for such fines will vary greatly depending upon these factors, we believe that the insurability of a fine for non-compliance with the GDPR is more of a grey area than a black or white certainty, with varying degrees of uncertainty depending on the geography and relevant insurers. For example, the prospects for insurability are generally more positive for companies domiciled in the US and Canada compared to those domiciled in Continental Europe. Therefore, in developing an informed view about insurability, companies should assume nothing: Consult your policy, insurers, insurance advisors, and legal counsel.

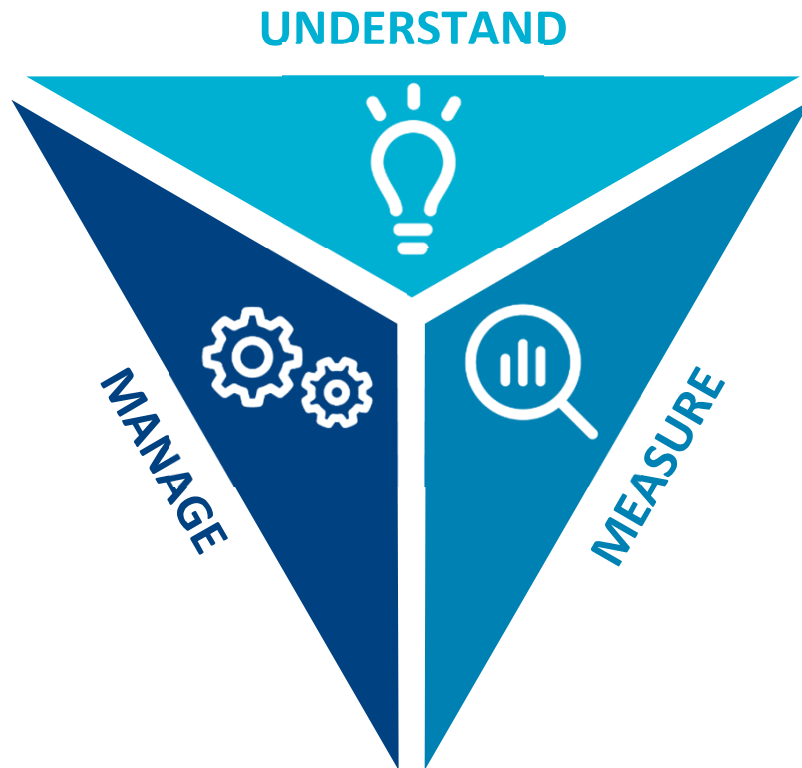
SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

**MARSH & MCGRAW HILL**  
COMPANIES

# RISK MANAGEMENT ACTIONS



# MARSH APPROACH TO CYBER RISK



## UNDERSTAND

Provide **CYBER CONTEXT** within a **BUSINESS PERSPECTIVE**



## MEASURE

Quantify the **FINANCIAL IMPACT** of cyber exposures



## MANAGE

Actionable steps to **SECURE, INSURE** and **RECOVER**

# RISK MANAGEMENT: SUGGESTED CHECKPOINTS

- Risk identification
- Crisis management
- IT disaster recovery
- Reputational risk
- Non-damage business interruption

# EXAMPLE OF INCIDENT AND RESPONSE

- On Monday March 18<sup>th</sup> March Norsk Hydro (one of the world's largest aluminium producers) was hit by a major ransomware attack.
- Resulted in production stoppages in Europe & USA
- Impact lasted until Wednesday afternoon (20<sup>th</sup> March)
- Eivind Kallevik (CFO) said that there was no fixed timeline for when all systems would be up and running
- Crucially, no ransom paid due to an effective system of back-ups
- The malware used was relatively new and difficult to detect (LockerGoga). As this is not self-propagating, which means someone uploaded and deployed the software across the network. This was a targeted attack
- Insurance was in place, back-ups were robust and the ITDR plan responded effectively.
- This is a good example of how disruption was minimised through effective planning

• Source: Wired.co.uk 21<sup>st</sup> March 2019

## PRESENTER CONTACT

Eric Alter

[eric.alter@marsh.com](mailto:eric.alter@marsh.com)

+44 (0) 7920 212079



This is a marketing communication.

Registered in England and Wales Number: 1507274, Registered Office: 1 Tower Place West, Tower Place, London EC3R 5BU

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

Copyright © 2019 Marsh Ltd All rights reserved.

This PowerPoint™ presentation is based on sources we believe reliable and should be understood to be general risk management and insurance information only.

The publication contains third party content and/or links to third party websites. Links to third party websites are provided as a convenience only. Marsh is not responsible or liable for any third party content or any third party website nor does it imply a recommendation or endorsement of such content, websites or services offered by third parties.



**Chartered**

