AON

Industry Risk Insights

Mining & Natural Resources

Q3 2024

Introduction

Welcome to our Q3, 2024 Mining Risk Insights!

Whilst not our intention to run a theme each quarter, you'll notice that this edition definitely leans towards Cyber. Ranked as the #1 risk across the totality of Aon's Global Risk Management Survey respondents in 2023, and ranked #5 by Natural Resources, cyber risk has evolved dramatically over recent years.

Cyber is still typically perceived to be a risk of un-authorised access to network or data. With ever growing reliance on technology and third-party vendors, we have started seeing a rise in exploits directed to Operational Technology environments causing Business Interruption and Property Damage events – both malicious and incidental.

Cyber threats, cyber-attacks and data breaches are distinct but closely related risks:

- A cyber threat is a possibility that a specific vector or vulnerability will result in un-authorised access to data and network.
- A cyber-attack (or cyber event) is an attempt to gain un-authorised access to data and network via a specific attack vector.
- An attack vector is the way or means used by a hacker to gain access to network or data. Common attack vectors include Social Engineering (Phishing), Credential theft, inside job, and exploitation of a vulnerability in a software or system, etc.
- A successful cyber-attack may impact the Confidentiality, Integrity, and Availability of critical data and systems, that may result in loss of revenue, investigation costs, ransom demands, breach of privacy laws, property damage, and costs to rebuilt systems, etc.

The Mining Industry is not immune to these risks and as the shift towards IoT, automation, and autonomous technology continues, losses from these events will continue to increase.

We trust that you will find this publication to be insightful and as always, please do contact us if you wish to discuss any of this content further.

Kind Regards,
Stacey Lloyd
National Director, Mining

1

Risk Management

Industry Risk Insights - Cyber

Ranked number five by the industry in the 2023 Aon Global Risk Management Survey and number one globally, cyber threats and ransomware attacks have become more frequent, sophisticated and severe in the past four years, with impacts ranging from reputational and financial damage to critical operations being compromised.

After peaking in 2021, the number of ransomware attacks declined in 2022 amid a period of decreased funding for and activity among threat actors, together with improved risk mitigation (including more rigorous cyber-insurance underwriting).

Unfortunately, ransomware attacks jumped 176 percent in the first half of 2023, signalling a need to remain vigilant in managing this threat through strategies such as focused risk assessments, investment in appropriate controls and insurance.

Addressing and recovering from cyber events has become increasingly complex and will continue to be so - Cyber events can have an impact on all areas of an organisation and regulatory bodies are tightening cyber-security requirements.

Interestingly, while 86% of industry respondents indicated that they had a plan or formal review in place regarding cyber risk, the breakdown of mitigation actions that have been undertaken by the industry tells a different story and suggests more work needs to be done to ensure organisations can effectively protect themselves and respond to cyber events.

Top 10 Risks – Mining and Natural Resources	
1	Business Interruption
2	Regulatory/Legislative Changes
3	Commodity Price Risk/Scarcity of Materials
4	Property Damage
5	Cyber Attacks/Data Breach
6	Environmental Risk
7	Political Risk
8	Weather and Natural Disasters
9	Climate Change
10	ESG/CSR

Mitigation Actions - Cyber	
Assessed Risk	23%
Developed Continuity Plans	21%
Developed Risk Management Plan	20%
Evaluated Risk Finance/Transfer Solutions	18%
Quantified Risk	16%

Source: Aon Global Risk Management Survey – Cyber Attack

Current and Emerging Cyber Risk Examples

Risk	Description	Key Insights
Cyber threats to ICS/ SCADA	With the number of major attacks against critical infrastructure increasing, the US Cybersecurity and Infrastructure Security Agency (CISA), along with other Western cyber agencies, continue to issue multiple advisories about threats to operational infrastructure and industrial control systems from state-based threat actors and criminal syndicates. https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf	• Threat actors most commonly exploit known 'critical-path' vulnerabilities. These are pre-existing weaknesses within an organisation's IT infrastructure or cyber defenses. • With geo-political tensions continuing to rise and major east / west and middle-east divisions emerging; attacks on critical infrastructure linked to ICS/SCADA are plausible cyber risks. • Aside from the enormous financial cost of these attacks, they also have national security implications. • Use of ageing and outdated operational software, and the unregulated use of cyber-physical systems in operational infrastructure environments are creating new vulnerabilities.
Lack of cybersecurity skill sets increasing risks for Australia	Australia's Cyber Security Sector Competitiveness Plan 2023 noted in their 2030 outlook the Australian cyber security sector will require almost 5,000 additional dedicated roles each year to meet the demand for 2030. The challenge for the Australian cyber security sector is more than a skills gap. It is a challenge relating to the rapidly evolving technology landscape. At its core, the rapid evolution of cyber threats demands a workforce that is not only technically proficient, but also continuously updated with the latest in cyber threat intelligence and mitigation techniques. SCP - Archive | AustCyber	• Where skills sets are unavailable, businesses' ability to effectively monitor and manage cyber risks decreases • Australia will fall behind other countries and become less competitive in the market • Increase in vulnerabilities across multi-sectors increasing risk of cyber attacks • Inability to keep up to date with advancing technology and associated emerging risks

Risk	Description	Key Insights
Directors and Executives at Risk of Prosecution for Cyber-Attacks	In late 2023, the US Security & Exchange Commission (SEC) commenced proceedings against the Chief Information Security Officer (CISO) and SolarWinds, following the devastating two-year long cyber-attack from 2020. The SEC alleged that the CISO and SolarWinds misled investors about the company's cyber-security practices. In Australia, ASIC is now actively targeting company directors for failing to take adequate measures to protect their organisations from cyber attack. U.S Securities and Exchange Commission Press Release	• Company officers have an obligation to ensure that all practical measures are being taken to protect the organisation's information assets. This coincides with an increase in litigation for climate inaction • Executives and board directors need to satisfy themselves that adequate measure are being taken to protect the organisation against cyber-attack, including: ○ Receiving regular updates on how the cyber threat landscape is changing, including emerging risks ○ Confirming that the organisation has adequate investment in cyber-resilience. This includes strategies to combat potential cyber skills shortages ○ Ensuring the organisation has up-to-date and proven cyber incident response plans in place ○ Participating in regular cyber exercising at the board and executive level

How Can Aon Assist?

Risk Management

- Aon Cyber Impact Analysis - identify and quantify your cyber risks
- Aon CyQu – a self-assessment tool to grade your organisation's cyber risk posture within your digital ecosystem, including key suppliers

Insurance

- Cyber Liability – may provide cover in relation to first- and third-party costs, including business interruption, resulting from a cyber event
- Cyber Physical Damage – may provide cover in relation to physical damage resulting from a cyber event

Industry Profiling – Mining

The Modern Mining Business

Highly coordinated, transnational businesses running diverse production operations across multiple sites, in multiple countries with varied geopolitical climates, all whilst responding to the supply and demand needs of a market-driven global economy.

Operational Hierarchy

Regional offices oversee operations at each mining location & house the Remote Operations Centre (ROC), used to monitor & manage autonomous equipment at site level. Regional offices communicate with the corporate headquarters and each other to coordinate production and other functions.

Vast Exploration Data Sets

The exploration phase generates vast data sets, analysed by geologists to identify new ore deposit locations. This exploration data is very expensive to generate and is critical to the company's future growth and success.

Criticality of Supply Chains

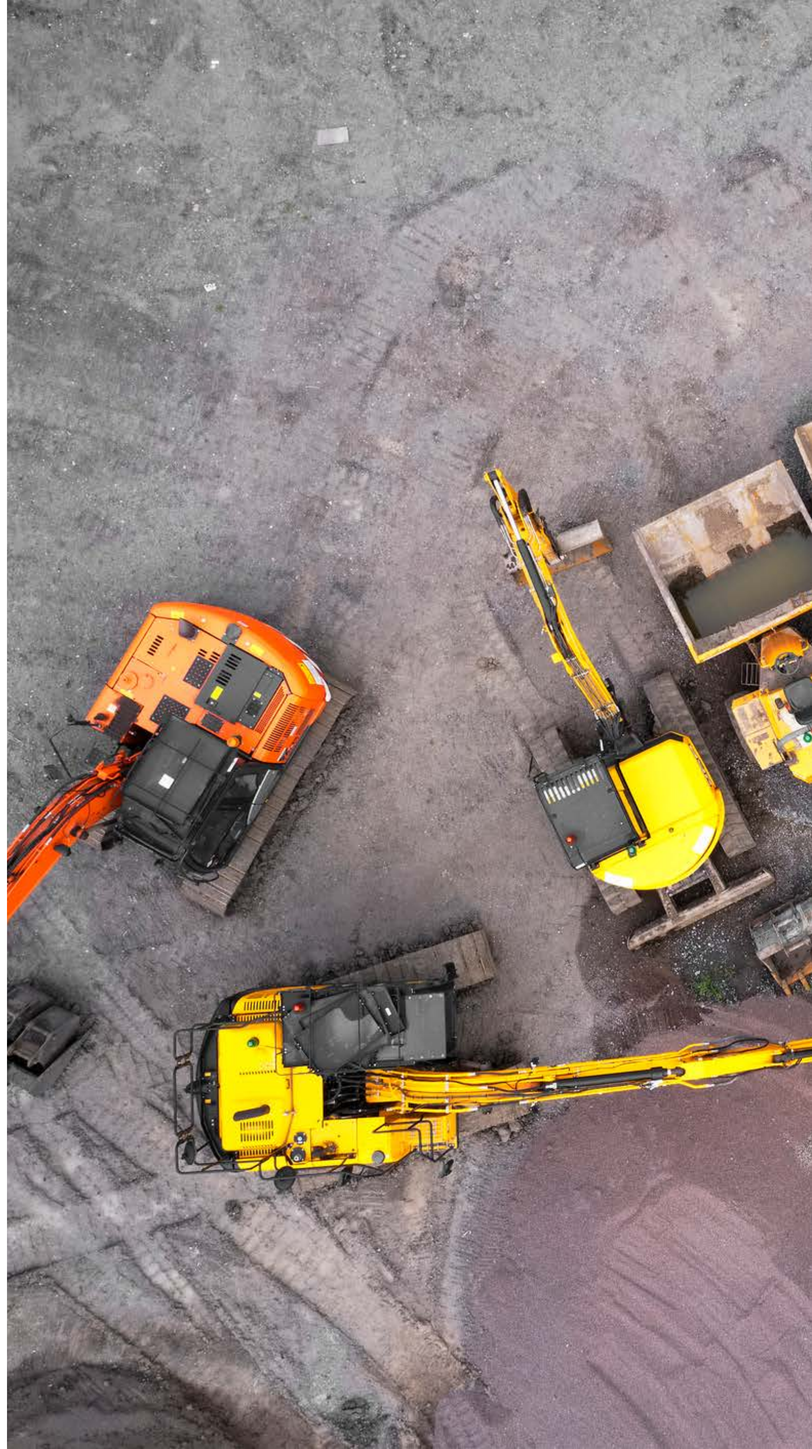
Heavy reliance on key production inputs – electricity, compressed air, diesel & water - with any disruptions to supply chains of any of these major utilities resulting in the cessation of mining operations. The remoteness of many mining locations means sourcing alternative supply is challenging.

From Mine to Port

Mining activities involve accessing, breaking, transporting & processing ore, then shipping to market. Complex industrial technology used includes autonomous and semi-autonomous machinery, SCADA, PLCs, command and control systems, radar, laser, sonar & a vast range of IIoT monitoring devices

Automation and Digitisation of the Industry

Across this vast array of mining activities, automation has become key to achieving maximum ore yields. Automation also bring improved safety, reduced operational costs, greater production consistency, and reduced equipment wear and tear.



Cyber Risks facing Mining Companies

- A Remote Operations Centre can represent a single-point of failure to the supporting mining sites and thus if compromised due to a cyber-attack will result in significant disruption to the overall mining operations
- Highly sensitive and valuable exploration data sets represent a lucrative target for cyber espionage campaigns
- As companies seek to modernise and automate physical mining activities it opens ever increasing remote and cloud-connectivity to OT networks via enterprise networks and software vendors, increasing the attack-surface from which cyber threat-actors can deploy malware and compromise data
- Where the normal operation, control and visibility of equipment is impacted by a cyber-attack it may lead to injury, and damage to assets and the environment: blocked tanks and pipelines, damage to AVs, shut-down of HVAC, cooling and fire suppression systems, catastrophic failure of equipment due to over-speeding, train derailments, port blockages, unsafe furnace shutdowns and uncontrolled chemical reactions.

Risk Transfer Solutions

The Aon CYPD product may provide both conventional cyber and cyber property damage cover to address the key cyber exposures faced by mining organisations, that may include:

- Costs incurred to engage experts to establish cause and extent of a cyber-attack, to mitigate the threat and to restore damaged digital assets;
- The replacement or repair of equipment and plant damaged, as well as any resulting business interruption revenue loss

Mining Industry Cyber Events

Intrusion / Attack Method	Incident Description	Potential Insurability
Third Party Software	• The attack allowed hackers to leak employees' family information on to the 'dark web', as well as a wealth of company data • The stolen data was the result of an attack on GoAnywhere, a piece of third-party file transfer software offered by the cyber security firm Fortra • In addition, payroll information, including pay slips and overpayment letters, was also seized[1]	Substantial
Ransomware	• A mining company experienced a cyberattack that led to the public disclosure of confidential corporate data • The security breach involved sensitive information such as social security numbers, payroll reports, financial details, and residential addresses and phone numbers of top executives, all published online by hackers • The cyber assault targeted critical infrastructure, compromising the integrity of sensitive data and posing potential threats to operational continuity and investigations indicated a high level of sophistication in the attack, emphasising the need for enhanced vigilance and proactive measures to counter evolving cyber threats[2]	Material
Compromised login credentials leaked onto dark web	• Ransomware attack impacted IT systems at the mine and corporate office • As a result of the attack, treatment plant was placed on "preventative" shutdown, with full production resumed by a week later • The company advised that the ransom demand came from a criminal organization likely based in Russia[3]	Material

The information contained in the table above is in summary format only for ease of interpretation, and in respect of the historical incident examples is based on publicly available information. The anticipated insurance coverage position has been offered based on publicly available information relating to the various historical incident examples when reviewed against the ARPC Wrap and BCAP policy wordings to form an abstract view as to whether coverage could have been available under these policies for these incidents.

Intrusion / Attack Method	Incident Description	Potential Insurability
Ransomware	• Ransomware attack - owing to the data whipping capability of the LockerGoga ransomware strain, operations were shut-down for security reasons • Shift to manual operations with production was halted in 170 plants • 35,000 employee devices encrypted and more than 3,000 servers disabled • Company refused to pay the ransom, with the ultimate financial impact totally between $70-$90m from lost sales and remediation costs	Substantial
Ransomware	• Attempted ransomware attack led to significant temporary disruption for a mining supply company • Response require isolating and shutting down IT systems including core Enterprise Resource Planning (ERP) and engineering applications • Progressive restoration of capabilities on a priority basis took place over a period of weeks, with operations still impacted into the following quarter • The incident led to shipments, manufacturing, and engineering disruption, which resulted in overhead under-recoveries and revenue deferrals of £50m in September alone.	Substantial

The information contained in the table above is in summary format only for ease of interpretation, and in respect of the historical incident examples is based on publicly available information. The anticipated insurance coverage position has been offered based on publicly available information relating to the various historical incident examples when reviewed against the ARPC Wrap and BCAP policy wordings to form an abstract view as to whether coverage could have been available under these policies for these incidents.

Aon Cyber Risk Management Solutions

Helping Clients Understand and Quantify Cyber Risk

Cyber Impact Analysis

Aon's Cyber Impact Analysis helps evaluate an organisation's risk exposure through the financial quantification of relevant cyber scenarios.

Insights from our data and analytics highlight what investments in risk management strategies may be needed — including information security, business continuity and cyber insurance.

The results help organisations treat cyber risk with the same sophistication as other enterprise risks by providing data-driven analysis based on relevant cyber scenarios, which can inform these corporate risk management functions:

- **Governance** - Aligning the financial exposures from cyber risk with the corporate risk appetite framework to better demonstrate a reasonable risk-based approach
  to stakeholders
- **Cyber security and business continuity** - Coordinating the roadmap and investment strategy for the cyber risks that could cause the most material financial loss — and better articulating the ROI of these investments
- **Risk Transfer** - Stress testing current cyber insurance limits and retentions to help address the complexity and materiality of cyber exposures to optimise the Total Cost of Risk

Cyber Quotient Evaluation (CyQu)

CyQu is a self-assessment tool that uses leading data analytics to grade your organisation's cyber risk posture within your digital ecosystem, including key suppliers

Key benefits from CyQu include:

- **Instant Visibility** - Immediately after completing the self-assessment survey, you receive a score and breakdown of your key assets and exposures across critical control areas, which will highlight vulnerable areas of your network and potential cyber risks facing your organisation
- **Help Strengthen Security** - Following the snapshot report, a detailed CyQ report from one of our cyber risk consultants is provided, with next-step recommendations and customised strategies to amplify your cyber resilience
- **Benchmarking** - Use your CyQu score to benchmark your cyber security posture against industry targets and your peers, making it easier to determine where to prioritise improvements
- **Simplify Insurance** - CyQu can inform the insurance decision making process by using the report to understand areas of critical vulnerability and transfer that financial risk to an insurance policy. The report can also supplement insurance market submissions to advance the insurance application process

Aon Cyber Property Damage Facility (CYPD)

A proprietary Aon solution for cyber-related physical damage

Following several high-profile cyber-attacks leading to substantial losses being paid by property insurers, the global property insurance market has now largely adopted a blanket exclusion in relation to malicious cyber acts.

Similarly, existing cyber insurance solutions do not provide cover for physical damage to tangible property and any resulting business interruption revenue loss.

Modernisation and automation of physical assets and processes by way of cloud or remote connectivity presents enormous opportunity; but equally introduces new risks for organisations at a time when all connectivity is considered a potential attack vector.

Nefarious actors are increasingly seeking ways to disrupt businesses & critical infrastructure through cyber-attacks, and in many cases actively seeking to cause both damage to real property as well as harm to intangible property

Businesses who rely heavily on operational technology to monitor and control production process, collect data from physical devices or automate and control specific processes are particularly exposed.

To address this gap in cover, Aon has collaborated with underwriters at Lloyd's of London to create an insurance policy that may cover:

Property Damage – caused by a security failure and/or network disruption and covers the costs to repair, replace or reinstate the damaged property

Business Interruption – interruption to business operations caused by the property damage/physical loss resulting from a security failure covering the actual loss of income and extra expenses incurred in restoring normal operations

The policy also includes a built-in bursary to help fund consultancy services relating to your cyber risk and insurance submission.

100%

Lloyd's 'A' rated capacity. Supported by eight major syndicates

75m

Offers up to $75m in capacity

Affirmative

Standalone, or buy-back capacity to traditional property placements

1

Involves a single Lloyd's lead

Bespoke

Primary or excess of loss coverage

100%

administered by Aon Underwriting Managers

2

Mining Industry Risk News

Recent Mining Risk News

Event: Coal miner fined for worker's death under Workplace Health & Safety prosecutor

Link: Carborough Downs mine fined for Brad Duxbury death, Cameron Best injury - ABC News

Solution: Statutory Liability product

While insurance doesn't provide a panacea for all associated impacts of statutory liability e.g. reputational damage; it may provide an efficient means of covering an organisation or individual's costs in responding to a statutory breach.

Aon has created a market leading statutory liability insurance solution, backed by a premier specialist insurer, that may provide cover for:

Strict liability – where the company/individual is responsible for the damages caused by their actions regardless of culpability (fault);

Vicarious liability – where the company or individual is held liable for a breach of legislation by an employee, irrespective of whether the employee intended the act, or the company or individual authorised it;

Personal liability of the directors and officers who may be exposed to fines and penalties regardless of direct involvement in the alleged breach;

Company fines and penalties – to the extent insurable at law (note, in some states/territories insurance policies are provided from providing cover statutory fines);

Defence costs.

Limited underwriting information is required to generate a premium quotation. Coverage under this policy is triggered from when the incident first occurs, not when a claim is brought against the company, as is the case for D&O or Liability coverages.

Event: Underground fire at Anglo's Grosvenor Mine

Link: Emergency services race to seal Grosvenor Coal Mine near Moranbah as fire burns underground - ABC News

Solution: Property Damage & Business Interruption insurance that may provide effective coverage.

3

Insurance Industry News

Recent Insurance News

Event: Updates to Western Australia Workers Compensation Act

Link: https://www.workcover.wa.gov.au/resources/modernising-was-workers-compensation-laws/.

Summary: The Western Australian Government has updated the WA Workers Compensation and Injury Management Act (The Act) effective 1 July 2024. The Act affects Workers Compensation insurance policies covering employment in Western Australia.

The new Act is the most comprehensive update to the legislation in over ten years and includes material changes to worker benefits, claims processes and insurance requirements. In addition, WorkCover WA has issued a new Prescribed Form which must be provided for the renewal and adjustment of a policy. The penalty for an employer not using the Prescribed Form is $10,000 per worker employed.

Event: Aon Launches Carbon Capture Product

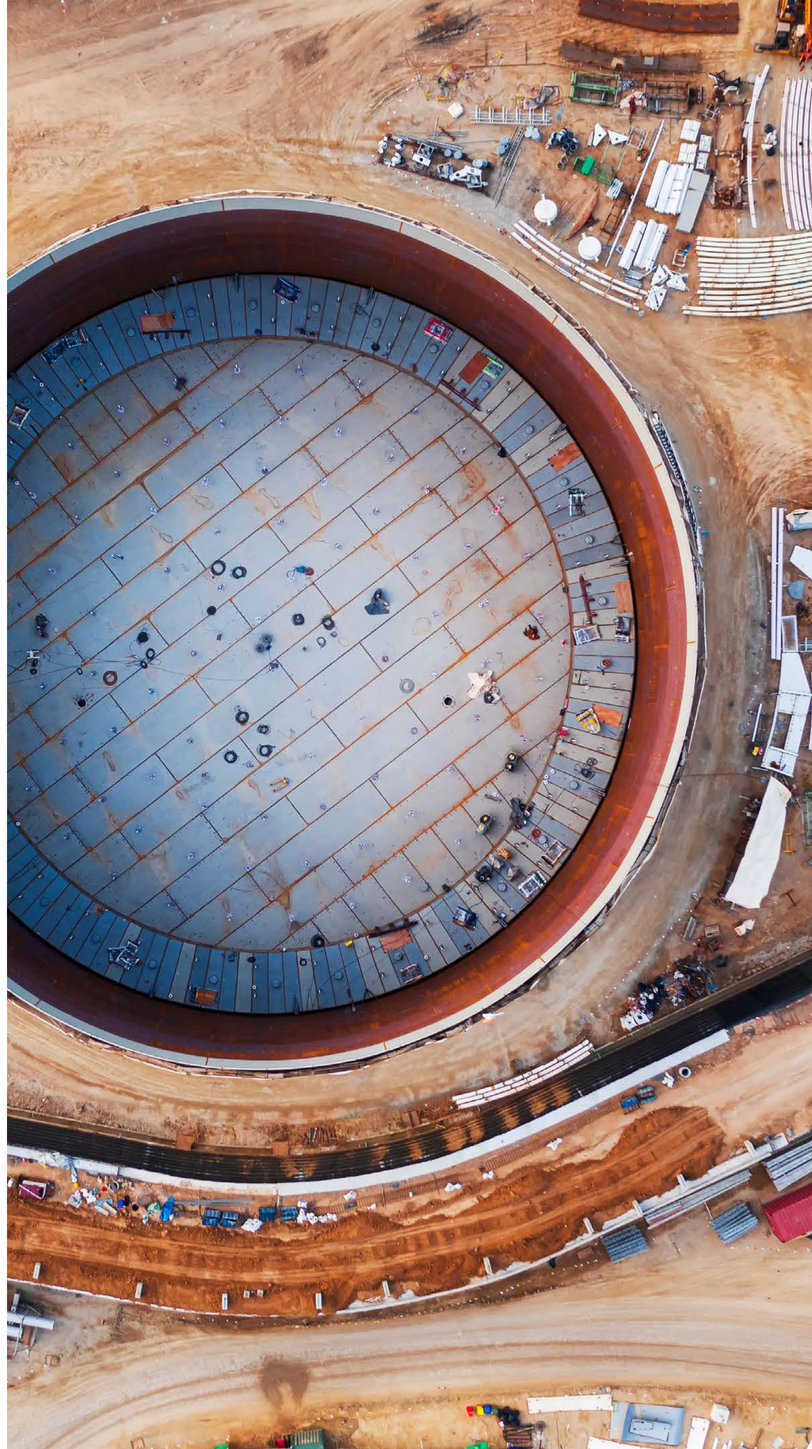
Link: Aon launches carbon capture and storage insurance product | Insurance Times

Summary: Aon has launched a new insurance product for eligible international transport and storage companies engaged in storing carbon monoxide. The new product is aimed at providing cover for risk exposures associated with carbon capture and storage, and may provide capacity for physical risk, loss of revenue and general liabilities for large-scale projects.

Event: Captive establishment & utilisation trending upwards after hard market

Link: Captive Insurance: Uptick in Use Reflects Market Realities | Global Risk Management Survey (aon.com)

Summary: As more companies become comfortable using captives and understanding the value they add, captives are likely to become further embedded into corporate risk strategies, regardless of market conditions.



Event: Aon launches the first fully comprehensive carbon capture and storage insurance solution to support energy transition

Link: Aon UK Media Room Article: Aon launches the first fully comprehensive carbon capture and storage insurance solution

Aon has announced that it has developed a new insurance product designed specifically for international transport and storage companies that are engaged in storing carbon dioxide.

The new product is aimed at providing cover for key risk exposures associated with Carbon Capture and Storage (CCS) and advances the role of insurance in de-risking global CCS projects. This, in turn, opens up access to capital providers and investors, addresses a significant protection gap for these developments, and changes the perception of what is insurable. Carbon Capture Utilisation and Storage addresses aspects of environmental, social, and governance (ESG) by reducing carbon emissions and allowing energy and other emitting industries to meet their net zero goals and objectives.

Aon's energy transition product was created through its role as insurance broker to Eni UK, the lead company in the consortium delivering the innovative low carbon and hydrogen HyNet North West project (in which Eni is the transportation and storage operator), and the Northern Endurance Partnership (NEP), comprising of bp, Equinor, and TotalEnergies. This project is among the first large commercial-scale and complete carbon transportation and sequestration processes for capturing, removing and storing industrial carbon dioxide emissions – which is key to the decarbonisation of the UK's industrial heartland. The product has been developed acknowledging energy regulators and stakeholder expectations and in support of the assessment of available insurance coverage. While it was initially created in conjunction with a UK project, it has been designed to work for projects globally.

Aon's multi-component CCS solution has the following key features:

Sufficient capacity for physical risks, loss of revenue and general liabilities for large-scale projects;

Newly created and bespoke coverage that responds to issues with storage reservoir integrity, including loss of revenue;

Indemnity for loss of tax credits or requirements to purchase carbon credits associated with a leak of CO_2 from the carbon storage facility; and

Placement with A- or higher-rated insurers, predominantly in the London market.

William Lynch, business leader for natural resources at Aon, said:

"Carbon capture is a fundamental component in reducing emissions and supporting the energy transition. While challenges remain, this is a first-of-its-kind risk transfer solution, aimed at providing comprehensive cover under an agreed policy wording, for transport and storage companies engaged in CCS. Cover spans the construction and repurposing of existing assets as well as the operational phase. A huge benefit for operators and their investors, as well as their customers, is knowing what their insurance costs and coverage will be in an otherwise uncertain market.

"Aon has spearheaded the development of this product over the last 18 months, working in collaboration with leading underwriters, and the legal community and we look forward to working on many similar projects.

Links

https://www.aon.com/en/insights/reports/global-risk-management-survey

https://www.aon.com/en/industries/natural-resources

https://www.aon.com.au/australia/aon-global-risk-consulting/files/agrc-value-proposition.pdf

Contact Us

Paul Pryor (VIC)
Global Mining Practice Leader
+61 478 321 376
paul.pryor@aon.com

Stacey Lloyd (VIC)
National Director, Mining
+61 436 535 085
stacey.lloyd@aon.com

Joshua Kelliher (VIC)
Client Executive
+61 458 820 327
joshua.Kelliher@aon.com

Neil Massey (NSW)
National Manager, Client Risk
+61 478 879 330
neil.massey1@aon.com

Emma Andersson (NSW)
Client Executive
+61 413 234 009
emma.andersson@aon.com

Michael McLachlan (QLD)
QLD Mining Leader
+61 421 617 806
michael.mclachlan@aon.com

Blair Sands (QLD)
Client Manager
+61 414 312 200
blair.sands@aon.com

Jordan Allen (QLD)
Client Manager
+61 438 855 540
jordan.allen@aon.com

Joe Felfer (QLD)
Client Executive
+61 425 060 495
joe.felfer12@aon.com

Rohan Lambert (QLD)
Client Executive
+61 421 133 677
rohan.lambert@aon.com

Steve Bergin (WA)
Client Manager
+61 407 422 998
steve.bergin@aon.com

Dylan Ellis (WA)
Client Executive
+61 457 664 586
dylan.ellis2@aon.com

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues in over 120 countries provide our clients with the clarity and confidence to make better risk and people decisions that protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

aon.com