CYBERSECURITY THREATS TO THE CANADIAN MINING INDUSTRY: IS YOUR BUSINESS READY?

Posted on January 10, 2023

Categories: Insights, Publications

Cybersecurity attacks on critical infrastructure are on the rise especially considering the significant potential negative consequences such attacks can cause to both a country's domestic and the global economy. One of the most notorious cybersecurity threats organizations currently face is ransomware, which is a type of malicious software that threatens to publish a victim's data assets or block access to a victim's key networks or related infrastructure unless a material sum of money is paid. In the first half of 2021, global ransomware attacks increased by a staggering 151%. Ransomware incidents can devastate organizations by disrupting their critical operations to the extent that they are reliant on network and system connectivity.

In Canada, the mining industry has long been a key contributor and supporter with respect to critical infrastructure through the production of raw materials used to create necessary equipment and goods. As a result, the risk of cybersecurity attacks on businesses operating in the mining industry is high. The threat to businesses operating in the mining industry is often exacerbated due to their high degree of dependence on technology in their business operations, their need for consistent and reliable communication with remote locations, and the fact that not only are the minerals being extracted valuable in their own right, but they are often key minerals in the production of key technologies globally. There have been several recent high profile ransomware attacks, including the widely publicized attacks on Nvidia, Kaseya and Colonial Pipeline. Then, on December 27, 2022, Copper Mountain Mining was the target of a ransomware attack which resulted in a shutdown of the southern British Columbia mine for nearly a week, and an immediate 5.5% drop in their share price.

Impact of Cybersecurity Attacks

Ransomware attacks often force a complete shutdown of a business' operations, making such attacks one of the most disruptive forms of cybercrime for mining organizations. The shutdown of key operating, safety and processing systems can cause significant economic damage to the mining business which, when coupled with the fact that such attacks can also damage, destroy or result in the release of sensitive data (including personal information), the consequences are severe for a business hit by a ransomware attack. In addition to those immediate impacts, ransomware attacks can have long-lasting consequences on the business including a loss

of trust, negative public perception, greater branding risks, and investor trepidation.

At a high level, cybersecurity incidents such as ransomware attacks can result in serious financial, regulatory and operational challenges for a business, including:

1. The compromise of key informational assets, including confidential information, personal information, trade secrets and key intellectual property;
2. Operational disruptions caused by being locked out of essential information systems;
3. Regulatory scrutiny, including complaints and investigations;
4. Potential civil liability; and
5. Demands for extortion payments by threat actors.

Because these impacts are so severe on an organization, many businesses who are subject to a ransomware attack are willing to pay the ransom to get back up and running as quickly as possible. However, paying the ransom does not necessarily prevent these consequences. A recent survey of Canadian businesses found that only 42% of organizations who paid a ransom had their data completely restored. In light of these risks, mining organizations require robust cybersecurity protections and processes as well as a strong privacy compliance programs to mitigate the risk of any cybersecurity incidents.

Cybersecurity Incident Response

Mining firms should be proactive in developing plans and processes to both protect against, and to clearly outline the steps to be taken in response to, a cyberattack. While it is not possible to eliminate the risk of a cybersecurity attack, organizations can minimize their exposure and the impact such attacks might have on them by prioritizing incident response planning. For example, every organization should, at a minimum:

1. Define the key members of their incident response team and how and when they will communicate in the event of a crisis;
2. Take inventory of the sensitive and proprietary data on the organization's systems (or that can sit with third party service providers) and the associated legal obligations that can apply if such data is compromised;
3. Ensure that critical policies and procedures are in place that will help to limit exposure in the event of a crisis (such as an appropriate document retention and destruction policy); and
4. Consider the feasibility of putting in place cyber-risk insurance coverage.

Incident response to a cybersecurity attack should focus on both the immediate and long-term protection of your organization. The appropriate features of an incident response plan will vary based on the unique needs and circumstances of each organization. Responses may focus on:

1. Providing timely and effective incident response services in connection with cybersecurity incidents, including ransomware attacks, employee snooping, misdirected emails and other incidents;
2. Recommending and implementing a reporting and notice strategy to comply with legal obligations and reduce litigation risk; and
3. Crafting internal statements, public responses and FAQs to reduce litigation risk and reputation concerns.

Conclusion

As ransomware attacks evolve and grow more sophisticated with the development of new technology, attacks will continue to be an omnipresent threat for all businesses, especially those operating in the mining industry. McMillan is available to assist mining firms in developing strategies to prevent and prepare for cybersecurity incidents, and provide support for incident response.

by Robert Piasentin, Mitch Koczerginski, Kristen Shaw and Gemma Walsh (Articled Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.