CLIENT ALERT

Managing Cybersecurity: What the Mining Industry Should Know and Do

Summer 2015

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 "hacktivists," 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 practices—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.

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.

Other Articles in This Issue:

- Confidentiality in Crisis: the Government Agency Assault on Company Confidentiality Policies and Agreements
- Diesel After DEMS: Regulatory Developments on the Horizon for Mining

---

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

Preetha Chakrabarti
Counsel – New York
Phone: +1 212.895.4327
Email: pchakrabarti@crowell.com