

Deloitte.



Tracking the trends 2022

Redefining mining

Deloitte's Global Energy, Resources & Industrials specialists provide comprehensive, integrated solutions to all segments of the Oil, Gas & Chemicals, Power & Utilities, Mining & Metals, and Industrial Products & Construction sectors by offering clients deep industry knowledge and a global network.

Introduction

Redefining mining

What will successful mining and metals companies look like in a low-carbon, low-waste, purpose-driven future?

The beauty of this question is that there is no definitive answer. While the core objective of the mining industry remains unchanged going forward: to extract and provide metals and minerals to downstream sectors, many of the factors that have influenced how mining companies should look, feel, and act in the past, have shifted in recent years.

The way in which companies fulfil this mission is now open to interpretation. And today, there is a rare opportunity for leaders to reorganize, generate new value, and forge partnerships to create a more responsible and attractive future for the industry.

While some early movers saw the need for change coming 10, 15, even 20 years ago and have been redefining their organizations and operations accordingly, for many firms, the necessity for fundamental change only really hit home in 2020-21. The convergence of factors including the ongoing effects of the COVID-19 pandemic on the world of work, continued drive towards digitization, the growing need to integrate ESG commitments with central business functions, and the need to pivot in response to fast-moving business and operating environments, has opened many choices for companies.

Of course, the biggest underlying driver and opportunity for transformation lies in the green energy transition. The 2021 United Nations Climate Change Conference (COP26) held in Glasgow in November, highlighted the mining industry's integral role in supplying the metals and materials critical for a low-carbon future¹. The way in which mining companies position themselves today in preparation for this change, will determine their sustainability, and could make or break their competitive advantage over the next decade.

Change on this scale is undoubtedly daunting, which is why in this, its 14th year, Tracking the trends has focused on effecting transformation. The following 10 trends provide a toolkit to help mining companies start thinking through, and moving towards, their vision of future success.

In them, our global team of experts share insights and case studies designed to get ideas flowing. We explore how to evolve traditional mining and metals businesses through new business models, capital allocation, agile work practices, and data-driven technologies to create organizations fit for the 21st century; ones that can not only survive but profit from whatever the future might throw at them and leave a positive social impact in their wake.

The next decade will be one of the most exciting and transformative in the mining industry's history. We look forward to discussing the trends with you and supporting your company on its journey. Thank you for your ongoing support.

Endnote:

1. Judith Magyar, "COP26 Takeaways: Renewables Replace Fossil Fuels As Metals Become A Major Force", published 28 November 2021 <https://www.forbes.com/sites/sap/2021/11/29/cop26-takeaways-renewables-replace-fossil-fuels-as-metals-become-a-major-force/?sh=948a2f626763>, accessed 3 December 2021.



Trend 9

Closing the IT-OT vulnerability gap

The next frontier in cybersecurity

René Waslo, Global Risk Advisory Leader, Energy, Resources & Industrials, Deloitte US
Andrew Kwong, Partner, Risk Advisory, Deloitte Canada

Over the past five years, the acceleration of digitization, information technology (IT) and operational technology (OT) convergence and value-chain integration in the mining sector has produced new levels of efficiency, driven down miners' costs, and created exciting new business opportunities.

However, with opportunity also comes risk and, for many companies, rather than security efforts keeping pace with their digital growth, the gap between risks and controls has widened.

According to computer-security firm McAfee, the cost of cybercrime globally now tops US\$1 trillion, with monetary losses accounting for US\$954 billion.¹ Higher metal prices and the strategic importance of certain metals have brought the mining sector to the attention of criminals in recent years, and a number of firms (both metal producers and METS companies) have found themselves victims of security breaches.

For example, Norwegian aluminum and renewable energy company Norsk Hydro faced a ransomware attack in 2019 that affected more than 35,000 employees across 40 countries. The financial impact was estimated at US\$71 million.² More recently, Weir Group PLC was the victim of a ransomware incident in September 2021.³ This led to disruptions in the company's engineering, manufacturing, and shipping operations which resulted in revenue deferrals and overhead under-recoveries.

Vulnerability through IT-OT convergence

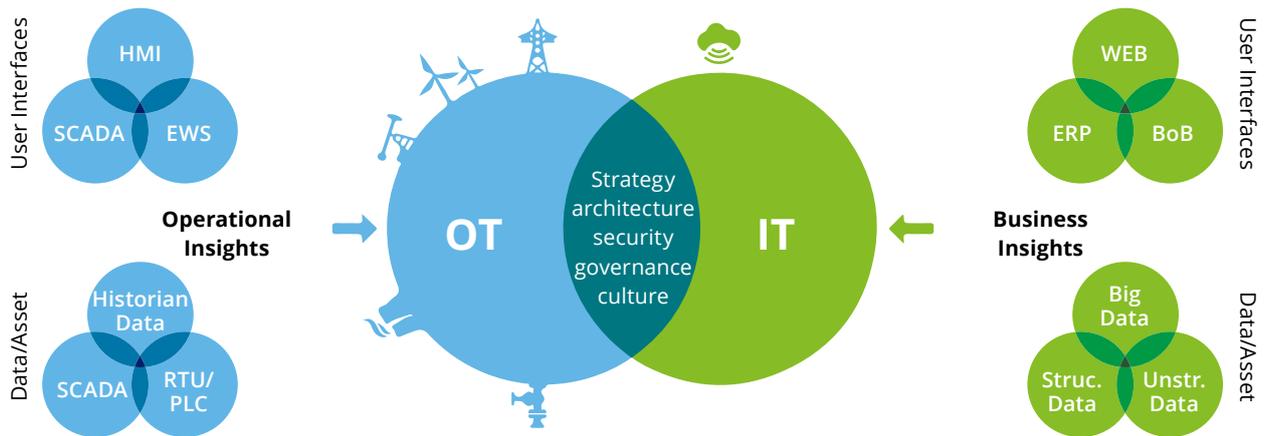
Traditionally, mining companies have placed heightened security focus on protecting data and systems in functions like finance or human resources, but not enough on the ground at mine sites. However, IT-OT convergence is increasing, and more devices are being connected than ever before, sometimes without the proper due diligence for security. The result is that, today, some of the industry's biggest cyber vulnerabilities are around OT, industrial control systems (ICS), and Industrial Internet of Things (IIOT).

René Waslo—Global Risk Advisory & Cyber Leader, Energy, Resources and Industrials, Deloitte US, explains, "While companies have begun to place more emphasis on the operations side of their businesses, we still see opportunities for improvement in the OT environment. Until there is equal focus on the front and back office, we'll continue to see breaches."

Future bites

Advanced digital technologies such as blockchain and artificial intelligence are already a reality. However, as future technologies, such as quantum computing for industrial applications emerge, it's important to consider the potential security issues that data management on this scale could entail in advance of implementation. Out of 600 respondents to Deloitte's 2021 Future of Cyber Survey, 64% ranked security capabilities as the top consideration in their decision to implement emerging technologies.⁴

Figure 1: IT-OT environments in mining are becoming increasingly connected



Source: Deloitte analysis

- HMI: Human Machine Interface
- SCADA: Supervisory Control and Data Acquisition
- EWS: Engineering Work Station
- RTU/PLC: Remote Terminal Unit/ Programmable Logic Controller
- ERP: Enterprise resource planning

Historically, OT systems were designed to be isolated, running less-known industrial protocols and custom software. Those systems had limited exposure to cyber-related threats whereas, today, as an enabler of business innovation and efficiency, OT environments are becoming increasingly connected to other networks and are remotely accessible to allow remote process monitoring, system maintenance, process control, and production data analysis/integration (see figure 1).

The adoption of remote and hybrid operating models as ‘the new normal’ means that now is a good time to review cybersecurity measures around interconnected or segmented networks, and ensure they are robust enough to sustain current practices and support future business growth.

Other key challenges include the high cost associated with ICS upgrades, patching, or changing configuration files on legacy systems, and a lack of redundancy in production schedules as supply chains move to more integrated or just-in-time models.

Restoring trust in the value chain

Twenty years ago, cybersecurity in mining was a technology implementation issue; as solutions were scaled up, security measures were added. While there’s still an element of

association today, the ubiquity of digital technologies and work practices means that businesses now need to factor security threats and solutions into every decision they make. As value-chain integration accelerates, there are touchpoints where miners need to ensure that third-, fourth- or fifth-party organizations with whom they are doing business have a strong cyber posture.

There is also a reputational element to consider. In the future, a mining company’s security stance could affect its ability to engage or trade with other organizations.

Andrew Kwong, Partner, Risk Advisory, Deloitte Canada explains: “When it comes to new technologies and systems, businesses are making strategic choices on how their organizations change, and those changes could have a big impact on security. Today, it’s important to put a cybersecurity lens over every business decision or technology implementation, and make sure that secure processes are in place to support these organizational changes.”

Of course, mining companies are just at the beginning of their digital journeys, so it’s worth putting the time, attention, and investment in now to ensure operations are not left exposed in the future.

Securing the mining OT environment

- **Knowledge is power:** Create and maintain a holistic inventory of all connected devices at the shop-floor level. Review this regularly to ensure OT cybersecurity measures are sufficient and properly allocated.
- **Uncover asset vulnerabilities:** Perform a passive detection of the network by collecting and analyzing traffic circulating between OT devices. This will allow vulnerabilities in the discovered assets to be uncovered.
- **Perform regular OT security assessments:** Assessments allow the identification of security gaps and missing controls, and can help leaders to gauge the maturity level of their organization's approach to OT cybersecurity. Based on this, recommendations can be made on work lots to achieve target maturity and strategic deployment roadmaps built to support this effort.
- **OT third-party risk assessment:** Conduct a workshop with critical third-party stakeholders, such as original equipment manufacturers or service providers, to discuss the controls in place to secure the interface between their systems and the mine's. Ensure these are robust and up to date.
- **Create an OT governance framework:** Establish a corporate-wide security objective for OT by defining the OT cybersecurity strategy. Also, create a functional IT/OT governance working model.
- **Consider an IT-compromise assessment:** It's also worth assessing the current IT environment, infrastructure, and selected systems to identify previously undetected backdoors, compromises, or exposures that reveal data and system integrity to significant risks.
- **Perform a thorough market review:** The traditional OT security market is niche and mature. However, OT/IT convergence is accelerating, and a growing number of cyber-physical systems are emerging in operational and mission-centric environments, creating a new security market with shifting dynamics. It's worth scanning the market on a regular basis to ensure access to the latest security systems and services.

Endnotes:

1. Zhanna Malekos Smith, Eugenia Lostri and James Lewis, "The hidden costs of cybercrime," McAfee, published December 2020 <https://www.mcafee.com/blogs/other-blogs/executive-perspectives/the-hidden-costs-of-cybercrime-on-government/>, accessed 9 October 2021.
2. Bill Briggs, "Hackers hit Norsk Hydro with ransomware. The company responded with transparency," Microsoft, published 16 December 2019 <https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>, accessed 14 November 2021.
3. "Q3 trading update and cybersecurity incident," Weir, published 7 October 2021 www.global.weir/newsroom/news-articles/q3-trading-update-and-cybersecurity-incident/, accessed 14 November 2021.
4. "2021 future of cyber survey," Deloitte, published October 2021 <https://www2.deloitte.com/global/en/pages/risk/articles/future-of-cyber.html/#>, accessed 29 October 2021.

Global contacts

Rajeev Chopra

Global Leader—Energy, Resources & Industrials

Deloitte Touche Tohmatsu Limited

+44 20 7007 2933

r Chopra@deloitte.co.uk

Andrew Swart

Global Sector Leader—Global Mining & Metals

Deloitte Touche Tohmatsu Limited

+1 416 813 2335

aswart@deloitte.ca

Regional/Country Mining & Metals Leaders

Africa

Andrew Lane

+27 11 517 4221

alane@deloitte.co.za

Ecuador

Jorge Brito

+59 32 381 5100

jorgebrito@deloitte.com

Argentina

Alejandro Jaceniuk

+54 11 4320 2700 ext. 4923

ajaceniuk@deloitte.com

France

Veronique Laurent

+33 1 5561 6109

vlaurent@deloitte.fr

Australia

Steven Walsh

+61 8 9365 7097

swalsh@deloitte.com.au

Francophone Africa

Damien Jacquart

+33 1 55 61 64 89

djacquart@deloitte.fr

Brazil

Patricia Muricy

+55 21 3981 0490

pmuricy@deloitte.com

India

Rakesh Surana

+91 22 6122 8160

rvsurana@deloitte.com

Canada

Andrew Swart

+1 416 813 2335

aswart@deloitte.ca

Indonesia

Ali Henry

+62 21 2992 3100

ahery@deloitte.com

Chile

Dominic Collins

+5 622 729 8089

dcollins@deloitte.com

Japan

Yuichi Shibata

+81 80 9087 4406

yuishibata@tohatsu.co.jp

China

Kevin Bin Xu

+86 10 8520 7147

kxu@deloitte.com.cn

Mexico

Valeria Vazquez

+52.55.50807548; ext 548

vavazquez@deloittemx.com

Colombia

Andres Roa

+57 1 426 2008

andresroa@deloitte.com

Peru

Karla Velásquez

+51 1 211 8559

kvelasquez@deloitte.com

Poland

Zbig Majtyka

+48 32 508 0333

zmajtyka@deloittece.com

Russia – CIS

Andrei Shvetsov

+74957870600; ext 5188

ashvetsov@deloitte.ru

Southeast Asia

Jiak See Ng

+65 93 877 958

jsng@deloitte.com

Switzerland

Geoff Pinnock

+41 58 279 6066

gmpinnock@deloitte.ch

Turkey

Elif Dusmez Tek

+90 312 295 47 00

etek@deloitte.com

United Arab Emirates

Bart Cornelissen

+971 4 376 8888

bpcornelissen@deloitte.com

United Kingdom

Roman Webber

+44 20 7007 1806

rwebber@deloitte.co.uk

United States

Amy Chronis

+1 713 982 4315

achronis@deloitte.com

Authors

Trend 1: Aligning capital allocation to ESG

Andrew Swart | Global Mining & Metals Leader, Deloitte Touche Tohmatsu Limited | aswart@deloitte.ca

Andrew Lane | Energy, Resources & Industrials Leader, Deloitte Africa | alane@deloitte.co.za

Trend 2: Reshaping traditional value chains

Andrew Lane | Energy, Resources & Industrials Leader, Deloitte Africa | alane@deloitte.co.za

John O'Brien | Partner, Financial advisory, Deloitte Australia | johnobrien@deloitte.com.au

Trend 3: Operating in the new super-cycle

Roman Webber | Mining & Metals Leader, Deloitte North South Europe: UK | rwebber@deloitte.co.uk

Valeria Vazquez | Mining & Metals Leader, Deloitte Mexico | vavazquez@deloittemx.com

Trend 4: Embedding ESG into organizations

Henry Stoch | Sustainability Leader, Deloitte Canada | hstoch@deloitte.ca

Harsha Desai | Associate Director, Consulting, Deloitte Africa | hardesai@deloitte.co.za

Trend 5: Evolving mining's world of work

Janine Nel | Partner, Consulting, Deloitte Canada | jnel@deloitte.ca

Marcello Cordova Alvestegui | Director, Consulting, Deloitte Chile | macordova@DELOITTE.com

Trend 6: Establishing a new paradigm for Indigenous relations

Professor Deen Sanders OAM | Lead Partner, Integrity, Deloitte Australia | deensanders@deloitte.com.au

Joe Hedger | Partner, Indigenous Services Group, Deloitte Australia | jhedger@deloitte.com.au

Jason Rasevych | Partner, National Indigenous Services Leader, Deloitte Canada | jrasevych@deloitte.ca

Trend 7: Continuing the journey toward innovation-led organizations

Steven Walsh | Mining & Metals Leader, Deloitte Australia | swalsh@deloitte.com.au

Roland Labuhn | Partner, Consulting, Deloitte Canada | rlabuhn@deloitte.ca

Trend 8: Unlocking value through integrated operations

Eamonn Treacy | Director, Consulting, Deloitte Canada | etreacy@deloitte.ca

Dominic Collins | Energy, Resources & Industrials Leader, Deloitte Chile | dcollins@deloitte.com

Trend 9: Closing the IT-OT vulnerability gap

René Waslo | Global Risk Advisory Leader, Energy, Resources & Industrials, Deloitte US | rwaslo@deloitte.com

Andrew Kwong | Partner, Risk Advisory, Deloitte Canada | akwong@deloitte.ca

Trend 10: Preparing operations for climate change

John O'Brien | Partner, Financial Advisory, Deloitte Australia | johnobrien@deloitte.com.au

Patricia Muricy | Mining & Metals Leader, Deloitte Brazil | pmuricy@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s more than 345,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.