Thank you for joining; the webinar will start shortly.
GLENN LEGGE
PARTNER
COMMODITIES
T: 713-706-1941
E: GLENN.LEGGE@HFW.COM

CADE WHITE
PARTNER
COMMODITIES
T: 713-706-4907
E: CADE.WHITE@HFW.COM

MICHAEL WRAY
PARTNER
SHIPPING
T: 713-706-4905
E: MICHAEL.WRAY@HFW.COM

MELANIE FRIDGANT
ASSOCIATE
SHIPPING
T: 281-305-5154
E: MELANIE.FRIDGANT@HFW.COM
Cyber Attack Response Strategies

Contractual Risk Allocation, Insurance Coverage and Regulatory Requirements – Who’s on First …?
AGENDA

• Evolving Cyber Threat Environment
• Types/Impacts of Cyber Attacks
• Risk Allocation Tools to Address Cyber Attacks and Resulting Impacts/Damages
• Cyber Insurance Coverage and Notifications
• Regulatory Requirements and Reporting
• Cyberattacks = the introduction of malicious viruses by state and non-state actors into digital processes that require maintenance and anti-virus updates.

• Utilization of contractual risk allocation and insurance coverages to address the liabilities and response costs arising from evolving cyber threats.

• Compliance with US regulations and industry standards when determining the appropriate response strategy to a cyberattack.
EVOLVING CYBER THREAT ENVIRONMENT

• CISA – ICS Alerts
  o **July 20, 2021** – Alert (AA21-201A) – Chinese campaign against US Oil and Gas Pipelines.
    ▪ 13 confirmed compromised pipelines, 7 unknown depth of intrusion, 3 near misses.
    ▪ Spearfishing and social engineering.
  
  o **February 09, 2022** – Alert (AA22-040A) – 2021 Trends Show Increased Globalized Threat of Ransomware.
    ▪ Increased professionalism – Ransomware as a Service (RaaS).
    ▪ Shift from "big game" targets to mid-sized business entities.
• CISA – ICS Alerts
  o **March 17, 2022** – Alert (AA22-076A) – CISA and FBI disclose threats to US and international satellite communication (SATCOM) networks.
  o **March 15, 2022** – Alert (AA22-074A) – Russian state-sponsored cyber actors gained network access through CISCO MFA protocols. Recommend increased use of time out/lock out defense to repeated failed logins.
• Types/impacts of cyberattacks
  ▪ Types
    ▪ Denial of Service (DOS), Distributed Denial of Service (DDOS)
    ▪ Phishing/Whale Phishing
    ▪ MITM
    ▪ Spear-phishing
    ▪ Ransomware
    ▪ Brute force attack
• Impacts
  - Loss of confidential, operational and/or financial data.
  - Loss of critical control systems
    - Navigation
    - Well control/MPD
    - RTM
    - Communications
• Damages
  - Physical/kinetic damage
  - Personal injury/death
  - Environmental impairment
  - Lost/delayed production
  - Business interruption
  - Loss of proprietary data
  - Costs of responding to cyber attacks
  - Reputational damage
• **Contractual Risk Allocation Terms and Conditions.**
  
  o Contractual defense, indemnity and additional insured clauses – will they be effective?
  
  o Coordination of contractual risk allocation, insurance coverage and management of cyber response activities and costs.
RISK ALLOCATION TOOLS TO ADDRESS CYBER ATTACKS

• Contractual Risk Allocation
  ▪ Express terms regarding cyber security procedures/systems/updates.
    o Industry standards
    o Regulatory requirements
    o Reporting past/current cyber incidents, sharing cyber threat information.
    o Extension to each Party's subcontractors/sub-subcontractors.
• Contractual Risk Allocation
  ▪ Knock Knock
    o Are standard KFK risk allocation terms applicable to identified risks (equipment, people, pollution) impacted by cyber-attacks on digital systems that were maintained to O&G industry and regulatory standards?
    o Current KFK risk allocation provisions based upon category of people/property – do they apply to cyber related damages?
    o Insurance policies supporting contractual D&I obligations may have a cyber-exclusions.
• **Warranty**
  - Generally accepted industry standards re: quality, specifications, performance and/or functionality.
  - Warranty require Supplier to provide/perform cyber security updates?
• Contractually Required Insurance Coverages
  o **Required insurance coverages** (Scheduled Property, COW, Redrill, Extra Expense Seepage and Pollution, Care Custody & Control, Extended Cost of Control or Redrill, ROW, Making Wells Safe) - **subject to cyber exclusions**?
  o **Cyber Response Insurance**?

• **Force Majeure**
  o Is a cyber-attack on a digitized control system provided by subcontractor/vendor an FM event?
  o Is a cyber-attack **beyond the reasonable control** of the party providing/maintaining the digitized control system?
  o Is the subcontractor/vendor obligated to provide notice of cyber updates to purchaser/lessee?

• **Limitation of Liability** – Impacted by failure to comply with cyber security industry standards and updates?
INSURANCE COVERAGE AND NOTIFICATIONS

- Coverages – Each cyber response insurance policy will have different terms, limits and notice requirements.
  - First Party Coverage
    - Notice requirements under insurance policy.
    - Initial expenses for response activities involving forensic analysis, notification and legal expenses.
  - Legal Privileges
    - Attorney Client
    - Investigative Privileges
  - BI and recovery costs – may involve required use of insurer's cyber security and cyber response contractors/advisors.
  - Ransomware coverages?
INSURANCE COVERAGE AND NOTIFICATIONS

- Third party coverages for damages arising from cyber attacks
  - Disclosure or misappropriation of confidential data.
  - Shareholder claims for violation of corporate cyber security requirements.
  - Third party and governmental claims arising from cyber event.
  - All dependent upon insured's compliance with insurer's cyber security requirements and possible utilization of insurer's IT cyber response contractors/advisors.
2021 Lloyd's Cyber Exclusions – Largely focused on state based cyber exclusion against another computers/digitized systems located in another state.

- **LMA5564** – Exclusion 1 – Excludes all losses from war or "cyber operations".
- **LMA5565** – Exclusion 2 – Excludes coverage arising from "retaliatory cyber operations" between specified states, including impacts on the availability of "essential services" in a state. Buy back for "other cyber operations" may be available.
- **LMA5566** – Exclusion 3, is very similar to Exclusion 2, but with no opportunity to buy back coverage for “other cyber operations”.
- **LMA5567** – Exclusion 4 is similar to Exclusion 3, but allows a buyback for "bystander cyber assets" that are affected by a "cyber operation" but is not required to be physically located in an impacted state.
• **USCG**
  - CG-5P Policy Letter No. 08-16 – Reporting Suspicious Activity and Breached of Security
  - NIST Cybersecurity Framework
  - National Cybersecurity and Communications Integration Center (NCCIC) – Incident response and management center for cyber incidents.

• **US Department of Treasury – Office of Foreign Asset Control (OFAC)**
  - OFAC – Advisories on Sanctions Risk for Facilitating Ransomware Payments
    - September 21, 2021 OFAC Update
    - OFAC Designation of Malicious Cyber Actors
    - Ransomware payments with sanctions nexus
    - Ransomware payments may violate OFAC Regs
      - Mitigation possible if company paying ransomware maintains:
        - Sanctions compliance program;
        - Updated cybersecurity practices

• **Cybersecurity & Infrastructure Security Agency (CISA)**
  - Ransomware Guide 2020
QUESTIONS?
CONTACTS

GLENN LEGGE
PARTNER
COMMODITIES
T: 713-706-1941
E: GLENN.LEGGE@HFW.COM

CADE WHITE
PARTNER
COMMODITIES
T: 713-706-4907
E: CADE.WHITE@HFW.COM

MICHAEL WRAY
PARTNER
SHIPPING
T: 713-706-4905
E: MICHAEL.WRAY@HFW.COM

MELANIE FRIDGANT
ASSOCIATE
SHIPPING
T: 281-305-5154
E: MELANIE.FRIDGANT@HFW.COM