purves redmond limited

WHITEPAPER

How does the IIOT affect your business?

The Industrial Internet of Things (IIOT) has allowed businesses to excel with smart monitoring and asset tracking, providing insight into employee safety and environmental sustainability. These pieces of hardware rely heavily on the internet to function, and while the benefits of the IIOT are ever-growing, it also raises a new set of cyber risks for businesses.

IIOT and Mining

The mining industry is especially vulnerable to the downfalls of the IIOT, whilst also being one industry that can fully utilize its potential. IIOT has improved health and safety, physical security of assets, and environmental sustainability using sensors and smart monitoring.

This form of technology is growing within the mining industry and has room to establish more benefits as time passes, however the disadvantages appear to be troubling. One of the common concerns of the IIOT in the mining industry is connectivity issues. Cyber-attacks and potential connection issues can interrupt production and, depending on their severity, impact company profits. Mining corporations that are affiliated with governments and are integrated with global supply chains should take extra precautions as attacks may be more frequent and sophisticated.

> *"[I]f a hacker is able to control the mine remotely, it puts safety, security and all the mine's information at risk. Furthermore, hackers can install malware and demand ransoms in order to restore functions. That makes the urgency to resolve the situation and the possible damage accomplished by the attack even more significant."*
>
> ***— Abhay Raman, EY Cyber Risk Services Leader***

POTENTIAL USES FOR THE IIOT:

- Sensors to monitor dam levels
- Geo sensors to spray water to avoid dust clouds
- Sensors to detect if workers are injured by machinery
- Wearable sensors to warn staff to evacuate unsafe areas

Cyber Insurance

Cyber insurance is not the only risk management solution to combat cyber security risk, although it can help with the recovery after a cyber attack has taken place. A combined approach of layering cyber insurance (risk transfer) with cyber security, helps improve overall resiliency. When focusing on the risk transfer component, cyber insurance policies require thorough review and insightful customization to each business as there is currently no standardized policy language. Part of the challenge is due to the evolution of cyber attacks both in terms of their frequency and sophistication; many find it difficult to keep up with the changes required to stay current.

CYBER INSURANCE PROTECTS INSUREDS FROM CLAIMS ALLEGING:

- Breach of privacy rights
- Spreading of computer viruses, malware, ransomware and defamation
- Violation of obscenity laws
- Infringement or misappropriation of intellectual property

The way the cyber peril has integrated itself in all aspects of business operations seems to have happened quicker than traditional insurance policies were able to evolve. This makes it more important now than ever before to dissect your traditional property and casualty insurance program to identify where there may be exposures and gaps in coverage to property and equipment that is connected to the network.

How PRL Can Help

The complexity of cyber insurance policies make insurance brokers a necessary part of the risk management equation. Brokers can assist in explaining the way multiple policies can work collaboratively in order to address any coverage disparities in the overall insurance program. As your risk management partners, brokers can further help organizations customize the policy language to align with your business' specific business risks and exposures.

CONTACT OUR CYBER LEADER FOR EXPERT GUIDANCE:

Sean Gibson, JD
Cyber & Transactional Risks Practice Leader
sgibson@purvesredmond.com
Direct: 647.695.3386