

# RISK FRONTIERS BRUSSELS

30 November 2017  
Brussels, Belgium.



Dear colleague,

We are delighted to invite you to Commercial Risk Europe's **RISK FRONTIERS - BRUSSELS 2017: CYBER RISK - RISING TO THE CHALLENGES** seminar on 30 November at the Thon Hotel Bristol Stephanie, Brussels.

This popular annual event, now in its sixth year, is organised in partnership with Belrim, the Belgian risk management association, and also supported by Narim, the Dutch risk management association, and European risk management federation Ferma. It will provide European risk managers with an in-depth guide to the complex and fast-changing area of cyber risk exposures and what the market is doing to help mitigate and risk transfer some of those exposures.

Leading European and international experts in this challenging and often confusing area will explain what the key risks are for risk managers and how they can be more effectively identified and measured. Experts will also explain how such risks need to be managed and, if possible, transferred or at least shared.

This one-day seminar has been designed in collaboration with Belrim and Ferma to ensure that risk manager delegates will benefit from an in-depth and interactive series of presentations, case studies and panel debates covering such key areas as:

- The current and future cyber risk landscape in which European large corporates operate
- Latest developments in the law and regulation in this rapidly evolving area
- Crisis response
- Internal and external threat - people, culture and awareness
- IT failure and business interruption
- Risk transfer & claims

The event is free to attend for all corporate risk and insurance managers.

We hope you can join us and we look forward to welcoming you on 30 November.

Kind regards

**Gaëtan Lefèvre**

*Vice President of Belrim, Ferma Board Member,  
Group Risk & Insurance Manager, CMI Group*

**Adrian Ladbury,**

*Editorial Director, Commercial Risk Europe*

**ATTENDANCE  
IS FREE FOR RISK  
MANAGERS  
£120 (ex VAT) for other  
delegates and £60  
for BELRIM/NARIM  
members**

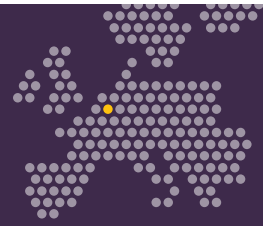
**REGISTER HERE:** <http://www.commercialriskonline.com/rfbrussels2017>

IN ASSOCIATION WITH

## RISK FRONTIERS BRUSSELS

## CYBER RISK – RISING TO THE CHALLENGE

30 November 2017



### 8.50 – 9.00 WELCOME ADDRESSES

#### PART I – THE RISK

### 9.00 – 9.15 FERMA ECIIA CYBER RISK GOVERNANCE REPORT

European risk experts have called for organisations to create dedicated internal cyber risk governance groups to address digital risks across the whole enterprise as the threats evolve – CRE Editor Adrian Ladbury asks the report author about the key findings.

### 9.15 – 9.45 THE RISK LANDSCAPE

Speaker from – **Aon Global Risk Consultants / Stroz Friedberg**

To set the scene, a leading cyber risk expert will explain the current and future cyber risk landscape in which companies will have to operate. Key questions to be tackled include:

- What are the main cyber threats faced by European companies today?
- How is this landscape changing and what is driving this evolution?
- What are the main exposures to companies and economies in this new landscape?
- What is the potential cost and how is this measured in financial terms?

### 9.45 – 10.15 THE TRUE COST OF CYBER – PRICING CYBER INSURANCE PRODUCTS BY HYBRID METHODOLOGY

Speaker – **Dr Madhu Acharyya**, Senior Lecturer in Risk and Finance, Glasgow Caledonian University

### 10.15 – 10.35 Q&A

### 10.35 – 11.00 COFFEE BREAK

#### PART II – THE EVOLVING EXPOSURES

### 11.00 – 11.45 CRISIS RESPONSE – SPEED IS ALL

Main Speakers – **Alex van den Doel & Bart Klijnsma**, Aon Holland

One very important question that risk managers and their management colleagues need to tackle when working out their cyber risk management system is: What to do when the crisis occurs to make sure the damage is limited and any insurance coverage in place actually responds as intended.

This session will address the key issues and questions facing risk managers including:

- Why is a rapid response to a cyber incident so important?
- How should you organise your response plan? How should it be triggered; how should it operate and who need to be the key players?
- What type of third party service providers will it prove useful to have lined up to help deal with an incident?
- What can expert service providers do to help protect and restore your company's reputation?

### 11.45 – 12.30 INTERNAL AND EXTERNAL THREAT – PEOPLE, CULTURE AND AWARENESS

Speaker – **Frank Vanhoonacker**, Underwriting Manager Professional Liability and Cyber, AIG

The Business Continuity Institute recently revealed that six in every 10 organisations view their employees as the biggest threat to successful GDPR adherence. A recent study by the German Federal Association for Information Technology, Telecommunications and New Media (Bitkom) also revealed that in many cases (around 52%), current or former staff members were responsible for cyber incidents.

One leading Lloyd's insurer (Beazley) recently revealed that unintended breaches caused by an employee or third-party vendors actually are almost as much of a problem as external hacker-style attacks.

This risk needs to be better appreciated and managed whether it comes maliciously or accidentally. This session will explore how this can be achieved and discuss key questions such as:

- What monitoring tools are available to help manage this risk?
- How can greater employee awareness help companies to be better prepared?
- How should businesses create a cyber security culture that spreads throughout the business and what role does the risk manager have to play in this?
- What insurance can be bought to cover such third-party risks and how can contracts be constructed to ensure a fair apportionment of the liability?

**REGISTER HERE:** <http://www.commercialriskonline.com/rfbrussels2017>

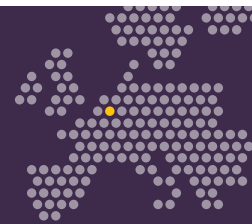
#### SPONSORS



## RISK FRONTIERS BRUSSELS

## CYBER RISK – RISING TO THE CHALLENGE

30 November 2017



### 12.30 – 2.00 LUNCH

#### PART III – RISK IDENTIFICATION AND MANAGEMENT

##### 2.00 – 2.40 RISK IDENTIFICATION AND MAPPING

Accepting that the company faces an unacceptable level of uncertainty about its cyber exposure is a first step. The next, and most important, step is properly identifying and mapping the risk so that mitigation and potentially transfer measures can then be taken. This session will address:

- Who should be involved in the risk identification and mapping process?
- Does it make sense to use a third party to help in this process?
- How can desktop studies, workshops and dialogue across the businesses be used to assess more complex risks?
- How should IT security and data processes, business continuity plans and breach response procedures be analysed in a structured way?
- How can you use risk mapping of your data and IT risks to help work out which risks can be avoided, accepted, controlled or transferred?

##### 2.40 – 3.20 RISK MITIGATION

Speaker – **Kyle Bryant**, *Regional Cyber Risk Manager, Europe, Chubb*

Once the modelling and mapping has been completed businesses and their risk managers need to implement effective risk mitigation measures to actually control the risk as much as possible and prevent it manifesting and leading to an incident and loss.

- What form of user education and awareness training is needed?
- How can you most effectively adopt monitoring policies and procedures for all networks and systems?
- What incident management procedures, including response and disaster recovery, are needed?
- What kind of network security policies and procedures are best used?
- How should you implement an effective governance structure that maintains board engagement and delivers appropriate information security policies?

##### 3.20 – 3.50 COFFEE BREAK

#### PART IV – CYBER RISK TRANSFER & CLAIMS

##### 3.50 – 4.30 RISK TRANSFER

Speakers & panellists:

**Raf Duyver**, *Cyber Risk Expert Advisor, Aon Belgium*

**Katty Debremaeker**, *Financial Lines Major Loss Claims Adjuster, Europe, AIG*

The insurance market is banking on cyber risk insurance to bolster its growth potential in this long, soft market in which profitable growth is hard to find. But this is a risky business as the risk itself evolves rapidly and everyone involved faces a sharp learning curve.

A panel of leading insurers, brokers and reinsurers will tackle the following questions:

- Is cyber risk really insurable?
- How should insurers help risk managers manage cyber risk?
- Is there adequate primary capacity currently in Belgium, Europe and worldwide and is this fairly priced?
- What impact will the GDPR have upon the cyber insurance market and the ability of the market to properly assess and price this risk?
- Should governments create cyber pools as with terror and natural catastrophe to help foster the growth of a more vibrant cyber insurance market, particularly given the rise of state-backed cyber attacks?

##### 4.30 – 5.15 BUSINESS RECOVERY AFTER A CYBER INCIDENT

As a young and fast developing market, the cyber insurance offer remains largely untested. Those risk managers that have bought policies to date cannot be certain that they will react as intended. This session will explore and debate how to best help risk managers prepare for the inevitable day when the policy needs to be called upon:

- What are the main potential pitfalls that could lead to coverage dispute within the cyber risk area?
- How could and should risk managers work effectively together, supported by brokers and claims experts, to ensure that policies react as intended during policy negotiation?
- If coverage disputes do arise over cyber incidents how can they be most effectively resolved?

##### 5.15 – 5.20 CLOSING REMARKS

##### 5.20 – 6.30 DRINKS

**REGISTER HERE:** <http://www.commercialriskonline.com/rfbrussels2017>

#### SPONSORS

