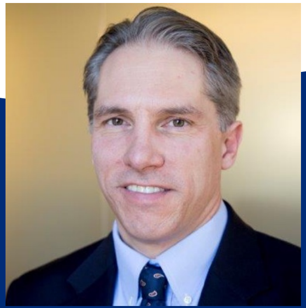
Mind the Gap: Best Practices in 1st Party Cyber Coverage for Energy, Power, and Renewables

November 4, 2020

Panelist Introductions



Michael Gaudet
FINPRO Energy & Power Industry Leader
Moderator

Monica Tigleanu
London Cyber Practice
Panelist

Kaitlin Upchurch
South Central Zone Cyber Leader
Panelist

Elisabeth Case
Client Engagement Leader
US Cyber Practice

Panelist

Robert Albino
Energy & Power East Zone Leader
Panelist

Sarah Baldys
FINPRO Energy & Power Advisor
Panelist

Toby Hudson
Cyber Consulting Practice
Panelist

Agenda

- Historical Background of Lloyds Mandate
- Property Insurance Placement Strategy
- Cyber Insurance Placement Strategy
- Power of Analytics
- Best Practices Recap

A Difficult Problem: Silent Cyber

“We cannot solve our problems with the same level of thinking that created them”

Albert Einstein

Historical Background of Lloyd's Mandate

Insurer & Regulator Actions to Address Silent Cyber Risk

- Risk concern over silent cyber exposure moved **UK regulators** to take steps to remove the "silence."
- **January 2019:** **Prudential Regulatory Authority (PRA)** instructed insurers to "have action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover."
- **July 2019:** **Lloyd's** Market Bulletin Y5258 required all policies be **clear** on coverage for **losses caused by a cyber event** – either **providing affirmative coverage** or **excluding coverage**.
  - Lloyd's **problematic definition of cyber risk** makes an arbitrary distinction between acts of misfeasance and malfeasance.
- **EIOPA** (European Insurance and Occupational Pensions Authority) likely to issue **similar directive**.
- **January 2020**: Lloyd's Market Bulletin Y5277 confirmed **phased implementation** across all classes. (*see next page*)
- Rating agencies such as **Fitch** have cited failure to manage non-affirmative cyber risks & exposures as **ratings criteria**.

LLOYD'S DEFINITIONS

- ***Cyber Risk:*** *any risk where the losses are cyber-related, arising from either* ***malicious acts*** *(e.g. cyber-attack, infection of an IT system with malicious code) or non-malicious acts (e.g. loss of data, accidental acts or omissions) involving either tangible or intangible assets.**
- ***Non-Affirmative Cyber:*** *policies where no exclusion exists and no express grant of coverage.*

**Defined by UK Prudential Regulation Authority*

Problematic Initial Response by Insurers

- Confusion and haste as insurers rush to comply.
  - Lack of consistency across markets / lines regarding affirming / excluding / sub-limiting cover.
- Flawed definition of cyber risk by PRA & Lloyd's.
  - Focuses on type of event (malicious vs. non-malicious; tangible vs. intangible), rather than resulting loss.
- Overreaching exclusion of previously covered physical perils where technology is a cause.
  - Endorsements are inconsistent and overreach in excluding loss from previously covered physical perils simply because technology was in chain of causation.
- Markets tending toward overly broad exclusions vs. affirming cover.

BEWARE:

- Absolute cyber exclusions. No coverage for **any loss** if connected to a **cyber event**. (ex: CL380, LMA 5401, LMA5402, IUA -01-081, IUA -09-082)
- Exclusions that differentiate cover based on the type of **event** (malicious versus non-malicious), rather than the **resulting loss.** (non-physical or physical). (ex: LMA5400, LMA5403, AIMU2015)
- Exclusions that provide a carve back for only limited named perils such as fire or explosion, or that seek to impose a sublimit on cyber risk. (ex: NMA2914, LMA5400, CL437)
- Wordings that take away otherwise covered **ensuing loss** if **technology** or **data** is **implicated in** the chain of **causation**. (ex: LMA5400)

Property Insurance Placement Strategy

Property Placement Strategies
Maximize Coverage, Resolve Gaps/Overlaps

Traditional Policies

- Should cover resultant physical damage regardless of technology involvement
- Should cover malicious & non-malicious acts
- Should delineate between physical and nonphysical impacts
- For cyber events involving IT/OT/Comms:
  - Loss should be affirmed for ensuing physical damage
  - Replacement or loss of computers due to non-physical cyber can be excluded if covered by cyber policy (bricking)
  - Exclude non-physical loss is it is covered under a cyber policy

Cyber Exclusions

- Should not overreach to restrict or remove core policy cover simply because technology or data was impacted or implicated in the chain of causation
- Should not conflate underlying intent of the bad actor with impact to the insured
- Should be clear when delineating between physical and non-physical impact

Stand-Alone Cyber Insurance

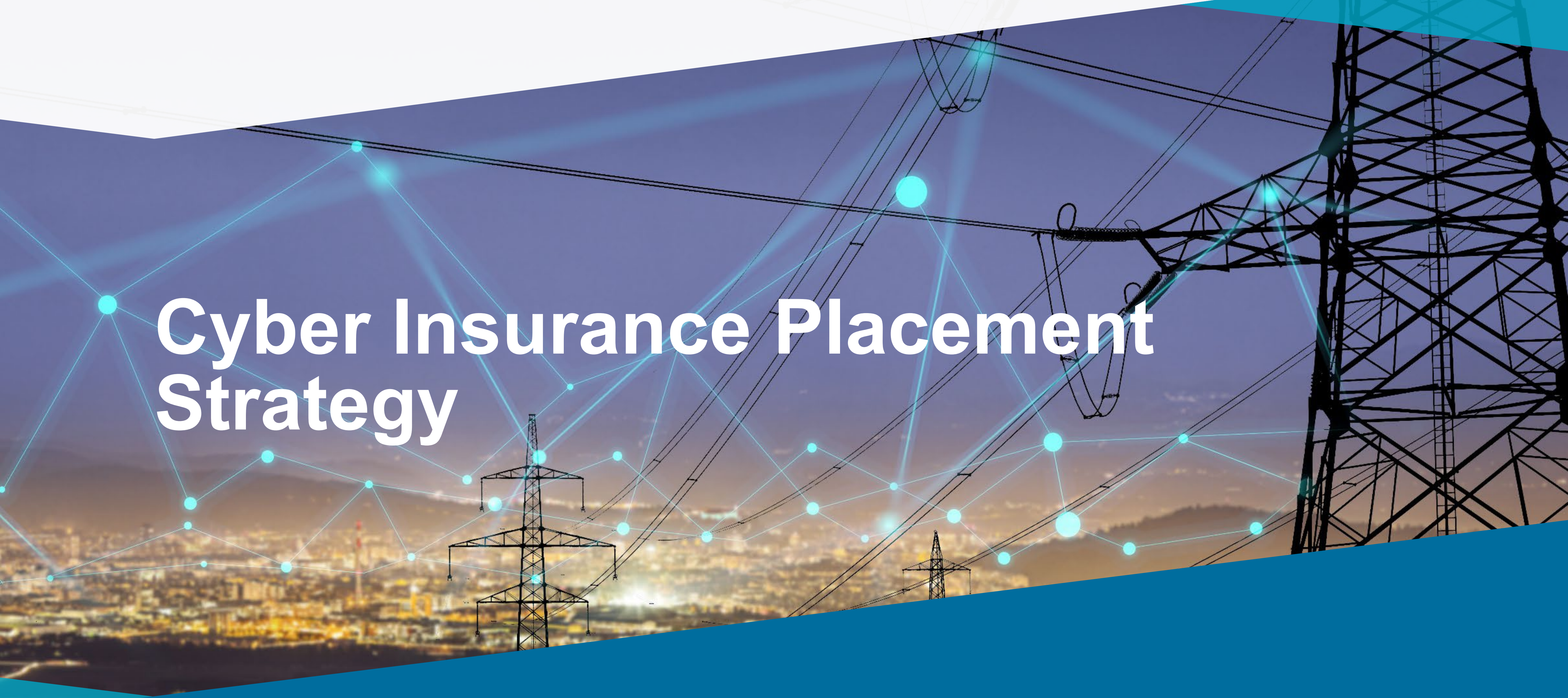
- Superior (limits and breadth) to adding affirmative cyber sub-limits to non-cyber policies
- Cover losses arising from the confidentiality, integrity, or availability of data or technology
- $500M - $750M limit capacity
- Broad coverage for 1st and 3rd party risks:
  - Incident response
  - Business interruption (non physical)
  - Data breach
  - Data restoration, hardware replacement
  - Cyber extortion / ransomware

Property Placement Strategies
When Traditional Lines Insurers Attach "Silent Cyber" Exclusions

Option	Advantages	Disadvantages
Reject the exclusion	• Not paying for "phantom" residual loss cover. • Retain coverage for resultant physical cyber losses.	• Lloyd's of London insurers will not offer capacity without silent cyber wordings as that puts them out of compliance. • Likely to reduce the overall capacity available to you for risk transfer.
Request a less restrictive version	• Better coverage certainty. • Retain coverage for some resultant physical perils, typically fire and explosion.	• Some resultant physical perils will still not be covered. • May not include coverage for malicious cyber events.
Accept the exclusion as offered	• Easiest path to retention of overall coverage capacity.	• Likely to exclude more resultant physical loss than expected. • May need to sue insurer for coverage following a carrier declination.
Accept the exclusion and purchase a "gap filler" policy	• May provide greatest overall coverage.	• Gap filler policies tend to be expensive. • Coverage offered may not fully replace coverage taken away by the cyber exclusion.

NOTE:
None of these options alleviate the need to purchase a standalone cyber policy for full scope of cyber coverage. A combination of options may be best for resultant physical loss or damage cyber cover – for example requesting a less restrictive exclusion and purchasing a "gap filler" policy.

Cyber Insurance Placement Strategy



Understand the Impact and Consequence of a Cyber Event

Cyber Event

Malicious attacks or accidental events to your digital system (incl. IT & OT), data (in house or outsourced), or technology

Resulting in:

Impact

Non-physical

- Confidentiality issues
- Integrity issues
- Availability issues

Physical

- Property Damage
- Bodily Injury

Leading to losses/claims:

Consequence

- Loss of Income
- 1st Party Costs
- 3rd Party Liability
- Fines & Penalties
- Extortion Demands
- Negligence in Services
- Shareholder Litigation

Cyber Insurance

Network Security & Privacy policies [aka: “cyber policies”] arose to fill the gap in traditional policies and to cover liabilities and costs associated with the impact of a cyber event that impacts the confidentiality, integrity or availability of data or technology.

Event Management / Breach Response

Forensics, public relations, call center, notification and credit monitoring services

Business / Network Interruption

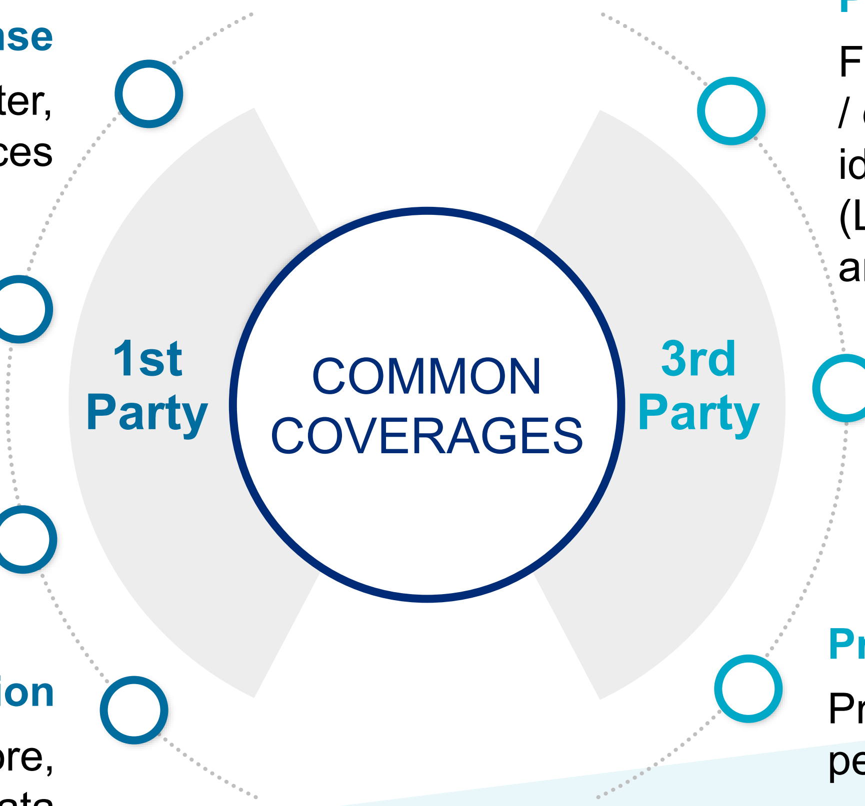
Extra expense and loss of business income

Cyber Extortion / Ransomware

IT Forensics, investigation and ransom payments

Data Restoration

Costs to replace, restore, recreate damaged or lost data



Privacy Liability

Failure to prevent unauthorized access / disclosure of entrusted personally identifiable or confidential information (Liability and defense costs, PCI fines and penalties)

Network Security Liability

Failure of system security to prevent or mitigate a computer attack (Liability and defense costs)

Privacy Regulatory Defense Costs

Privacy breach and related fines or penalties assessed by Regulators

Energy Sector Cyber Gap Filler Sample Solutions

1 Brit – CZ Property Solution / Cyber Attack / OIL WRAP

- Ground up solution
- Covers ensuing physical loss or physical damage to the insured's real & property arising from a cyber act (aka - malicious cyber event)
- Meant to serve as a carve back to LMA5400, but includes traditional cyber capacity.
- Availability – Brit led, Lloyd's based consortium
- Limit - up to $150M+ per policy
- Target insureds - Oil & gas / Upstream, midstream, downstream / utilities sector / logistics / manufacturing / transportation / other heavy industries

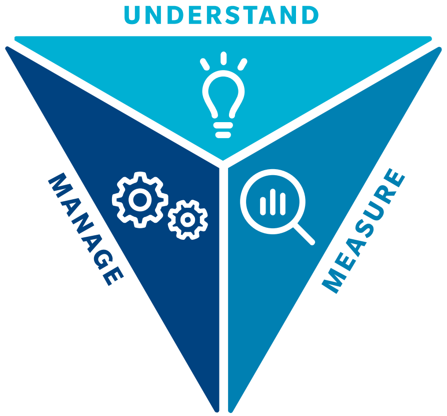
2 Munich Re – Stream Consortium

- Buy back solution, with potential to include ground up traditional capacity in program.
- Cover what would be excluded by a cyber exclusion clause on the property policy, for property damage, business interruption, and operator's extra expense
- Cyber exclusion must be triggered under the property policy for this to respond – aligns with LMA5400
- Availability – MunichRe led, Lloyd's based consortium
- Limit - $275M max for the buy back. May be combined with a traditional cyber policy - $100M is max limit for the traditional
- Target insureds - Oil & gas; $50m dedicated capacity available to power & utility

3 Other Solutions

- AEGIS has limited appetite
- AIG & Chubb DIC / DL approach used in conjunction with cyber policy.
- Approximately 20 London markets can provide capacity on buyback basis.

Cyber Insurance Placement



Understand

- Provide cyber context within a business perspective.

Measure

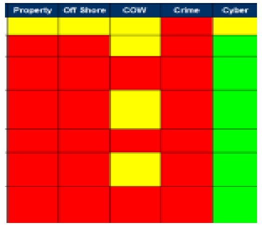
- Quantify the financial impact of cyber exposures.

Manage

- Actionable steps to secure, insure and recover.

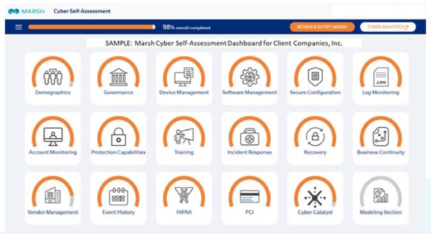
Apply Analytics

- Coverage gap review
- Risk quantification
- Drive program design & limits



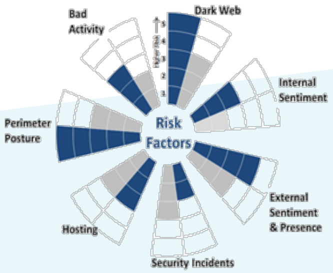
Cyber Submission

- Controls Assessment Application
- CISO level underwriting presentation

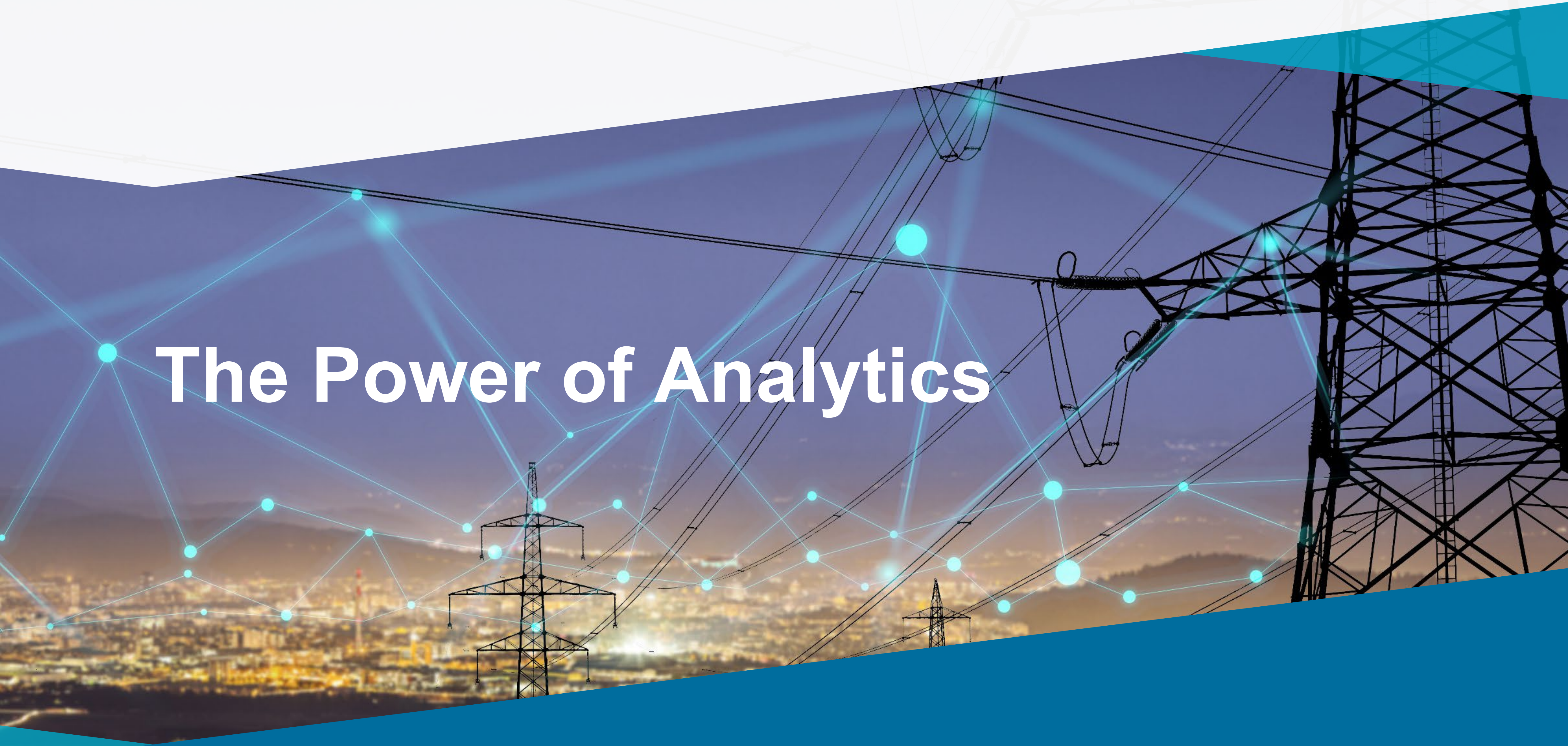


Physical Damage

- Property submission
- Statement of values
- Engineering data reports
- EML data



The Power of Analytics



Measuring Cyber Risks

Resiliency today requires that organizations:

- Evaluate volatility to operations and impacts across both insurable and non-insurable risks
- Determine the efficacy of risk financing strategies and risk capital investments

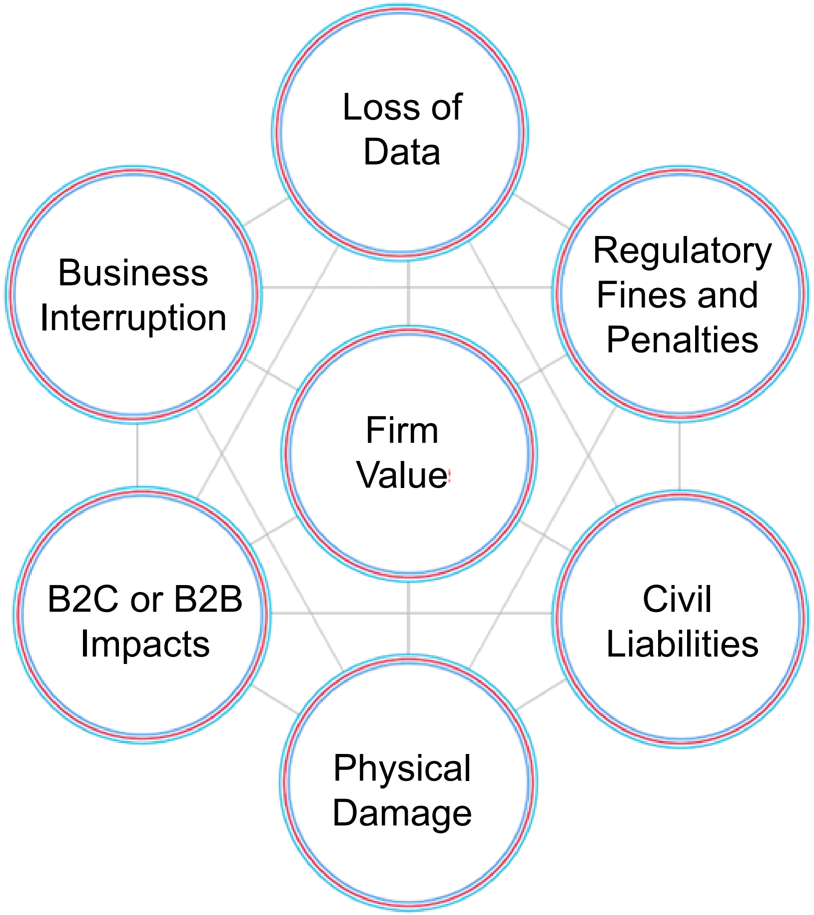
Quality of risk is changing creating the need for an evolution in 'risk understanding'

Deployment of risk capital should be viewed through lens of ROI and financial KPIs

IMPERATIVES IN PRICING EMERGING RISKS

- Technology risks are not 'discrete' in nature
- Traditional measurement approaches limit visibility
- An integrative view to risk is required
- Must evaluate risk in terms of current year P&L and the future strategy impact

Value Chain Threats



Value Chain Analysis

MEASURING VALUE AT RISK

PRODUCTION

DISTRIBUTION

TECHNOLOGY PLATFORMS

CUSTOMERS

We must map risks beyond the enterprise to the full ecosystem.

Evaluating Risk Transfer Strategies

CASE STUDY – CONNECTING CYBER & PROPERTY RISK

Challenge: complex and evolving risk exposure across multiple sites and products.

Solution: data scraped 260 risk engineering reports, layered with additional client data, such as 3rd party contracts.

Output:
- Interactive digital dashboard, stress testing multiple defined risk scenarios to understand the system risk and impact by legal entity, reportable segment, geography, site, and by mechanical and electrical risk factors.
- Evaluation of control efficacy over time and a measurement of insurable and non-insurable risks.

1 CREATE RISK SIMULATIONS
- Client Specific
- Forward-looking
- Capture Risk to Business

2 DETERMINE COST VS. VOLALITY
- Frequency
- Severity
- Estimated Loss & Volatility

3 OPTIMIZE RISK STRATEGIES
- By Risk & Portfolio of Risks
- Evaluation of Risk Capital Investment
- Insurance Coverage Gap Analysis, Limits, & Deductibles
- Captive Solutions & Alternative Risk Transfer

Best Practices Recap

- Move the markets: Marsh’s Global Silent Cyber Initiative
- Use cross functional strategies in property & cyber
- Prioritize property capacity
  - Energy mutual insurers affirmatively cover ensuing damage
  - Identify Lloyds markets with more favorable wording
- Prepare to differentiate the risk to underwriters
  - Provide details on maturity of cyber security controls
- Prioritization of coverage versus exposure
- Quantify your exposure
- Consider risk transfer efficiency

Q&A