crowell moring

MINING LAW MONITOR

VOLUME 28 | ISSUE 1 | SUMMER 2015

Daniel W. Wolff, Editor

INSIDE THIS ISSUE

Confidentiality in Crisis: the Government Agency Assault on Company Confidentiality Policies and Agreements

By Christopher Calsyn, Thomas P. Gies

Your company's confidential information may no longer be safe. Federal government agencies, including many that regulate mining companies, are aggressively scrutinizing company confidentiality policies and agreements. This scrutiny is all in the name of preventing corporations from muzzling potential whistleblowers. Although there is no evidence that confidentiality policies and agreements actually stifle whistleblower activity, this new regulatory initiative is having tangible impacts. Mining companies should take steps now to minimize the odds that they will be the next target of the regulators.

Agency Challenges to Confidentiality Policies and Agreements

The SEC's KBR Cease and Desist Order

The Securities and Exchange Commission (SEC) is the latest agency to challenge commonly used confidentiality agreements. The SEC announced this initiative in March 2014. Sean McKessy, who heads the SEC's Office of the Whistleblower (OWB), stated that his office was "actively looking for examples of confidentiality agreements, separat[ion] agreements, [and] employee agreements that ... in substance say 'as a prerequisite to get this benefit you agree you're not going to come to the commission or you're not going to report anything to a regulator.'"

This warning was amplified in the SEC's 2014 annual report on the state of the Dodd-Frank Whistleblower Program. The SEC noted there that the OWB:

> *is actively working with Enforcement staff to identify and investigate practices in the use of confidentiality*

and other kinds of agreements that may violate … Commission rule[s]. We will continue to focus on agreements that attempt to silence employees from reporting securities violations to the Commission by threatening liability or other kinds of punishment.

In February of this year, the Wall Street Journal reported that the SEC had sent letters to numerous publicly traded companies demanding production of any documents, policies, or agreements that contain provisions that may restrict an employee from reporting potential violations to the SEC. Many observers believed it was only a matter of time until the SEC initiated litigation against a company over a confidentiality policy or agreement.

That belief was vindicated when the SEC announced, on April 1, 2015, that KBR, Inc. had agreed to a cease and desist order (KBR Order) in a regulatory dispute over a confidentiality agreement that employees interviewed during an internal investigation were required by KBR to sign. The KBR Order requires the company to: (a) pay a $130,000 civil fine; (b) revise the offending policy; (c) make reasonable efforts to notify those subject to the prior policy of the change and that they are no longer subject to the prior policy; and (d) certify that it took those reasonable efforts.

The confidentiality agreement stated as follows:

I understand that in order to protect the integrity of this review, I am prohibited from discussing any particulars regarding this interview and the subject matter discussed during the interview, without the prior authorization of the Law Department. I understand that the unauthorized disclosure of information may be grounds for disciplinary action up to and including termination of employment.

The SEC asserted that the KBR agreement violated SEC Rule 21F-17. That rule, adopted by the SEC in 2011 as part of its regulations implementing the Dodd-Frank Act, states in relevant part:

(a) No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications.

According to the SEC, KBR's policy of requiring pre-approval by its legal department to disclose the subject matter of the interview undermined Section 21F's purpose of "encourag[ing] individuals to report to the Commission." The SEC acknowledged that it lacked any evidence that the requirement actually stifled putative whistleblowers from reporting, or that KBR had sought to enforce that provision to prevent whistleblowing. The SEC nonetheless found the agreement violated Rule 21F-17 on its face.

The new agreement implemented by KBR as part of the settlement removes the pre-approval requirement. Employees are also not required to notify KBR that they are providing information to the SEC. The agreement now contains the following amended provisions:

Nothing in this Confidentiality Statement prohibits me from reporting possible violations of federal law or regulation to any governmental agency or entity, including but not limited to the Department of Justice, the Securities and Exchange Commission, the Congress, and any agency Inspector General, or making other disclosures that are protected under the whistleblower provisions of federal law or regulation. I do not need the prior authorization of the Law Department to make any such reports or disclosures and I am not required to notify the company that I have made such reports or disclosures.

In the wake of the KBR Order, several commentators have questioned whether the SEC is empowered to regulate confidentiality agreements in this manner. Because KBR settled the dispute, that question remains unanswered. In the meantime, employers subject to SEC regulation are reassessing their own confidentiality policies and agreements.

The NLRB and EEOC Adopt Similar Approaches

The KBR Order follows similar efforts made by two other federal agencies very familiar to the mining industry – the National Labor Relations Board (NLRB) and the Equal Employment Opportunity Commission (EEOC).

NLRB Targets Confidentiality Instructions in Internal Investigations

First, decisions made by the NLRB prohibit employers from uniformly barring employees from discussing ongoing internal investigations. *See Banner Health Systems*, 358 NLRB No. 93, slip op. at 2 (2012) (employer's "generalized concern with protecting the integrity of its investigations is insufficient to outweigh employees' Section 7 rights").

Employers instead must specifically determine that the need for a confidentiality instruction outweighs the statutory right of the employees to discuss the subject of the investigation. This

determination must be made before the instruction can be given, based on the facts surrounding the particular investigation at issue. And the employer can only give the instruction if it finds that: (a) witnesses need protection; (b) destruction of evidence was possible; (c) testimony may be fabricated; or (d) there was evidence of a potential cover up. *Hyundai America Shipping Agency*, 357 NLRB No. 80, slip op. at 15 (2011).

The *Banner Health* and *Hyundai* rulings apply to all non-supervisory employees in all private sector companies, not just those working in unionized locations. All employers therefore must ensure they satisfy the *Banner Health*/*Hyundai* test before instructing employees to not discuss an ongoing internal investigation. In most cases, employers will be able to identify a significant risk of at least one of the four factors listed above coming true such that giving the instruction is defensible. Nevertheless, mining companies can expect the NLRB will continue to scrutinize such instructions.

The EEOC Targets Separation Agreements

In a similar vein, the EEOC filed two high-profile cases in 2014 claiming similar language in separation agreements improperly prevents employees from bringing charges of employment discrimination. *See EEOC v. CVS Pharmacy, Inc.*, No. 14-cv-863, 2014 WL 5034657 (N.D. Ill. Oct. 7, 2014); *EEOC v. CollegeAmerica Denver, Inc.*, No. 14-cv-01232, 2014 WL 6790011 (D. Colo. Dec. 2, 2014).

It is well settled that a separation agreement cannot include a waiver of an employee's right to file a claim of discrimination or retaliation with the EEOC. But in these recent cases the EEOC targeted confidentiality and related provisions included in most separation agreements. For example, in *CVS*, the EEOC argued, *inter alia,* that standard cooperation, non-disparagement, and confidentiality provisions improperly impeded the employee's right to bring a charge or cooperate with the EEOC.

In both cases, the courts dismissed the EEOC's relevant claims on procedural grounds at summary judgment. Neither court addressed the substantive merit of the EEOC's claims. Yet the EEOC appears undaunted by these procedural defeats; the EEOC's appeal of the *CVS* case is currently pending before the Seventh Circuit.

Employers should expect the EEOC will continue to target standard clauses in confidentiality policies and agreements that it claims improperly impede employees' rights to assert a claim of discrimination or retaliation.

Recommendations

So what should mining companies be doing now in light of these challenges to "standard" confidentiality provisions? Unfortunately, there is no one size fits all answer.

At a minimum, companies should review all policies and agreements that may arguably impede the ability of employees to act as whistleblowers. Such policies and agreements include those that regulate non-disclosure, confidentiality, non-disparagement, and cooperation. Any provisions that expressly bar cooperating with government agencies, or that require pre-approval from the employer to speak with these agencies, should be scrutinized and probably revised.

This is not to say that all mining companies should automatically adopt all of the language in the new KBR policy. In deciding whether to make any changes, employers instead should consider the likelihood of potential SEC or EEOC litigation in a manner consistent with the company's tolerance for risk. Companies may then decide to make changes to all policies and agreements that arguably relate to this issue. Conversely, some may only modify certain provisions such as confidentiality provisions in separation agreements, or agreements signed by witnesses during internal investigations.

At a minimum, companies should review all policies and agreements that may arguably impede the ability of employees to act as whistleblowers.

Employers face the challenge of deciding whether and which policies and agreements to modify now without additional guidance. The courts have not yet addressed the merits of the aggressive positions of the SEC and EEOC on these issues. It is thus unclear how courts will address employers' legitimate concerns. Such concerns include: (a) protecting the confidentiality of sensitive proprietary information; (b) ensuring the company's ability to conduct an internal investigation is not compromised by an employee's disclosure; and (c) properly preparing for any agency investigation.

In the meantime, companies subject to both SEC and NLRB authority should harmonize the confidentiality instructions given during internal investigations. After first determining

the *Banner Health/Hyundai* test is met, employers should inform employees that while they must not discuss ongoing investigations, that prohibition does not impact the employee's ability to report a possible violation of law to a relevant government agency.

Employers conducting such investigations under attorney-client privilege should also still convey proper *Upjohn* warnings (*i.e.*, notifying interviewed employees that communications made in the course of the company's internal investigation are within the company's privilege). None of the agency initiatives summarized above impinge on an employer's right to protect its privileged communications. Depending on a variety of circumstances, some mining companies may consider modifying the *Upjohn* warning to inform witnesses that the confidentiality directive is not intended to prevent the witness from disclosing underlying facts discussed with the attorney to a government agency as part of a report of an alleged violation of any applicable law or regulation.

Companies should also consider three additional changes. **First**, adding an explicit prohibition on employees disclosing proprietary information in reports of alleged violations of law made to applicable federal or state law enforcement agencies. Such a provision should be clear that the employee is free to report alleged violations to an agency, but cannot disclose proprietary information in doing so.

Second, companies should consider requiring employees to notify the employer of any report of an alleged violation of law they make to a government agency either before or immediately after making the report. Requiring notification is consistent with ensuring a corporate culture of compliance, as employers cannot investigate and remedy issues of which they are unaware. If employers maintain a notification requirement, the policy should be explicit that the duty to notify the employer is solely so that the employer can: (a) protect privileged communications as needed; (b) conduct an internal investigation; and (c) properly prepare for any agency investigation.

Third, employers should ensure their applicable policies and agreements include a statement that reporting alleged violations of law to a government agency will not result in retaliation against the employee. The SEC may take issue with the prohibition on disclosing confidential information and/or notification requirement described above. But tying these provisions closely to the anti-retaliation provision may suffice to prove the policy changes are intended solely to protect the employer's legitimate concerns. Moreover, ensuring a putative whistleblower will be free of retaliation is consistent with creating the desired compliance culture, and increases the chances of an employee reporting concerns internally before going to regulators.

Finally, employers should keep a close eye on the case law as it develops and be prepared to amend any relevant policies or agreements as needed.

* * *

Diesel After DEMS: Regulatory Developments on the Horizon for Mining

By Edward M. Green, Sherrie A. Armstrong

Diesel exhaust exposure for underground miners has been regulated since the Mine Safety and Health Administration (MSHA) issued Diesel Particulate Matter (DPM) rules for underground coal miners and underground metal and nonmetal miners in 2001. In a related effort, beginning in 1992, the National Cancer Institute (NCI) and the National Institute for Occupational Safety and Health (NIOSH) conducted a study of the effects of DPM on miners in eight nonmetal mines, seeking to determine whether a link existed between lung cancer mortality in the miners in those mines and exposure to DPM. That study, known as the Diesel Exhaust in Miners Study or "DEMS," extended over a 21-year period and is a major contributor to the prospect of revised (and more stringent) diesel regulations in the mining industry. As scientists begin to build on the work done by DEMS, agencies are taking preliminary steps that may prove to be the building blocks for future diesel regulation. This article explores what regulatory developments inspired by DEMS may be on the horizon for the mining industry.

MSHA's Current DPM Regulations

On January 19, 2001, MSHA issued DPM rules addressing the health hazards to underground metal and nonmetal miners and underground coal miners from exposure to

DPM. The preambles to these rules contained a comprehensive risk assessment[1] in which MSHA had determined that diesel particulate matter puts underground miners at increased risk for heart and lung disease, including lung cancer.[2] In metal and nonmetal mines, MSHA imposed permissible exposure limits (PELs) for underground miners of 160 micrograms of total carbon per cubic meter of air measured as an eight-hour equivalent shift concentration with staggered effective dates for implementation of that limit. Mine operators were required to achieve concentrations at or below the PEL by installing and maintaining feasible engineering and administrative controls. If not feasible, mine operators had to use engineering controls to achieve as low a level as feasible and then provide supplemental respiratory protection for the exposed miners. The rules imposed other requirements ranging from fueling practices, maintenance standards, training, exposure monitoring, and record-keeping requirements.

Protracted litigation over the metal/nonmetal DPM rule followed, culminating in a 2007 D.C. Circuit case upholding the legality of the DPM rules in their entirety.[3]

Diesel Exhaust in Miners Study (DEMS) and Reanalysis Efforts

Between 1992 and 2012, NCI and NIOSH undertook a major retrospective cohort lung cancer mortality and nested case-control study of 12,315 surface and underground workers at eight non-metal mines (trona, potash, salt, and limestone). The agencies collected data at those mines from 1992 through 1997. Because there is no means for assessing the toxicity of diesel exhaust when examined in its totality, the study used respirable elemental carbon (a component of diesel exhaust) as the primary surrogate for diesel exhaust. The study also used historical measurements to estimate, retrospectively, the exposure of each worker in the study.

That study culminated with the publication of seven peer-reviewed papers.4 The final nested case-control study and cohort mortality study papers were published in 2012.5 The DEMS

MSHA Spring 2015 Regulatory Agenda

The Administration announced its regulatory agenda just before the Memorial Day Holiday weekend. Included on the slate for the Mine Safety and Health Administration are the following actions:

- **Refuge Alternatives for Underground Coal Mines:** MSHA will continue to analyze comments in response to its August 2013 request for information on how to improve this standard, originally promulgated in 2008. The comment period, which had been extended several times, closed in April.
- **Request for Information to Improve the Health and Safety of Miners and to Prevent Accidents in Underground Coal Mines:** As of now, MSHA has extended the period for commenting on its RFI through June 26, 2015. The RFI posed a good number of questions and was published with the intent of addressing through future rulemaking a multitude of issues raised by the agency's investigation of the Upper Big Branch mine explosion.
- **Exposure of Underground Miners to Diesel Exhaust:** In the wake of the International Agency for Research on Cancer's June 2012 classification of diesel exhaust as a known human carcinogen, as well as findings by NIOSH and the National Cancer Institute based on their own study of the subject matter, MSHA plans to publish a request for information by the end of this year to explore new regulatory approaches for controlling exposure to diesel particulate matter and exhaust in both coal and metal/nonmetal underground mines.
- **Examination of Working Places in Metal and Nonmetal Mines:** MSHA plans to issue a request for information by September 2015 to explore new rulemaking that would address the examination of working places in metal/nonmetal mines, focused on (1) who conducts the examination; (2) the quality of the examination; and (3) examination recordkeeping. MSHA is also considering new guidance as an alternative approach.
- **Respirable Crystalline Silica:** MSHA continues to keep this issue on its agenda as an expected health standard for metal/nonmetal mines, although its long-anticipated notice of proposed rulemaking is now pushed back to April 2016. As envisioned, MSHA would adopt an exposure limit of 50 ug/m3. The delay is due, at least in part, to the fact that MSHA is essentially just waiting to adopt OSHA's health-effects and risk-assessment methodology from the analogous OSHA rulemaking already in progress. OSHA has not announced when it expects to promulgate its final rule, although the general belief is that it will be before the current administration leaves office.
- **Proximity Detection for Mobile Machines in Underground Mines:** MSHA's current plan is to publish a notice of proposed rulemaking by July of this year to address hazards in underground mines associated with the operation of mobile equipment.
- **Criteria and Procedures for Proposed Assessment of Civil Penalties:** MSHA anticipates publishing the final rule revising its Part 100 civil penalty criteria by the end of this year.

The complete regulatory agenda can be accessed at: http://www.reginfo.gov/public/do/eAgendaMain.

authors concluded that exposure to diesel exhaust caused a statistically significant increased risk of death from lung cancer in excess of that otherwise predicted from cigarette smoking and the natural occurrence rate.

DEMS is widely considered to be the most significant epidemiological study to date due to its size and the agencies' use of respirable elemental carbon as a quantitative marker of exposure to diesel exhaust. As one commenter put it, "[t]hese papers are expected to have considerable impact on the evaluation of the carcinogenic potential of diesel exhaust and, furthermore, on occupational and environmental limit value discussions related to diesel motor emissions and particle exposures."6

DEMS, is, however, a backwards-looking study that does not measure the impacts of exposure to today's improved diesel engens or diesel fuel.

DEMS is, however, a backwards-looking study that does not measure the impacts of exposure to today's improved diesel engines or diesel fuel. Furthermore, DEMS is not without its critics – and scientists attempting to replicate its findings have reached different conclusions than did the NCI and NIOSH authors. Specifically, after no small effort over a number of years, an industry coalition led by the Truck & Engine Manufacturers Association (EMA) obtained access, albeit somewhat limited access, to the DEMS data so that it could be reanalyzed by an independent team of epidemiologists and biostatisticians.7

The EMA independent team of researchers also examined the role of temporal factors in modifying the estimated effects of exposure to diesel engine exhaust on lung cancer mortality and characterized risk by mine type in the DEMS cohort.8 They found that the respirable elemental carbon-associated risk of lung cancer mortality in DEMS was driven by the DEMS limestone mine. No significant exposure-response relationship existed after removal of the limestone mine workers from DEMS. They also explored the importance of temporal factors in determining the risk of lung cancer mortality and opined that the modifying impact of temporal factors and effect modification by age should be addressed in any quantitative risk assessment of diesel exhaust exposure.

The EMA team also conducted a reanalysis of the DEMS case-control data to evaluate its suitability for quantitative risk assessment, adjusting for radon exposure and including alternative estimates of diesel engine exhaust exposure.9 Without adjusting for radon, their results were similar to those in the original DEMS analysis, but when exposure to radon was adjusted, the reanalysis team found that the evidence for an effect from exposure to diesel exhaust was greatly diminished. In addition, no consistent evidence of an effect from exposure to diesel exhaust was found for miners who worked only underground.

DEMS, therefore, remains an important study, but it is no longer the final scientific word on the effects of diesel exhaust exposure in surface and underground miners. Agencies have, nevertheless, been inspired to action by DEMS, as described below.

Regulation of Diesel After DEMS: What's On the Horizon for Mining?

DEMS likely will be used by agencies to conduct revised health risk assessments and to justify more onerous regulation of diesel exhaust. The DEMS-inspired developments that loom large on the horizon for the mining industry are summarized below.

IARC Reclassification. DEMS had an almost immediate impact when the International Agency for Research on Cancer (IARC), which is part of the World Health Organization, revised its classification of diesel engine exhaust in the summer of 2012 from *probably carcinogenic to humans* to *carcinogenic to humans*.[10] Based largely on the DEMS results, IARC determined that there was sufficient evidence that exposure to diesel exhaust is associated with an increased risk for lung cancer. The New York Times also reported that experts had identified diesel fumes as more carcinogenic than secondhand cigarette smoke.[11]

IARC's reclassification of diesel exhaust is significant because IARC has historically had enormous influence on cancer research and standard-setting.

MSHA/OSHA Hazard Alert. Also in 2012, MSHA and the Occupational Safety and Health Administration (OSHA) issued a diesel exhaust hazard alert informing workers that "[p]rolonged DE/DPM exposure can increase the risk of cardiovascular, cardiopulmonary and respiratory disease and lung cancer."[12] In that alert, the agencies highlighted IARC's diesel classification.

NIOSH. In 2014, NIOSH announced at a Health Effects Institute (HEI) workshop on "Diesel Exhaust, Lung Cancer and Quantitative Risk Assessment" that it will use DEMS as a basis for a new quantitative risk assessment of health effects of diesel exhaust. The starting date for that project is uncertain.

MSHA Request for Information. In response to two informal "petitions for rulemaking" received from the United Mine Workers of America and a group of public health academics, and in light of IARC's reclassification and the DEMS results, MSHA announced in its Fall 2014 regulatory agenda that it would publish a request for information (RFI) on "approaches that would improve control of DPM and diesel exhaust."[13] The RFI was projected to be published in April, but that did not occur. Instead, the Spring 2015 regulatory agenda has advanced the date to December 2015.[14]

> Diesel exhaust exposure for miners promises to be a continued focus for scientists and regulatory agencies alike.

Experience teaches that a date like this is a soft projection. MSHA rulemaking action, therefore, will almost certainly be time-bound by the lame duck Obama Administration. Even if this RFI were published in December, insufficient time will likely exist in the presidential election year of 2016 even to propose new rules, let alone promulgate them in final form. But depending on which party wins the next election, the RFI could eventually lead to new MSHA diesel rules. Unlike the current DPM rules (which apply to underground miners only), any new rulemaking also could extend to both underground and surface miners, as DEMS studied both types of mine workers. On this important point, it is noteworthy that MSHA already concluded in 2001 that "surface miners are entitled to the same level of protection as other miners; and the Agency's risk assessment indicates that even short-term exposure to concentrations of [diesel particulate matter] like those observed may result in serious health problems."[15]

EPA and HEI. In 2002, the U.S. Environmental Protection Agency (EPA) published its "Health Assessment Document for Diesel Engine Exhaust," which concluded that long-term exposure to diesel exhaust was likely to pose a lung cancer hazard as well as other types of damage to the lungs depending on exposure.[16] EPA may choose to revise that assessment based on forthcoming recommendations on whether DEMS will support a quantitative assessment from HEI, a public-private partnership between EPA and industry.

In 2012, HEI conducted an Advanced Collaborative Emissions Study (ACES) to attempt to distinguish between traditional diesel exhaust and new technology diesel exhaust. ACES found no evidence of gene-damaging effects in the rats and mice studied from exposure to new technology diesel engines and only a few mild effects on the lungs.[17] That study is the only new technology diesel study to date.

HEI has been charged by EPA to review recent epidemiologic studies including DEMS and the reanalysis papers to advise EPA on whether the agency should conduct a revised health assessment for diesel. At its annual conference in May 2015, the HEI Diesel Epidemiology Panel presented its preliminary findings in advance of issuing a formal report later this year.[18] Although HEI's report is not final, it appears that the panel is inclined to deem DEMS an appropriate study to be used in a future quantitative risk assessment. Many stakeholders believe, however, that the HEI panel has not yet given equal consideration to the EMA-commissioned DEMS reanalysis papers in its work.

Because the HEI Diesel Epidemiology Panel's work is ongoing, it is too early to speculate on a final outcome, which we expect before the end of 2015. Whatever the outcome, the Panel's work should be closely watched by the mining industry because it could serve as the driver for a future EPA quantitative risk assessment and as yet another step on the path to increased regulation of diesel use at mines.

Conclusion

In sum, diesel exhaust exposure for miners promises to be a continued focus for scientists and regulatory agencies alike. The next few years may see new MSHA rulemaking in this area, or at least MSHA, NIOSH, and EPA gathering additional information and making quantitative health assessments that could (and likely will) later be used to support downward revised exposure limits for mine workers.

[1] 66 Fed. Reg. 5,526 (Jan. 19, 2001) (DPM rules for underground coal miners); id. at 5,706 (DPM rules for metal and nonmetal mines). The DPM rules are found at 30 C.F.R. §§ 57.5060 through 57.5075. The risk assessment was published at 66 Fed. Reg. 5,752-855, and as corrected at 66 Fed. Reg. 53,518-520.

[2] 66 Fed. Reg. at 5,637-39.

[3] *Kennecott Greens Creek Mining Co. v. MSHA*, 476 F.3d 946 (D.C. Cir. 2007). For more information on the metal/nonmetal mine litigation, *see* L. Joseph Ferrara, *MSHA's Diesel Particulate Matter (DPM) Rulemaking for Metal/Non-Metal Mines: What Have We Learned?*, 24 Energy & Min. L. Inst. ch. 7 (2004), available here.

[4] For links to the study publications and more information on DEMS, *see* National Cancer Institute, Division of Cancer Epidemiology & Genetics, Diesel Exhaust in Miners Study (DEMS), (last visited May 16, 2015).

[5] Publication was delayed by Federal Advisory Committee Act litigation brought by the Methane Awareness Resources Group (MARG).

[6] Peter Morfield, *Diesel exhaust in miners study: how to understand the findings?*, J. of Occupational Medicine and Toxicology 2012, 7:10, available here.

[7] *See*, *e.g.*, Association of Equipment Manufacturers, Advisor Newsletter, *AEM Joins Coalition Seeking Review of 'Diesel Exhaust in Miners Study' Data* (Dec. 5, 2013). EMA was informed that, by data use agreement, the data cannot be linked and had to be viewed in a secure data facility.

[8] *See* Suresh H. Moolgavkar, et al., *Diesel Engine Exhaust and Lung Cancer Mortality: Time-Related Factors in Exposure and Risk*, Risk Analysis, available here.

[9] *See* Kenny S. Crump et al., *Reanalysis of the DEMS Nested Case-Control Study of Lung Cancer and Diesel Exhaust: Suitability for Quantitative Risk Assessment*, Risk Analysis (published online Apr. 10, 2015), available here.

[10] *See* IARC Press Release, *IARC: Diesel Engine Exhaust Carcinogenic* (June 12, 2012).

[11] Donald G. McNeil, Jr., *W.H.O. Declares Diesel Fumes Cause Cancer*, N.Y. Times (June 12, 2012), available here.

[12] OSHA/MSHA Hazard Alert, Diesel Exhaust/Diesel Particulate Matter at 1, available here.

[13] *See* Office of Information and Regulatory Affairs, Office of Management and Budget, DOL/MSHA RIN 1219-AB86, available here.

[14] *See* Office of Information and Regulatory Affairs, Office of Management and Budget, DOL/MSHA RIN 1219-AB86, available here.

[15] 66 Fed. Reg. at 5,531, 5,708.

[16] EPA, Health Assessment Document for Diesel Engine Exhaust (May 2002), available here.

[17] See Jacob D. McDonald et al. (Part 1), Jeffrey C. Bemis et al. (Part 2), Lance M. Hallberg et al. (Part 3) and Daniel J Conklin and Maiying Kong (Part 4), Advanced Collaborative Emissions Study (ACES) Subchronic Exposure Results: Biologic Responses in Rats and Mice and Assessment of Genotoxicity, available for download here; see also Press Release, Study Finds Few Health Effects From New Technology Diesel Engines (Apr. 12, 2012).

[18] See HEI Diesel Epidemiology Project (Sept. 2012); Katherine Walker, Health Effects Institute, Draft Report of the HEI Diesel Epidemiology Panel (Part II): Diesel Epidemiology and Lung Cancer. Those slides are drafts and we point to them only to demonstrate HEI's ongoing work on diesel.

* * *

Managing Cyber Security: What the Mining Industry Should Know and Do



By Evan D. Wolff, Maida Oringher Lerner, Preetha Chakrabarti

Mining companies, like most owners and operators of the nation's critical infrastructure, are becoming increasingly vulnerable to cyber-attacks as they streamline operations by automating more equipment and running facilities and assets from hundreds of miles away with the aid of sophisticated technology. Necessary reliance on industrial automation and control systems to monitor and control physical processes and proprietary data and other sensitive information and networks puts companies at risk. As recent incidents demonstrate, threat actors, including nation states and so-called political "hactivists," are becoming increasingly sophisticated. What's more, disgruntled or careless employees or business partners are better able to disrupt a company's systems and networks. Rising concerns about these evolving risks and threats have prompted the Executive Branch and various government entities to consider legislation, develop voluntary standards, encourage cyber information sharing, and issue guidance on cybersecurity best practices and mitigation tools. These standards and guidance, including cybersecurity guidance issued by the Securities and Exchange Commission's Division of Corporation Finance in 2011, often trigger disclosure obligations and may result in litigation.

This article describes some of the evolving cyber risks and threats the mining industry faces from an array of threat actors and discusses mitigation opportunities a company may consider.

Emerging Cybersecurity Risks and Threats

Reliance on enterprise networks increases vulnerability to cyber attacks

To further efficiency and cost-effectiveness, many mine operators, like other critical infrastructure owners and operators, have centralized the gathering, analysis, and dissemination of critical information, including financial and other proprietary information. Financial transactions are typically conducted over the internet and core proprietary information is stored in centralized networks. This centralized information management has given sophisticated threat actors, including those from overseas, increasingly easier access to sensitive information to facilitate cyber-attacks. In an April 2015 Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," President Obama called these developments "a national emergency" and allowed the Treasury Department to freeze assets and bar other financial transactions of entities engaged in cyber-attacks that pose "a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."

Political and anti-mining activists opposing the mining industry also now have a new tool in their arsenal. Aggressive activists have turned to hacking as they attempt to disrupt mining companies' activities, expose confidential information, and create, at minimum, complicated public relations fiascos, possibly motivated by a desire to shame or embarrass, if not outright disrupt the operations of, such companies. According to a report by Ernst & Young last year, more than 40 percent of metals and mining companies surveyed had experienced a rise in external threats over the previous 12 months. Further, as recent highly publicized attacks—on institutions ranging from retail chains to the U.S. government—demonstrate, insider threats pose an increasing problem as tech-savvy disgruntled employees gain greater access to a company's internal IT systems, giving them easier access to sensitive information.

Reliance on automated networks, such as ICS and SCADA, increases vulnerability to cyber attacks

The mining industry is not new to automated networks such as SCADA (supervisory control and data acquisition) and ICS (industrial control systems). Like the internet, these aging systems were developed to help companies operate efficiently, but not necessarily securely. In fact, the industry's reliance on systems that are often commercially available, combined with the push to greater efficiency and cost-saving measures, has left the systems more exposed. As the overlap between operational and information technologies continues to grow, operational systems—typically older and lacking in sophisticated security—become more vulnerable to cyber-attacks.

Government agencies are increasingly recognizing cybersecurity as a significant issue

The federal government and many government entities are taking note of the increasing frequency and severity of cybersecurity threats to the nation's assets and resources—often in the hands of private ownership—and are developing frameworks and proposals encouraging and providing opportunities for the private sector to address such concerns. In 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," directing the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practice—for reducing cyber risks to critical infrastructure. Released in 2014, the framework provides "guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk." Recognizing the potential for the framework to inform regulatory programs and to establish a standard of care for industry, some critical infrastructure owners and operators are using the Framework or similar constructs to review their cybersecurity posture and to benchmark performance.

Earlier this year, the White House issued an Executive Order, "Promoting Private Sector Cybersecurity Information Sharing," to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government. According to the Obama Administration, this Executive Order "lays out a framework for expanded information sharing designed to help companies work together, and work with the federal government, to quickly identify and protect against cyber threats." Congress is also considering legislation that attempts to address concerns that U.S. companies currently face liability risks, such as shareholder or customer lawsuits, when they choose to voluntarily disclose cybersecurity-related information.

Steps to Consider in Managing Cybersecurity Risks and Threats

Facing evolving threats and obligations, the mining sector needs to manage cybersecurity risk efficiently and effectively. Comprehensive and coordinated risk assessments and compliance reviews led by security personnel and legal counsel whose efforts can help direct compliance efforts and preserve privilege and confidentiality for confidential business and proprietary information and data are good tools to manage risks. These efforts can help inform the development of legally compliant cybersecurity policies and procedures, operations, and incident response plans (including restoration, mitigation, and contingency plans) and testing and exercise regimes.

Identify and classify data and systems, develop cybersecurity policies and procedures, and establish governance structure

A cybersecurity risk assessment and compliance review typically begins with identifying and classifying the company's sensitive and regulated data and systems and reviewing and updating cybersecurity policies and procedures to protect that information. The NIST cybersecurity framework may provide a useful tool for developing a risk-based approach. A company should then consider establishing a governance structure for responsibility and oversight for those policies and procedures and implementation of protective controls.

Develop incident response plan, data breach tool kit, and vendor management agreement

With this groundwork, a company should be better equipped to prepare for a cybersecurity event. Typically successful preparation activities will include development of an incident response plan and a data breach tool kit. It is also important to develop and implement vendor management agreements to help reduce the risk of vulnerabilities through third-party IT systems.

Perform testing and training

Engaging a third-party network consultant to perform a privileged security assessment should also strengthen a company's readiness to defend against a cyber-attack. Training personnel and third-party vendors who likely have access to sensitive information and systems is also critical in ensuring the cyber resiliency of organizations.

Cybersecurity threats have the potential to exploit the increased complextity and connectivity of critical infastructure systems, placing a mining company at risk.

Participate in information sharing opportunities

Increasingly, companies in the private sector recognize that their ability to combine data from many companies, and with the government, enhances their cyber defenses. Industries that share cyber-threat information can aggregate data from a larger pool of resources providing opportunities to spot and counter trends.

Recognizing that information sharing between industry peers and with the government is essential in preventing cyber-attacks, the government is providing increasing opportunities to serve as a clearing house for critical infrastructure owners to receive and disperse information and is considering enacting legislation to define legal protections (such as from exposure to antitrust liability) covering information sharing.

Summary

Cybersecurity threats have the potential to exploit the increased complexity and connectivity of critical infrastructure systems, placing a mining company at risk. A cyber-attack can drive up costs and have significant reputational, safety, economic, and security impacts for a company. The pace and complexity of the threats are growing, making it increasingly incumbent on mining companies to consider adoption of flexible, dynamic, and practical approaches to cybersecurity to protect critical business information and control systems.

* * *

Contact Us

Editor

Daniel W. Wolff
Partner
dwolff@crowell.com
Washington, D.C.
202.624.2621

Authors

Christopher Calsyn
Counsel
ccalsyn@crowell.com
Washington, D.C.
202.624.2602

Evan D. Wolff
Partner
ewolff@crowell.com
Washington, D.C.
202.624.2615

Thomas P. Gies
Partner
tgies@crowell.com
Washington, D.C.
202.624.2690

Maida Oringher Lerner
Senior Counsel
mlerner@crowell.com
Washington, D.C.
202.624.2596

Edward M. Green
Senior Counsel
egreen@crowell.com
Washington, D.C.
202.624.2595

Pretha Chakrabarti
Associate
pchakrabarti@crowell.com
New York, N.Y.
212.895.4327

Sherrie A. Armstrong
Associate
sarmstrong@crowell.com
Washington, D.C.
202.624.2522

Locations

Washington, D.C.
1001 Pennsylvania, Ave.
Washington, D.C. 20004
202.624.2500

New York
590 Madison Ave., 20th Floor
New York, NY 10022
212.223.4000

Los Angeles
515 South Flower St., 40th Floor
Los Angeles, CA
213.622.4750

San Francisco
275 Battery St., 23rd Floor
San Francisco, CA 94111
415.986.2800

Orange County
3 Park Plaza, 20th Floor
Irvine, CA 92614
949.263.8400

Anchorage
1029 W. 3rd Ave. Suite #402
Anchorage, AK 99501
907.865.2600

London
11 Pilgrim St.
London, EC4V 6RN
United Kingdom
+44.207.413.0011

Brussels
7 Rue Joseph Stevens
Brussels, B-1000
Belgium
+32.2.282.4082

Riyadh
Olaya St., Al-Rusis Trade Center
9th Floor, Office No. 901
Riyadh 11323
Saudi Arabia
+966.1.460.3098