Risk, Resilience
and Reputation

# Focus on Funds | Risk, Resilience and Reputation

## Don’t be the weakest link | Managing data and cyber risk

**9 June 2022**

| Chris Luck
| Emma Burnett
| Tom de Cordier
| Lee Gluyas
| Amit Tyagi

# Presenting today

## Moderators

**Chris Luck**
Partner | CMS UK
Funds
T +44 20 7524 6294
E christopher.luck@cms-cmno.com

**Emma Burnett**
Partner | CMS UK
Data Protection
T +44 20 7367 3565
E emma.burnett@cms-cmno.com

## Speakers

**Tom de Cordier**
Partner | CMS Belgium
Technology, Media & Communications
T +32 2 743 69 13
E tom.decordier@cms-db.com

**Amit Tyagi**
Partner | CMS UK
Insurance
T +44 20 7367 3578
E amit.tyagi@cms-cmno.com

**Lee Gluyas**
Partner | CMS UK
Dispute Resolution
T +44 20 7524 6283
E lee.gluyas@cms-cmno.com

# A few real-life examples. This could happen to you too…

Your data get exfiltrated & **cryptolocked** with request to pay ransom in virtual currency

**APT**: State-sponsored hack (originating from rogue state) + exfiltration of intellectual property

Hack into mailbox of senior management

**Purchase price for recent acquisition** was wired into fraudulent bank account

Hack into mailbox of senior management

**strategic information** about confidential **M&A transaction** potentially exposed

Threat by **disgruntled temporary worker** whose contract got not prolonged

IT-consultant published scripts on **Github** (public directory) containing **security credentials** which have been used by a Chinese IP address to intrude into your IT environment

# Tips & tricks based on our real-life experience

**Call** your insurer's or your broker's **hotline** asap (even if unclear whether incident is covered by policy)

Be mindful of **confidentiality**: only disclose the incident to those that have a strict need to know

Consider **legal privilege**: when involving external forensic experts you may want to contract them through CMS (external counsel) to vest legal privilege in the findings of the experts

**Hackers may listen in:**
use Signal, Threema or Whatsapp for fast and confidential communication between all the various stakeholders (internal IT; internal CISO; external forensics; external counsel; other stakeholders)

Make sure you have internal & external **communications ready** in case you need to communicate (pro-actively or re-actively) about the incident + make sure that your lawyers have approved the comms before they go out

In ransomware attacks: check for **IP address(es)** of **staging server(s)**. Hosting provider may be willing to take exfiltrated data off-line

# Tips & tricks based on our real-life experience

Set up **daily status update calls** with all involved stakeholders (internal IT/CISO; external forensics; in-house & external counsel; insurance broker; etc.)

**Fix** the common **weak spots**:

- Many cyberattacks could be avoided if multifactor-authentication was on
- Do not postpone patching of known vulnerabilities
- Your BoD and chairman may be using email clients that are not sufficiently secured
- Make sure sufficient logs are available

**Document** the incident
+ actions undertaken to remediate and improve

**Post-mortem follow-up**:
Never waste a good crisis. Use incident to define and implement improvements to your systems/processes

# Reporting obligations

You may have to **notify** the incident to:

The **Data Protection Authority** if personal data (e.g. of your workers) have been exposed.

- Two-step notifications in case the findings of the investigation are still unclear, but potentially causing serious risks to personal data
- Be mindful of international dimension: GDPR's 1-stop-shop may allow you to notify only one DPA (lead DPA)

**Financial markets supervisory authorities**

Affected data subjects

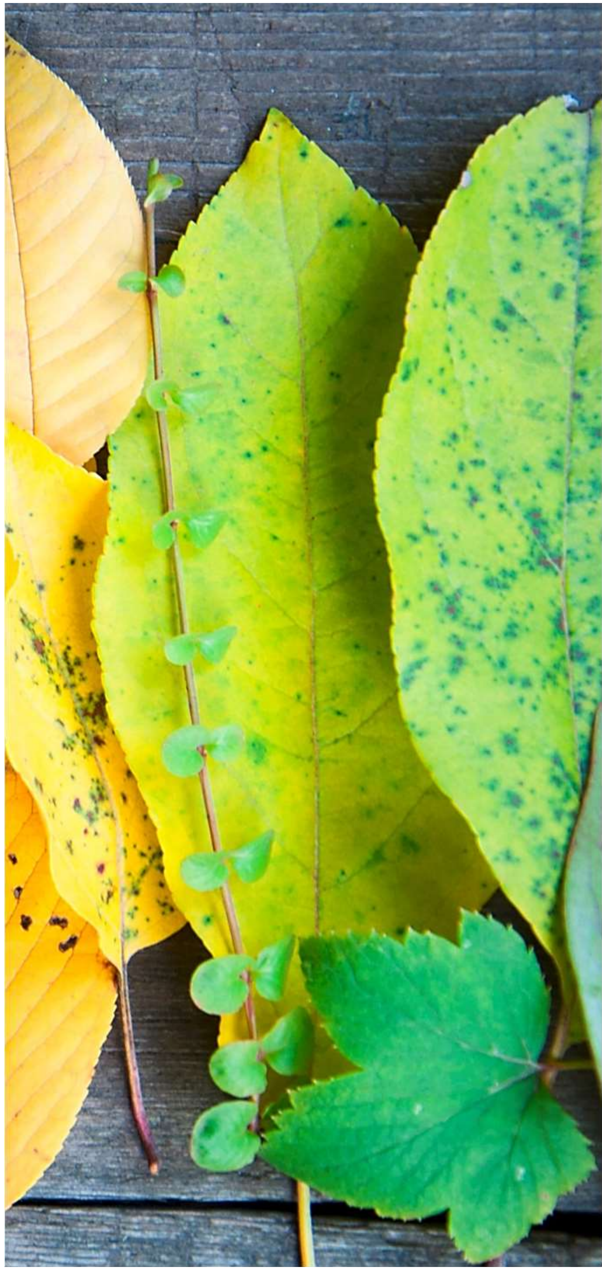
**Your customers:**
check your contracts to see whether they require you to disclose security incidents

Is it worthwhile notifying the **police**?

**Other governmental authorities**
(e.g. if you (or your customers) are active in regulated industries (e.g. financial services industry; defence industry; telecommunications; critical infrastructure; etc.))

# The cyber insurance market

- Growth of cyber insurance take up 20 – 25% per annum
- Still significant “under insurance” worldwide and in the UK
- Cost of cyber insurance rising and market hardening
- Ransomware driving rate increases and market changing to respond
- Insurance part of your holistic risk management programme



# Cyber policy: First party coverage | areas typically covered

Damage caused to the Insured

## Event Management

Legal & IT breach response services, Data restoration costs, restoration of computer systems (software and hardware); PR services; notification costs; credit/ID monitoring offered to data subjects

## Business Interruption

- Reduction in operating profit caused by cyber incident, costs incurred in mitigation of loss
- Set timeframe (e.g. 3 months)
- Consider untargeted v targeted attacks
- Consider supply chain issues

## Cyber Extortion

- Costs of ransom negotiator
- Payment of ransom
- Sanctions concerns
- War and terrorism exclusion

## Fines and penalties

- PCI Fines
- Cover unless uninsurable at law
- FCA fines = uninsurable
- DPA fines?

# Third Party Losses

## Damage caused to the Insured’s clients and others

### Defence costs

- Third party claims or regulatory investigations for claims arising out of data breach of security failure
- Typically require Insurers’ prior agreement
- Reimbursement of “reasonable and necessary” costs

### Damages

- Damages
- Claimants costs
- Settlements reached with third parties (with Insurers’ consent)

# Common exclusions

## 01 Uninsurable loss

e.g. FCA fines

## 02 Conduct

Reckless or negligent acts by a director/senior management

## 03 Betterment

Upgrades to Insured’s systems to improve IT infrastructure rather than response to ongoing incident

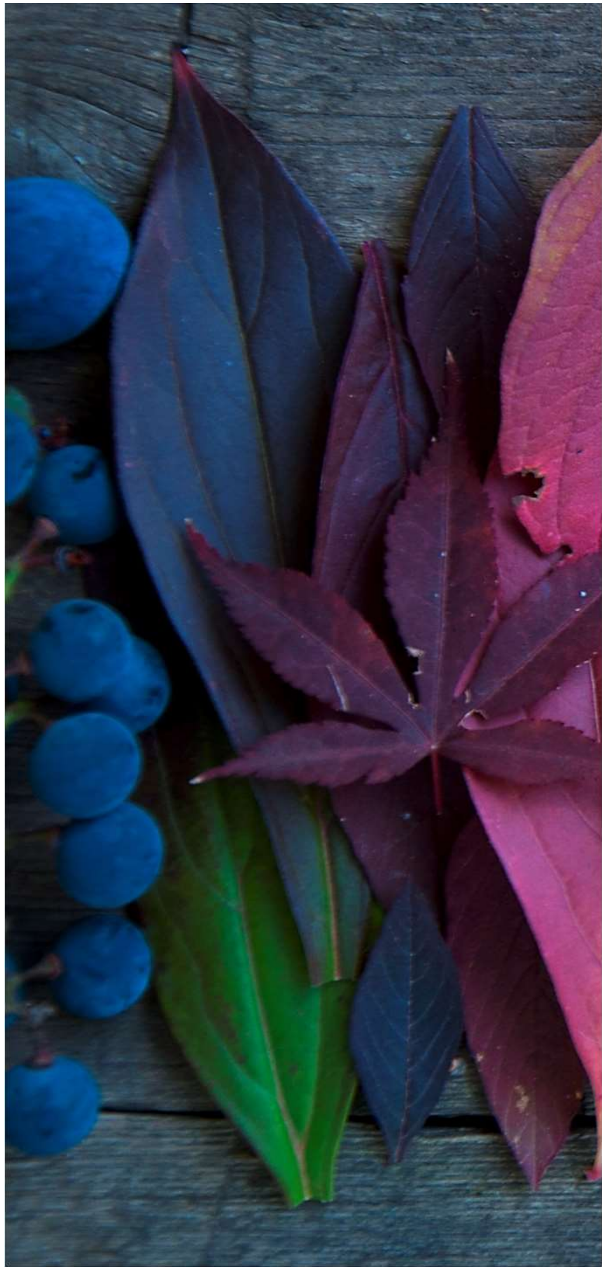
## 04 Property damage/ Infrastructure

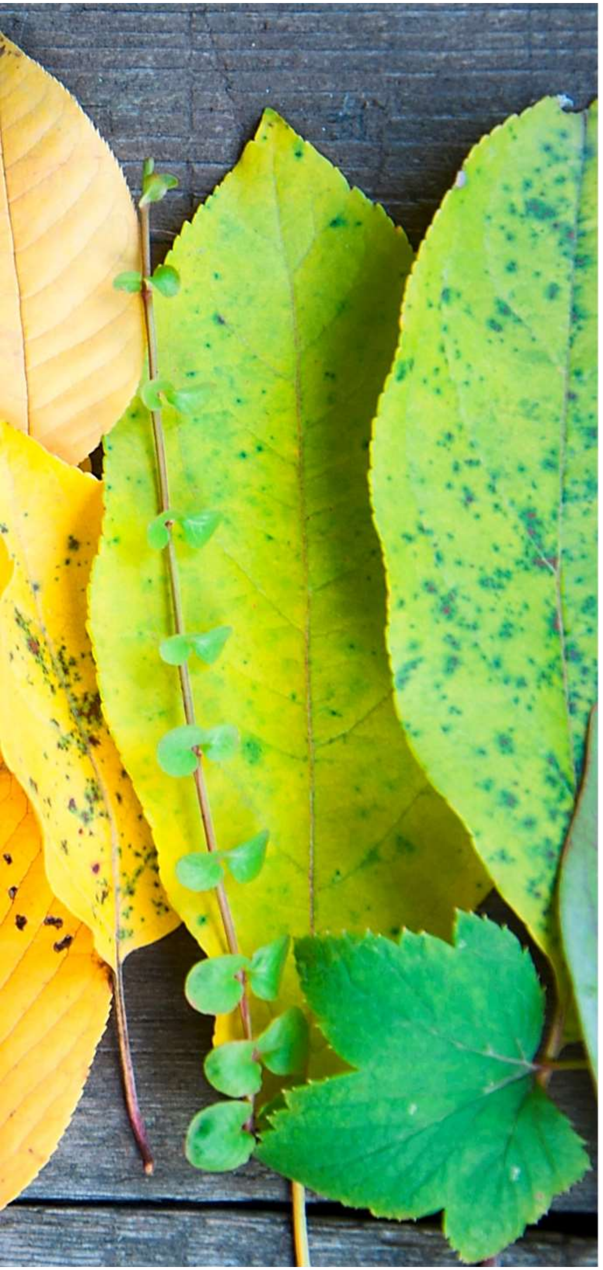
## 05 War & terrorism

- 4 LMA model wordings (November 2021)
- Burden on Insurer to prove it applies
- War does not have to be declared
- Attribution to a state

# Commercial claims which you may face following a cyber attack

- Compensation for direct financial losses suffered by clients or customers
- Damages for breach of contract; failure to provide services
- Claims by data subjects whose personal data is compromised by the cyber attack
- Class actions/group litigation

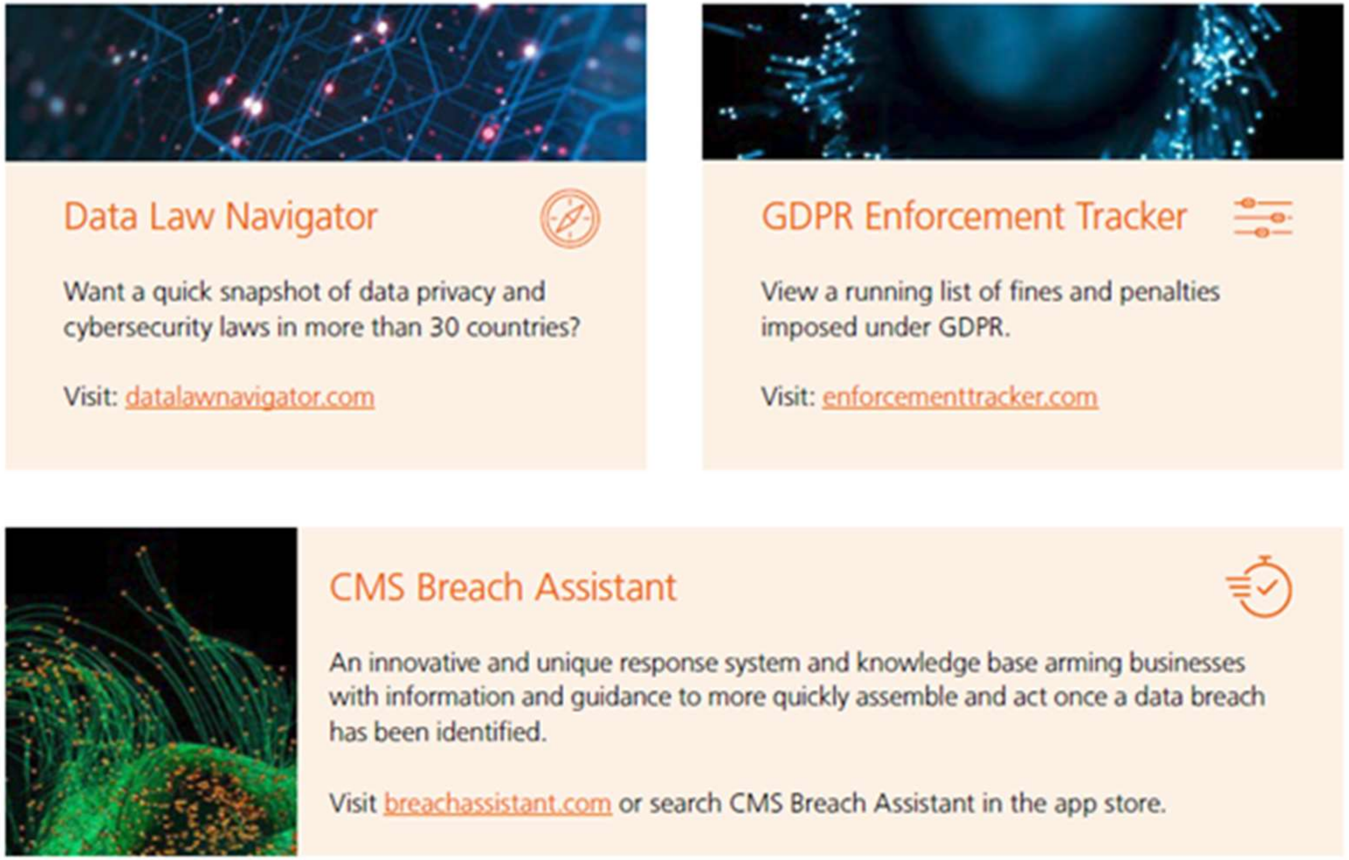




# Claims against suppliers

- IT consultants/MSPs; admin services; banking services
- Contractual claims - security levels/updating/testing
- Reasonable care and skill – good industry practice
- What can be recovered – foreseeability and causation
- Limitations and exclusions of liability
- Minimising risk – procurement; testing; limitations; insurance

# Helpful resources



## Data Law Navigator

Want a quick snapshot of data privacy and cybersecurity laws in more than 30 countries?

Visit: datalawnavigator.com

## GDPR Enforcement Tracker

View a running list of fines and penalties imposed under GDPR.

Visit: enforcementtracker.com

## CMS Breach Assistant

An innovative and unique response system and knowledge base arming businesses with information and guidance to more quickly assemble and act once a data breach has been identified.

Visit breachassistant.com or search CMS Breach Assistant in the app store.

CMS Law-Now™

**Your free online legal information service.**

A subscription service for legal articles on a variety of topics delivered by email.

**cms-lawnow.com**

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice. It was prepared in co-operation with local attorneys.

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG’s member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name “CMS” and the term “firm” are used to refer to some or all of the member firms or their offices; details can be found under “legal information” in the footer of cms.law.

**CMS locations:**
Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Beirut, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Strasbourg, Stuttgart, Tel Aviv, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

**cms.law**

# Thank you for joining us