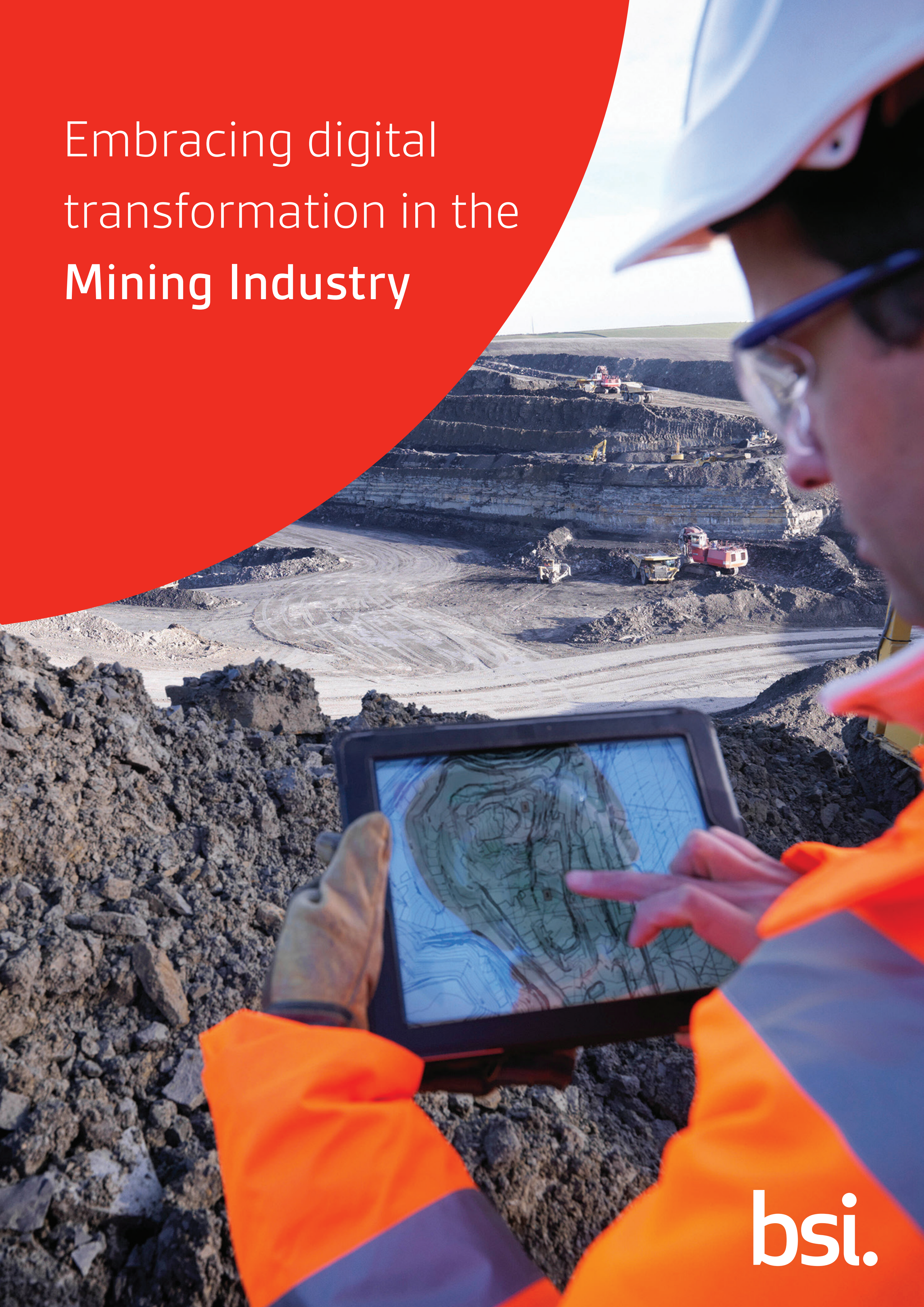
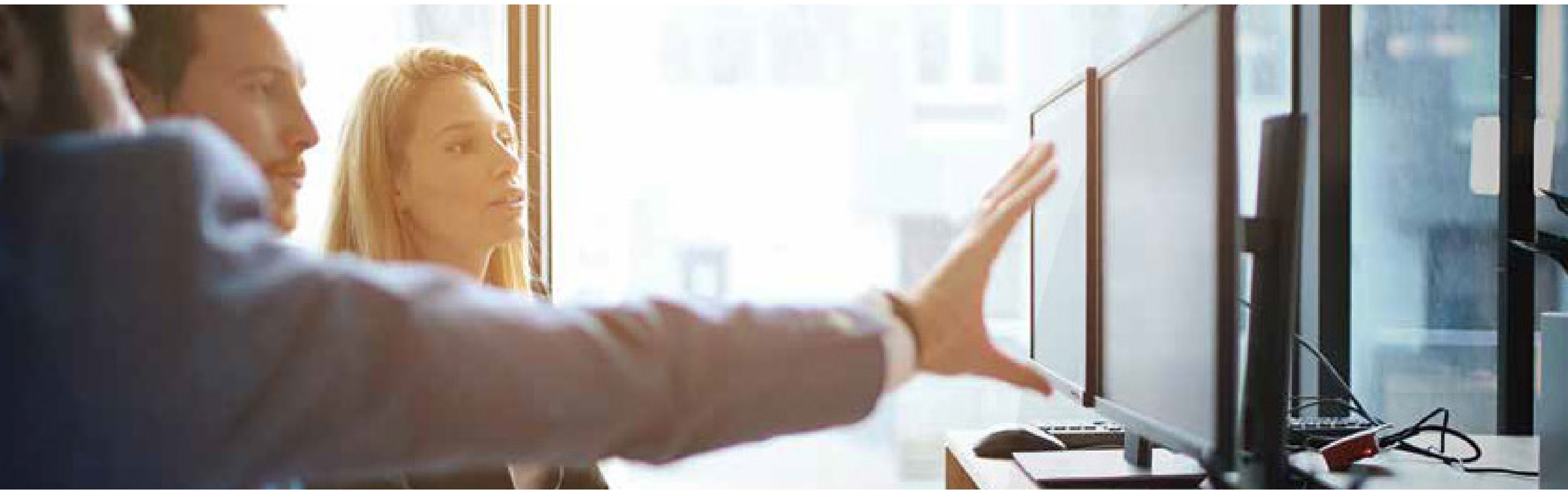
Embracing digital transformation in the **Mining Industry**



bsi.

Achieving a state of Information Resilience

To future-proof mining operations, South Africa and Africa's mining and minerals sectors are increasingly using Artificial Intelligence (AI), Robotic Process Automation (RPA) and Industrial Internet of Things (IIoT) systems. The COVID-19 pandemic is known to have accelerated the move by organizations to integrate digital technologies and the increased application of other Fourth Industrial Revolution (4IR) technologies. With this convergence in the IT and operational technology (OT) space, mining operations could also potentially create greater opportunities for accelerating the use of innovative digital solutions. However, this could also mean they may be more vulnerable to cyber-attacks, which can result in shutdowns of critical infrastructure or, in the most extreme cases, loss of life. In fact, according to Ernst and Young (EY), 54 percent of mining companies have experienced a significant cyber incident in the past 12 months.*



A changing cyber risk landscape – the cyber battlefront will only get bigger

Many mining processes were often dependent on the use of relatively closed operational systems and technologies which were developed separately from IT. But mining sectors across the globe have evolved, and today it is believed that many operations see technology-driven mining as a way to secure a sustainable future.

The post pandemic environment presents mining operations an opportunity to fast-track the process of adopting new-frontier technologies across the entire pit-to-port chain. Prior to the pandemic mines may have felt they had reasonable control of their information security. But, as mines seek to accelerate the application of 4IR technologies to manage operations more effectively, they may equally need to prepare for increased cyber risk in their next-normal. In fact, and according to the World Economic Forum's latest Future of Jobs Report[1], globally 79% of mining companies are accelerating the digitalization of their operational processes – with many viewing the COVID-19 pandemic as an opportunity to innovate.

The greater the move to digital, the higher the risk

Digital transformation in mining would create a hyperconnected infrastructure network that links every aspect of an operation. It is believed that this extensive connectivity could also lead to a highly-mutable cyber risk environment.   And it is the realization of this risk that is starting to drive a change in attitude to cyber security in SA mining.

So far local mining operations have not experienced many major breaches[2], but with more operations likely to embrace emerging technologies, becoming digitally robust and secure could be one of the sectors biggest future challenges. Simply put, the more mines become dependent on digital technology, the more vulnerable they could become to the risk of targeting by random cyber criminals, activists, competitors or national enemies.

For mines facing the cyber challenges head-on, collaborating with the right partner – one that fully grasps the future of mining and has knowledge and insight gained from years of experience – would have unquestionable benefits. And that's where BSI can help.

Cyber risk - Mining's safety blind side

Essentially, the mining industry is under threat from cyber-attacks aimed at exploiting its strategic position in global supply chains[3]. Some of the prevalent threats to have front of mind include:

Cyber espionage:

Mining companies wield valuable pots of data. While the prime target for data theft in mining is information about a mine's cost structure (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 information about a mine's processing technology, to name a few[4]. As a geopolitical and economic target, data stolen through cyber espionage can have a severe and lasting impact 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 could sabotage data for on-selling to third parties[5]. A big concern with insider attacks is the time lapse between a breach and detection of that breach. It could be years before an attack is discovered, particularly if it's a breach of unauthorised access.

Hacktivism:

Mines are increasingly becoming targets of syndicates wanting to manipulate social change[6]. They mostly target mines in protest of the effects of mining on the environment and wildlife habitats.

Imagine the consequences if a cyber syndicate targeted your mining operation and took control of automated drilling, blasting or a self-driving truck.

Securing your journey towards cyber resilience with ISO/IEC 27001

BSI helps organizations embed internationally recognized best practices to enables organizations to realize their opportunities by safely adopting new technologies.

As the mining sector accelerates its use of 4IR technologies, BSI recognizes that to achieve cyber resilience a holistic approach that covers all aspects of an operation could be critical.

For security programmes and systems to achieve optimal efficiency, there is a need for an integrated, all-encompassing information security culture – one in which cyber disruption is quickly discovered, the impact minimized, and business continuity maintained.

ISO/IEC 27001 – the international standard for Information Security Management Systems (ISMS)

ISO/IEC 27001 is an internationally recognized framework for managing information security and could represent an ideal first step for mining companies. This standard helps organizations implement, maintain and grow an independently assessed and certified Information Security Management System.

With an ISMS your mining operation would demonstrate commitment and compliance to global best practice, proving to your workforce, suppliers, subcontractors and all other stakeholders that security is a primary consideration in the way you operate.

How ISO/IEC 27001 can help mining operations build resilience:

- Requires you to continually detect and evaluate information security risks and breaches and to ensure the procedures and controls you activate are sufficient to manage or minimize 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, whilst helping to embed an information security culture
- Requires you to communicate the ISMS policy throughout your organization, which will help you raise awareness and gain buy-in
- Creates an environment in which top management define ISMS roles and ensure individuals are competent
- Provides flexibility to adapt relevant controls across your operation
- Helps inspire trust that data is protected, which in turn will strengthen your reputation and help cultivate stakeholder confidence

Having your ISMS assessed by BSI, and successfully fulfilling the requirements of ISO/IEC 27001, provides you the opportunity to show your commitment to excellence by displaying the prestigious BSI Mark of Trust across your operation.

Benefits BSI Clients get from ISO/IEC 27001 certification:

- We have reduced our operational risk 88%
- We have improved our internal business confidence 86%
- We have improved customer satisfaction 85%

Reference: Voice of the customer survey 2020

Your ISO/IEC 27001 Journey

Whether you're new to information security management or looking to enhance your current system, we have the right resources and training courses to help you understand and implement ISO/IEC 27001. We can help make sure your system keeps on delivering the best for your business.

	You need to:	We help you:
Understand and prepare	• Buy the standard and read it; understand the content, your requirements and how it will improve your business • Contact us; we can propose a solution tailored to your organization's needs	• Discover information on our website, including case studies, whitepapers and webinars visit bsigroup.com/en-ZA • BSI ISO/IEC 27001:2013 Requirements training
See how ready you are	• Ensure your organization understands the principles of ISO/IEC 27001 and the roles individuals will need to play. Review your activities and processes against the standard	• Download self-assessment checklist • BSI ISO 27001:2013 Implementation training course • Schedule a BSI gap assessment to see where you are • BSI Business Improvement Software can support ISO/IEC 27001 implementation
Review and get certified	• Contact us to schedule your certification assessment • We will then carry out system and document assessments (a 2 stage process). The length of this may depend of the size of your organization	• BSI ISO/IEC 27001:2013 Internal and Lead Auditor training • BSI Business Improvement Software helps ISO/IEC 27001 implementation • Your BSI certification assessment

BSI is primed and ready to become your trusted partner

Nobody can know for sure what the future holds for South African mining operations. Will COVID-19's evolving impact start affecting our mining industry more severely? Will the accelerated introduction of 4IR technologies bring operations to a standstill or endanger lives?

What's important is that we need to continually rethink and redefine our approach and the systems that underpin sustainable organizational resilience to help safeguard against disaster.

As a global pioneer in standardization based on recognized best practice, the British Standards Institution (BSI) sits at the forefront in developing comprehensive solutions to combat cyber risk, to minimize disruption when there is an attack, and to help ensure business continuity.

BSI believes that the most effective cybersecurity countermeasures are those that benefit the entire mining operation – from its advanced technologies to its workforce and the processes and policies they follow.

Get in touch with us today to discuss your plans and how we can support you on your journey towards operational excellence.

Bibliography/References

1 Future jobs report
2. Mining and cyber breaches https://www2.deloitte.com/za/en/pages/energy-and-resources/articles/approach-to-combat-cyber-risk-mining.html
3. https://www.mining-technology.com/features/covid-19-majorly-disrupted-mining-supply-chains-was-it-a-taste-of-things-to-come/ https:/documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf
https://www.trendmicro.com/vinfo/es/security/news/cyber-attacks/cyber-threats-to-the-mining-industry
4. https://bedrockautomation.com/ot-cyber-security-issues-for-the-mining-industry/
https://miningglobal.com/automation-and-ai/how-digital-transformation-impacts-mining-cybersecurity
https://www.mdpi.com/1424-8220/20/24/7210/htm
https://www.trendmicro.fi/vinfo/us/security/news/cyber-attacks/cyber-threats-to-the-mining-industry
https://www.itweb.co.za/content/KwbrpOqgNjNMDLZn
https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Managing-Cybersecurity-What-the-Mining-Industry-Should-Know-and-Do
https://www.itp.net/608462-corporate-espionage-key-reason-for-cyber-attacks-in-mining-sector-report
https://www.mining-technology.com/features/mining-companies-need-wake-cyber-threat/
https://portswigger.net/daily-swig/mining-technology-company-gyrodata-hit-by-ransomware-attack-employee-data-leaked
5. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/energy-resources/za_Future_of_mining.pdf
6. https://www.pwc.co.za/en/assets/pdf/2017-sa-mine.pdf
7. * https://allafrica.com/stories/201906200243.html

bsi.

✉ bsi.za@bsigroup.com
🌐 bsigroup.com/en-ZA
☎ +27 (0) 12 004 0279