Cyber risk: Mining’s safety blind side

https://www.bsigroup.com/en-ZA/industries-and-sectors/mining-and-materials/Cyber-Security-in-Mining/

To future-proof mining operations, South Africa’s mining and minerals sector is increasingly starting to use or planning to use Artificial Intelligence (AI), Robotic Process Automation (RPA) and Industrial Internet of Things (IIoT) systems. The COVID-19 pandemic is further accelerating the move to smarter mining and the subsequent application of other Fourth Industrial Revolution (4IR) technologies.

With this convergence in the IT and operational technology (OT) space mining operations are becoming more and more vulnerable to cyber attacks – and the consequences can be catastrophic, such as the shutdown of critical infrastructure or even loss of life.

For mines facing the cyber challenge head-on, collaborating with the right partner – one that fully grasps the future of mining and has knowledge and wisdom distilled from years of experience – has become an absolute necessity.

Global pioneer in standardisation, the British Standards Institution (BSI) sits at the forefront in developing comprehensive solutions to combat cyber risk, to minimise disruption when there is an attack, and to ensure business continuity. BSI also believes that the most effective cybersecurity countermeasures are those that target the entire mining operation – from its advanced technologies to its workforce and the processes and policies they follow.

For mines the cyber battlefront will only get bigger

Traditional mining processes were dependent on relatively closed operational systems and technologies mostly developed separately from IT. But mining sectors across the globe have evolved, and rapidly so. Many operations today realise that tech-smart mining is the only way to secure a sustainable future.

COVID-19 is of course fast-tracking this process of adopting new-frontier technologies across the entire pit-to-port chain. Prior to the pandemic mines were fairly content within their isolated perimeters where they had reasonable control of information security. Much of this changed in 2020 as mines sought greater application of 4IR technologies to manage operations more effectively and to adjust to an ever-changing new-normal.

In fact, and according to the World Economic Forum’s latest Future of Jobs Report, globally 79% of mining companies are accelerating the digitalization of their operational processes – with many viewing the COVID crisis as an opportunity to innovate.

The greater the move to digital, the higher the risk

Digital transformation in mining creates a hyperconnected infrastructure network that links every aspect of an operation. It’s also this über-connectivity that leads to a highly-mutable cyber risk environment. While South African mining’s cyber battlefront has been lagging in digging its defence trenches, hopefully this will change without further delay.

Simply put, the more dependent and entrenched mines become with digital technology the more vulnerable they become to the risk of attack by random cyber criminals, activists, competitors or national enemies.

Cyberattacks against mining

Essentially, the mining industry is under threat from cyber attacks aimed at exploiting its strategic position in global supply chains. Some of the prevalent threats include:

Cyber espionage: Mining companies wield pots of gold of data. While the prime target for data theft in mining is information about a mine's pricing (which gives competitors an edge when negotiating a highjacked sales deal), cyber criminals are also after a mine's exploration research, classified corporate strategy documents, process information, and even info about a mine's processing technology, to name a few. As a geopolitical and economic target, data stolen through cyber espionage can have disastrous effects on operations, finances, and a mine's market credibility.

Insider threats: Insider threats come in many forms, whether it's fraud, intellectual property theft, cyber system sabotage, or even a disgruntled former employee seeking revenge. For one, rogue elements within a mining operation can sabotage data for on-selling to third parties. A big concern with these insider attacks is the time lapse between a breach and detection of that breach. It may even take years for such an attack to be discovered, particularly if it's a breach of unauthorised access.

Hacktivism: Mines are increasingly becoming targets of syndicates wanting to manipulate social change. They mostly target mines in protest of the effects of mining on the environment and wildlife habitats. Ultimately, hacktivists aim to provoke and challenge those in power who threaten their moral stance, and they have the cyber-means to do so.

Imagine the devastating consequences if a cyber syndicate targets your mining operation and takes control of automated drilling, blasting or a self-driving truck – lives *will* be at stake.

BSI – securing your journey toward integrated cyber resilience with ISO/IEC 27001 and ISO 22301

It is high time for South Africa and Africa's mining sectors to take the necessary steps to safeguard their operations, workforces, and precious data.

As the UK's official standards body and as a member of the International Organization for Standardization (ISO), BSI has quickly adapted to mining innovations resulting from this COVID age and the acceleration of 4IR technologies.

BSI further understands that the only way for mines to achieve cyber resilience is through a holistic approach that covers all aspects of an operation. For security programmes and systems to achieve optimal efficiency, there simply needs to be an integrated, all-encompassing cybersecurity culture – one in which cyber disruption is quickly minimised and business continuity is expedited.

ISO/IEC 27001 – the international standard for information security management

ISO/IEC 27001 represents the first big step for mining companies to implement, maintain and grow an independently assessed and certified Information Security Management System (ISMS). With this system your operation will be demonstrating commitment and compliance to global best practice, proving to your workforce, suppliers, subcontractors and all other stakeholders that security is primary in the way you operate.

Some of the benefits of ISO/IEC 27001 for mining operations include:

- Requires you to continually detect and evaluate information security risks and breaches and to ensure the procedures you activate are sufficient to manage or eliminate them
- Helps you identify all internal and external stakeholders relevant to your ISMS
- Helps establish an operational environment in which there's a continuous improvement of your ISMS
- Ensures information is always protected, available, and can be accessed
- Reduces the likelihood of insider threats to security breaches
- Shows commitment to information security at all levels of the business, in the process entrenching a cybersecurity culture
- Requires you to communicate the ISMS policy throughout management and workforce hierarchies, thereby ensuring that all employees understand how they contribute

- Creates an environment in which top management define ISMS roles and ensure individuals are competent
- It has the flexibility to adapt controls to all or selected areas of your operation
- Will help you gain internal and external trust that data is protected, which in turn will strengthen your reputation and help cultivate stakeholder confidence

Once your ISMS has been assessed by BSI as fulfilling the requirements of ISO/IEC 27001 you can then show your commitment to excellence by displaying the prestigious BSI Assurance Mark across your operation.

You will now also be ready to take the next vital step toward achieving holistic cybersecurity, and with ISO 22301.

ISO 22301 – the leading international standard for Business Continuity Management Systems (BCMS)

The ISO/IEC 27001 and ISO 22301 frameworks complement each other in your journey toward cyber resilience. With ISO/IEC 27001 you've laid a foundation to combat cyber risk, whilst with ISO 22301 you're further refining your business continuity management system (BCMS) and minimising the impact of disruptive incidents – whether it's a cyber breach, COVID-19, a natural disaster, or unplanned IT and telecom outages, the list is endless.

To date, COVID-19 has not had such a devastating effect on South Africa's mining sector, as most operations have gone ahead with business as usual and even during hard lockdowns. Yet, there's still little consensus on how this pandemic will impact mining in the future.

Mining companies simply must remain on guard, and keep cultivating and integrating the best standards to protect against disruption and to ensure business continuity and optimisation, especially in light of the increased adoption of emerging technologies and the risks they pose.

The ISO 22301 framework will ensure continuous stability in your mining operation and allow you to move forward during a time of crisis. Some of its benefits include:

- Help your operation build confidence in its ability to continue functioning throughout a disruption
- Disruptions come at a price that can cripple any business – this framework will help reduce the cost implications of any disruption
- With full BCMS framework integration your operation's strategic objectives will have a stronger anchor which will enable greater future resilience
- Through providing clarity on BCM strategy implementation in all levels of your operation you're further strengthening that culture of resilience
- A company's reputation can suffer severe effects if a crisis is mishandled due to an ineffective management system. With structural integration of the ISO 22301 framework your reputation is protected.

As a joint force of management systems, ISO 22301 and ISO/IEC 27001 will embed continual improvement and systems robustness starting at the heart of your mining operation and throughout its workforce, processes, policies and technologies.

BSI is primed and ready to become your partner in achieving operational excellence

Nobody knows what the future holds for South African mining, not in this age of uncertainty. Will COVID-19's evolving impact start affecting our mining industry more severely? Will the acceleration of 4Ir technologies cause the type of cyber catastrophes that can bring operations to a standstill or endanger lives? Instead of continuing to rely on traditional methodologies because thus far they've worked relatively well, we need to keep rethinking and refining our approaches and systems that drive operational excellence and help us safeguard against disaster.

ENDS

BSI enables people and organizations to perform better. We share knowledge, innovation and best practice standards to make excellence a habit – across the globe, every day. To develop and promote standards that reflect good business practice, annually we publish over 3100 standards – all *underpinned by a collaborative approach that engages with industry experts, government bodies, trade associations, businesses of all sizes and consumers.*

For more info visit https://www.bsigroup.com/en-ZA/. Contact the South African office on (0)12 004 0279 or email bsi.za@bsigroup.com