Risk-Transfer considerations & Insurance Landscape

September 2020

Empower Results®

What is going on in the Cyber Insurance World

Why is the uptake in cyber insurance so low when the risk is so clear?

- 400% increase in maritime cyber incidents
- Ransomware is increasing in frequency and size:
  - Average ransom in Q4 2019 was close to $100,000 with some in the millions
  - One client suffered an extortion attack which created a $100M loss
- Average downtime after a breach varies between six days to well over two weeks
- Still a low uptake in the maritime sector

AON
Empower Results®

Resilience through insurance

"The ability to prepare & plan for, absorb, recover from & more successfully adapt to adverse events"

Financial resilience (post event) consists of two dimensions

- The amount of damage sustained
- The speed of recovery

Why do we buy insurance?

- Because we have to – Legislation, Financial etc.
- Because it is part of a risk management philosophy
- Increasingly, cyber insurance is being required by contract and is demonstrative to clients and vendors that a company has contemplated multiple aspects of cyber risk across the enterprise and has invested in balance sheet protection.

AON
Empower Results®

Cyber risk, change is optional

- If we accept that digitalisation is advancing at a rapid pace then we must also accept that we are more at risk from cyber breaches than ever before

- Old process is being replaced by new technology
  - New IMO regulations (IMO 2021) may change the concept of “Seaworthiness” for a vessel

- Everything becoming connected with enormous advantages but significant risk

- Dependence on data changes the risk profile and is one of the fastest growing areas of concern in the Marine industry

- No simple fix. No single solution

- However, Insurance is not the (only) answer

AON
Empower Results®

Cyber Insurance

- As Chronis discussed, once you are engaged in the process of cyber resilience preparation - and quantification - companies will find more than one way to transfer and manage this quantified cyber risk.

- Perhaps it does make sense to transfer a portion to the cyber insurance market, but maybe an alternative risk retention, or self-insurance financing strategy, is warranted.

Cyber is an ever-changing landscape and the coronavirus pandemic has highlighted the capacity of a non-cyber event to impact cyber security.

AON
Empower Results®

Cyber Insurance

- Cyber insurance will cover;
  - financial losses due to data breaches and other cyber events, such as loss or damage to electronic data,
  - loss of income
  - recovery costs
  - and notification costs (voluntary or as required by law) of parties affected by a data breach.
  - Cyber insurance can also provide liability coverage for claims against your firm by anyone injured as a result of the breach

- Cyber insurance **will not** instantly solve all of your cyber security issues, and it will not prevent a cyber breach/attack. Just as homeowners with household insurance are expected to have adequate security measures in place, organisations must continue to put measures in place to protect what they care about

Empower Results®

Cyber Insurance

- We all need to be clear that cyber insurance does not equal cybersecurity. They are two different things
- Cyber insurance does not make your company or its data more secure and having cyber insurance should not help you sleep better at night.
- In fact, I would argue that having cyber insurance could provide a false sense of security, leading to lax controls and taking some of the pressure off the constant vigilance needed to protect your systems – we have seen many marketing examples of cyber insurance purporting to “solve” the cyber security issue……..
- While cyber insurance will pay for remediation and recovery, that's all it pays for.
- It doesn't address damage to your brand, loss of trust, client churn, lost contracts… In short, it can't protect you against many of the consequences that will impact your business

AON
Empower Results®

Should I purchase Cyber Insurance?

IMO Resolution MSC.428(98) - IMO member states are encouraged to ensure that cyber risks are addressed in Safety Management Systems no later than the first annual verification after 1st January 2021 of a company's Document of Compliance which will then have to include a chapter on cyber security.

- Common objections to purchasing cyber insurance:
  - I'm already covered through other insurances (Crime, Property).....maybe…….maybe not !
  - "New insurance" so getting budget internally can be difficult
  - It won't happen to me!
  - No mandatory aspect to the cover……yet! IMO 2021 seems to be generating interest
  - Confusion amongst buyers between buy back or stand alone cover
    - Most breaches seem to give rise to non-damage B/I claims……perhaps more communication is needed…..
  - Whereas traditional property, business interruption or fire or flood policies have established market language and wordings, cyber policies are still very new, and every policy is different

AON
Empower Results®

Cyber Risk Matrix

POLICY / SCENARIO	PD/BI	LIABILITY	CRIME	CYBER
Data / Information Disclosure: Intentional disclosure of customer, employee or other third party PII by a disgruntled employee.		Policy may respond to disclosure of confidential third party data.		Specifically for fines & penalties following GDPR investigation – where fines are legally allowable it is unlikely that the policy would respond.
Failure of Network Security: Liability for economic harm suffered by others from a failure of your computer or network security (including written policies & procedures designed to prevent such occurrences).				
Denial of Access: Accidental denial of access (failed maintenance attempt) to key management system for e.g. 48 hours.				
Denial of Access: Deliberate denial of access to master database via global malware incident (e.g. Wannacry / NotPetya). A 72-hour downtime results.	Policy may respond to applicable data restoration costs following a malware attack			
Data Modification: Intentional modification of bank account details within a client's billing system to re-route payment funds.			Loss / theft of funds is covered by the Crime policy – Forensic investigation and data restoration costs are not	
System/Physical Destruction: Intentional hacking of key datacentre causing destruction to data and physical property.	Physical damage following a cyber loss may be covered - wording dependent			Cyber policy would not respond to certain losses (e.g. physical damage to property/equipment), the PDBI policy may provide coverage.
Data / Information Disclosure: Accidental disclosure of client's intellectual property – e.g. patents.				Generally, IP related losses not be covered -Forensic investigations and legal expenses may be covered in some instances.

AON
Empower Results®

Marine Exclusions (Typical)

Marine Hull

- Typically had cyber exclusions (clause CL380) now LMA 5403 that eliminates or limits coverage for losses arising from computer software, operating systems, program or data
  - CL 380 First written in 2003 – before iPhone, WiFi
  - However, it fails to address non malicious risks
- Many existing hull insurance policies will not cover the risk of a navigation system being jammed or the physical damage to a ship caused by a breach

LMA 5403

- The new clauses published by the LMA comprise a cyber endorsement and exclusion clause
- All clauses explicitly supersede or replace conflicting policy wording related to cyber loss and data
- The marine clauses rule out coverage for any loss or expense related to the “failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system.”
- They similarly exclude coverage for “the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or anv other electronic system.”

AON
Empower Results®

Marine Exclusions (Continued)

Protection & Indemnity

- No specific exclusion……. And no specific inclusion !
- Excludes cyber as a result of War or Terrorism
- Current thinking suggests clubs would cover up to club retention limits and perhaps one cat event (over $100M) may be covered before reinsurers say no

D&O

- Most D&O policies are broadly constructed and will provide cover for cyber matters but only for individual Directors & Officers, not the insured company

AON
Empower Results®

Marine Exclusions (Continued)

Commercial Crime Insurance

- Won't cover data breaches and business interruption, but address direct financial losses related to social engineering and funds transfer fraud.
- Electronic data exclusion

Silent Cyber

- Lloyd's mandated that with effect from 1 Jan 2020, all policies clearly state whether they will provide affirmative coverage for cyber risks
  - Liability and reinsurance phased during 2020-21
- Three phase process
  - Phase 1 of the initiative, effective January 1st, 2020, required underwriters in the marketplace to clarify whether first-party property damage policies affirm or exclude cyber cover.
  - Phases 2-4 are for specific classes
- No exclusion/no clear cover policies will be deemed as non affirmative
- Will affect Cargo, War and Hull insurances

This rapidly changing and still misunderstood landscape creates coverage uncertainty.

AON
Empower Results®

I will take the risk

- Initial breach Thursday morning (Ransomware)
- By Friday morning systems are disabled, Company is unable to trade
- Engage with Remediation firm – initial terms of agreement signed on Friday 12pm
- Remediation firm repair breach over the weekend
- Ongoing repair and testing post breach

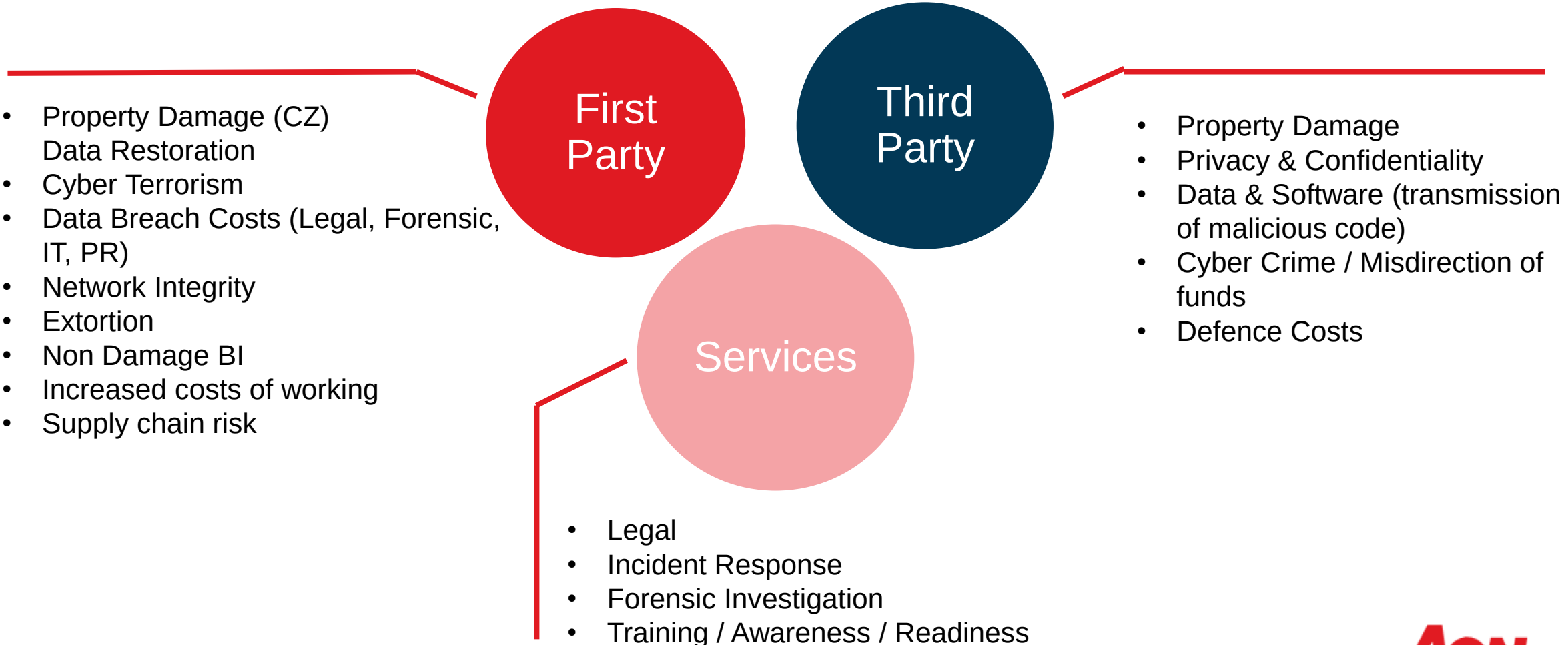
Costs of the data breach

System remediation (more than)	$200,000
Estimated cost to firm in lost trade and systems	$450,000.

AON
Empower Results®

Example Cyber policy: Chaucer

CHAUCER CYBER



- Property Damage (CZ) Data Restoration
- Cyber Terrorism
- Data Breach Costs (Legal, Forensic, IT, PR)
- Network Integrity
- Extortion
- Non Damage BI
- Increased costs of working
- Supply chain risk

- Property Damage
- Privacy & Confidentiality
- Data & Software (transmission of malicious code)
- Cyber Crime / Misdirection of funds
- Defence Costs

- Legal
- Incident Response
- Forensic Investigation
- Training / Awareness / Readiness

AON Empower Results®

Available coverage

- As coverage continues to evolve, it is becoming more valuable for companies.
- According to Aon data, over 75 insurers now provide over $1B in cyber insurance capacity across North America, London, Europe, Bermuda and Asia. This growing number of insurers has helped develop appetites for large, complex risks.
- Global markets
  - Specialist marine providers: SigCo, Shoreline, Aspen, Brit
  - Most larger insurers: AIG, NHC, Zurich, AXA XL, Chubb, Chaucer, Liberty
  - DNK cover for shipowners
- Some cover aggregated across a portfolio
  - So others can exhaust the capacity before you do
- Some Property insurers trying to adapt their policies/wording to fit marine risks
- Risk assessment is key
  - Our strong view is that firms need to identify their exposure before looking at risk transfer

Empower Results®

When the ship has sailed…
How to navigate a breach

September 2020

Empower Results®

A cyber incident: it’s not a matter of “if” but “when”

- Cytelligence reports +250 breaches on a monthly basis
- Ransomware is the root cause in about 50% of cases
- COVID has also impacted the landscape

Empower Results®

That is it: we have a (significant) breach

- Do not immediately erase the malware – isolate or quarantine the infected machine
- Do not engage with the cyber criminals or pay the ransom right away
- Do not improvise! Mobilise the team to launch the next phases of the IR plan

AON
Empower Results®

Now what?

1 **Do you have cyber insurance?**

Yes: Immediately call the contact number.

No: move to #2

2 **Do you have vendors retained?**

Yes: Immediately contact them to scope the event.

No: move to #3

3 **What is the best way to proceed?**

Contact an IT forensics firm and outside council to investigate, and follow the plan.

Empower Results®

The importance of a cyber incident response plan

Empower Results®

Summary

- Cyber risk landscape continues to evolve
- The maritime industry is as attractive as any other for a motivated bad actor
- Security and insurance are pieces of the puzzle – RESILIENCE is the goal
- Return-to-work post Covid will require a new set of polices
- Resurgence of attacks are foreseeable when the economy bounces back

We can guide your efforts towards cyber resilience.

AON
Empower Results®

Risk-Transfer considerations & Insurance Landscape

September 2020

Empower Results®