Cyber hacking and information security: mining and metals

EY
Building a better working world

Cyber hacking and information security: mining and metals

Cyber hacking and the breach of information systems security is an emerging threat to mining and metals companies, tipped as one of the top risks in the sector. It can be vicious, well organized and undertaken by highly skilled operators. With 41% of the mining and metals respondents to EY's Global Information Security Survey reporting an increase in external threats,[1] cyber incidences are on the rise. Investing in the prevention of such an attack may be less costly than the downtime, loss of intellectual property and time spent fighting such an attack.

It was once thought that hackers were rebellious young students who would target symbols of authority as a protest and a reflection of their technological prowess. Consumer and financial organizations were thought to be at most risk. However, the list of cyber adversaries has grown to include criminals, national governments and hacktivists, and their target list has likewise grown. With the relative importance the mining and metals sector plays in the global, regional and local supply chains, it has now become a priority target.

Criminals are attracted to the sector because of the massive cash flows on investment. They understand the increasing dependence mining and metals has on technology and are actively looking for ways to threaten the denial of access to data, processes and equipment. Today's versions of kidnapping, extortion, blackmail and protection rackets are real threats. For example, a criminal could take a long position in copper on the LME and then proceed to use cyber hacking to disrupt supply at key copper production facilities causing prices to spike.

Global Information Security Survey 2013-2014

Participant profile

Sample size – 1,909 respondents from 144 countries, of which 39 are mining and metals

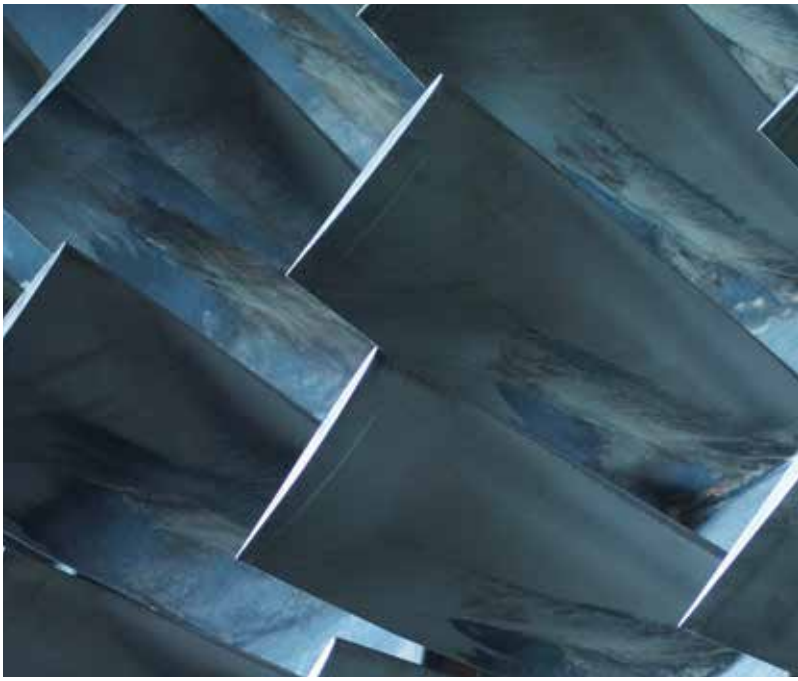
Respondent positions – Predominantly Chief Information Officer, Chief Information Security Officer, Information Security Executive, Information Technology Executive, Internal Audit Director/manager, Chief Security Officer, Network/System Administrator

Centralized functions make easier targets

These threats are heightened by the centralization of many business functions across the supply chain as a result of increasing cost rationalization. This has translated into the need for a more sophisticated IT system and network infrastructure to connect the geographically diverse workforce, which increases an organization's exposure to, and dependency on, the internet. Operations technology (OT) (e.g., PCN, safety systems or sensors) is increasingly connected. With the trend toward remote operation to improve cost efficiency, there is a convergence of IT and OT and this provides cyber hackers with an access path to the operation systems from the internet. Further, OT systems are inherently less secure as many old systems were not designed with security in mind.

Government-led cyber attacks

Intelligence agencies and the military of sovereign states, and their funded unofficial affiliates, have become increasingly active in cyber warfare. Their enormous capabilities are being directed at economic warfare and espionage to target key industries, posing a



1. *Under cyber attack: Global Information Security Survey 2013-2014*, EY.

real threat to mining and metals organizations. The objective may be the passive collection of commercially sensitive intelligence to assist national or state-owned companies in contract negotiations. However, the possibility of it being more sinister, with the use of malware to incapacitate important facilities (made infamous by the Stuxnet attack on the Iranian nuclear facilities), should not be ruled out. It is worthwhile considering the impact of disabling a remote operations center that controls trucks, drills, trains, ship loaders, mills or concentrators, or even the individual physical equipment being disabled.

Advanced persistent threats (APTs) are attacks that are conducted over a long period of time and use attack vectors that could be outside the control of the organization, e.g., attacking vendors' or employees' home systems. These are rumored to be state funded and, hence, have the capability to pull off highly sophisticated, complex and extended attacks. Many of these hacking teams have more resources (knowledge, manpower and time) at their disposal than any of their targets and may involve both human and cyber espionage.

The rise of the informal activists

In trying to maintain their social license to operate, mining and metals companies endeavor to meet as many stakeholder demands as they can. They will invariably not meet all demands, many of which are competing, nor may they choose to. Some more militant and extreme activists with unsatisfied demands can turn to hacking to disrupt mining and metals companies' activities, expose confidential information and create communications mischief, such as defacing websites or triggering false announcements. Hactivists' use of cyber hacking to pursue a political agenda is a real risk in today's operating environment.

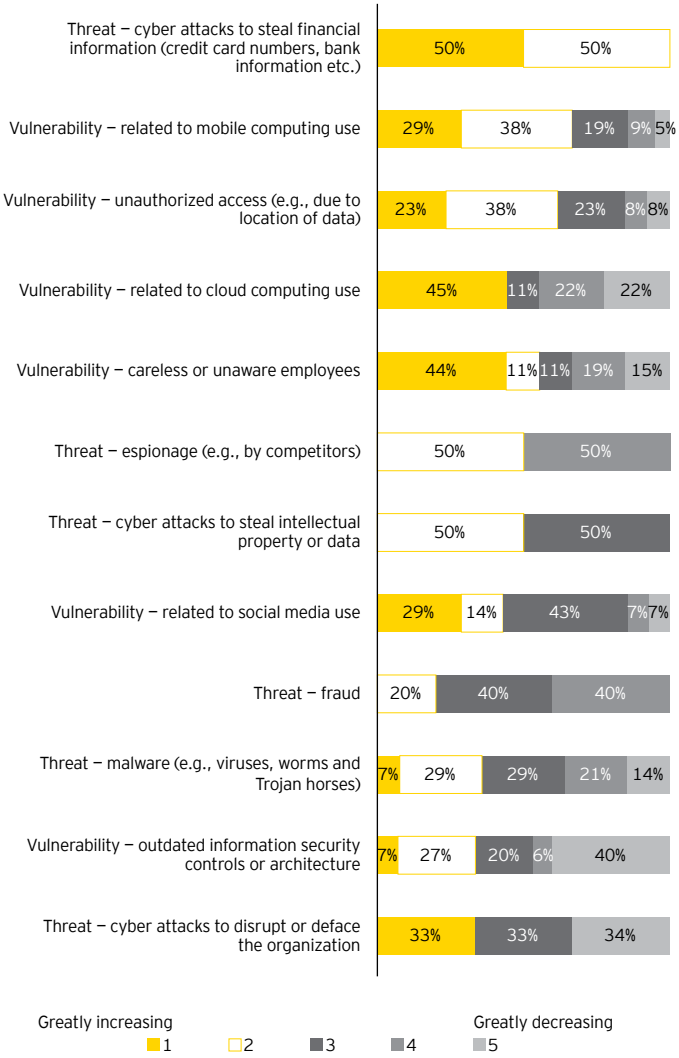
"Mine automation is intended to unlock cost and production efficiencies, but with this upside comes the very real threat of cyber attack, which tests the current level of robustness, integrity and resilience of IT systems."

Clement Soh
Director, Advisory, EY Australia

An increase in threats and vulnerabilities

The threats are real and on the rise. EY's *Global Information Security Survey 2013-2014* found that 41% of the mining and metals respondents experienced an increase in external threats over the past 12 months, with 28% experiencing an increase in internal vulnerabilities over the same period.

Which threats* and vulnerabilities** have most increased yourrisk exposure over the last 12 months



* Threat is defined as a statement to inflict a hostile action from actors in the external environment.

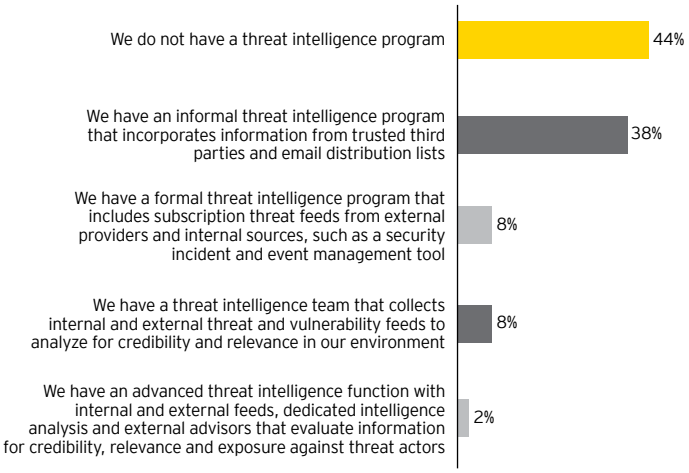
** Vulnerability is defined as the state in which exposure to the possibility of being attacked or harmed exists.

Source: *Global Information Security Survey 2013-2014,* EY, 2013.

Formal security programs not widely deployed

Surprisingly, 44% of the mining and metals survey respondents indicated that their organizations do not have a threat intelligence program in place and 38% have only an informal one in place. This leaves them completely unprepared to identify a cyber hacking or an information security threat. Also, it means that these organizations would not have the benefit of experiencing an early warning or of being prepared for any breaches, potentially increasing the impact. For some mining and metals organizations, the reasons for this are skill shortages, security maturity, headcount reductions or budget constraints, especially amid a volatile economic environment and falling commodity prices. Other organizations lack executive support of information security and may simply be hoping the issue will go away on its own.

The maturity of your threat intelligence program



Source: *Global Information Security Survey 2013-2014,* EY, 2013.

Not just pulp fiction – an example

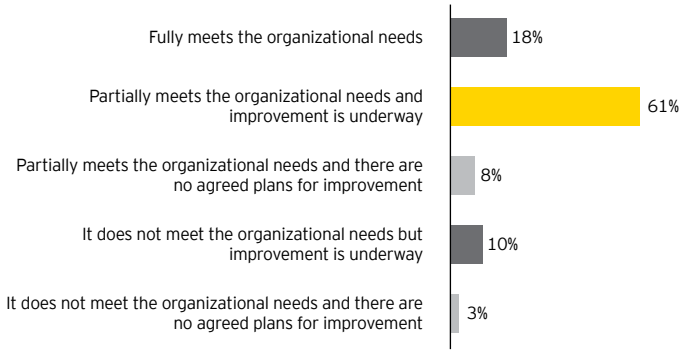
A mining company company uses a SCADA system to control the operations of certain assets involved in the logistics and product chain. After some problems with reliability of the equipment, the company undertook an exercise to compare current source code with an unedited version to check if changes made were impacting reliability.

The mining company found unauthorized changes (unrelated to the reliability issue) had been unintentionally uploaded into the source code from a maintenance contractor's laptop. The changes were designed to disable the auto-shutdown protections of the equipment and thereby allow the destruction of the equipment. A date trigger for this action was embedded in the code.

Addressing the threats head-on

The effectiveness of information security is important, and with only a small percentage of mining and metals respondents (18%) seeing that it fully meets the organization's needs, there is a long way to go in protecting organizations from these threats. However, with the issue becoming critical, time is something that organizations don't have.

The extent to which the information security function is meeting the needs of your organization



Source: *Global Information Security Survey 2013-2014,* EY, 2013.

There is usually not an organization-wide risk management approach to these threats. Often-times, it is viewed as an information systems security issue, and therefore the threat is narrowly defined and not widely embraced. A top-down approach needs to be taken to these threats in order for countermeasures to be effectively taken. This means that the executive level needs to understand and address this issue to get both the budget and buy-in to ensure information and operational security.

As Shawn Henry, a former FBI cyber investigator, recently remarked: "There are two types of companies: those that have been breached, and those that don't know they have been breached."[2] This is true of all risks and, while cyber hacking may not translate into a reality for many organizations, its rising profile and an increasing understanding of the threat it presents suggests it should not be ignored.

Steps to combat cyber hacking and bolster information security

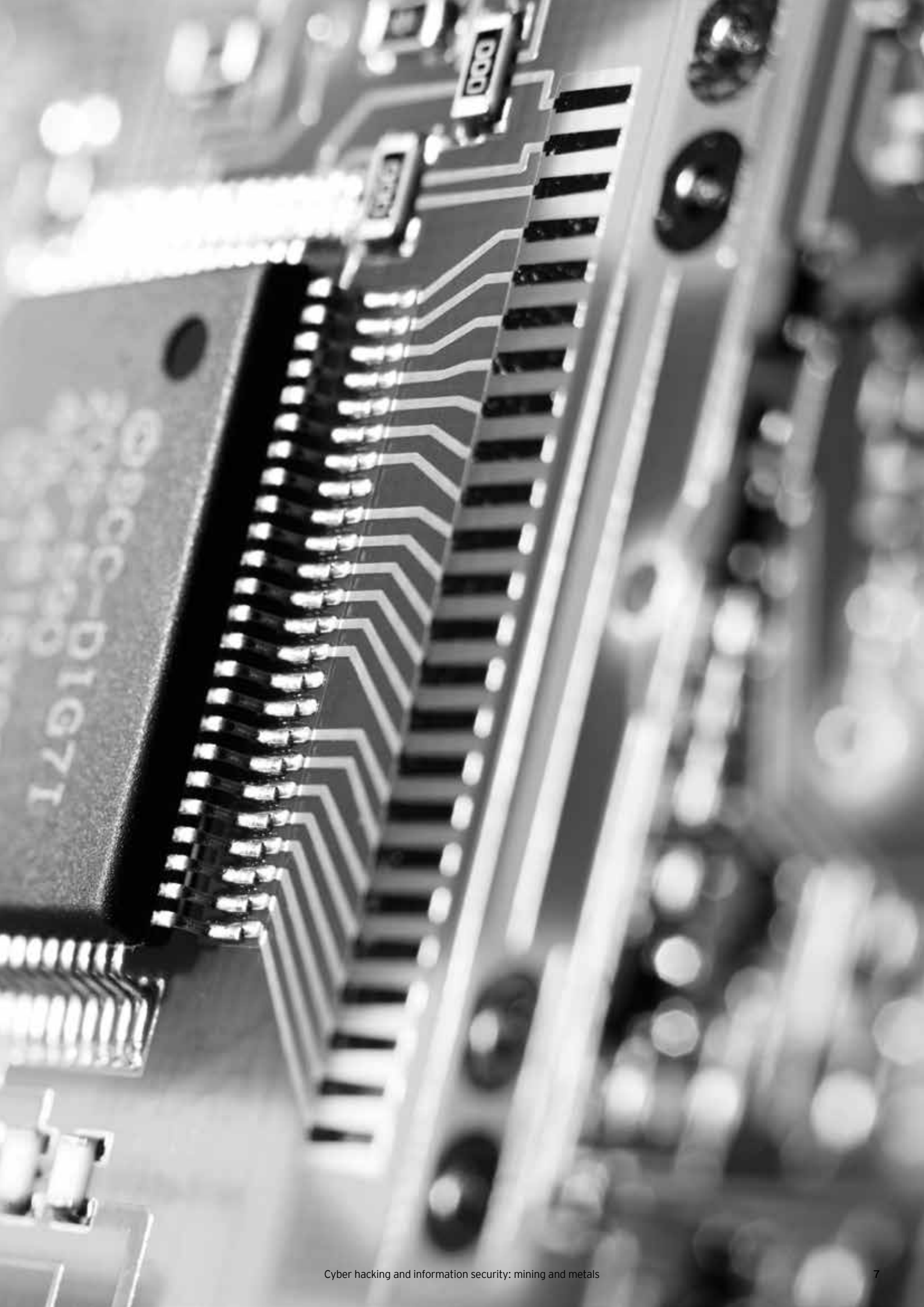
Strategic

- Making information security a board-level and senior management priority
- Developing an integrated strategy around corporate objectives, and considering the whole risk landscape
- Using data analytics to test the risk landscape and better understand the data/systems you need to protect the most
- Identifying the potential interest groups who would benefit from access to your organization's systems and information
- Assessing the current systems and understanding their vulnerabilities and where a breach could likely occur
- Understanding the laws and regulations that help protect your organization from a cyber attack and building a relationship with the agencies that enforce them
- Creating a cyber threat or attack response protocol

Operational

- Using a three- to five-year horizon for budgeting to enable long-term planning
- Creating a working team across the organization that includes senior management, risk advisors and information systems
- Ensuring accessibility to data across all the organization's systems
- Using data analytics to identify potential threats or a pattern of attacks
- Conducting attack and penetration tests more frequently
- Innovate, innovate, innovate

2. "Boards must consider internet's dark side," *ft.com*, 12 December 2012, http://www.ft.com/cms/s/0/764a60ec-4442-11e2-932a-00144feabdc0. html#axzz2V7CvBEB1, accessed 10 May 2013.



Area contacts

Global Mining & Metals Leader
Mike Elliott
Tel: +61 2 9248 4588
michael.elliott@au.ey.com

Oceania
Scott Grimley
Tel: +61 3 9655 2509
scott.grimley@au.ey.com

China and Mongolia
Peter Markey
Tel: +86 21 2228 2616
peter.markey@cn.ey.com

Japan
Andrew Cowell
Tel: +81 3 3503 3435
cowell-ndrw@shinnihon.or.jp

Europe, Middle East, India and Africa Leader
Mick Bardella
Tel: +44 20 795 16486
mbardella@uk.ey.com

Africa
Wickus Botha
Tel: +27 11 772 3386
wickus.botha@za.ey.com

Commonwealth of Independent States
Evgeni Khrustalev
Tel: +7 495 648 9624
evgeni.khrustalev@ru.ey.com

France and Luxemburg
Christian Mion
Tel: +33 1 46 93 65 47
christian.mion@fr.ey.com

India
Anjani Agrawal
Tel: +91 982 061 4141
anjani.agrawal@in.ey.com

United Kingdom & Ireland
Lee Downham
Tel: +44 20 7951 2178
ldownham@uk.ey.com

Americas and United States Leader
Andy Miller
Tel: +1 314 290 1205
andy.miller@ey.com

Canada
Bruce Sprague
Tel: +1 604 891 8415
bruce.f.sprague@ca.ey.com

South America and Brazil Leader
Carlos Assis
Tel: +55 21 3263 7212
carlos.assis@br.ey.com

Service line contacts

Global Advisory Leader
Paul Mitchell
Tel: +86 21 22282300
paul.mitchell@cn.ey.com

Global Assurance Leader
Tom Whelan
Tel: +1 604 891 8381
tom.s.whelan@ca.ey.com

Global IFRS Leader
Tracey Waring
Tel: +613 9288 8638
tracey.waring@uk.ey.com

Global Tax Leader
Andy Miller
Tel: +1 314 290 1205
andy.miller@ey.com

Global Transactions Leader
Lee Downham
Tel: +44 20 7951 2178
ldownham@uk.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Global Mining & Metals Center
With a volatile outlook for mining and metals, the global sector is focused on cost optimization and productivity improvement, while poised for value-based growth opportunities as they arise. The sector also faces the increased challenges of changing expectations in the maintenance of its social license to operate, skills shortages, effectively executing capital projects and meeting government revenue expectations.

EY's Global Mining & Metals Center brings together a worldwide team of professionals to help you succeed – a team with deep technical experience in providing assurance, tax, transactions and advisory services to the mining and metals sector. The Center is where people and ideas come together to help mining and metals companies meet the issues of today and anticipate those of tomorrow. Ultimately it enables us to help you meet your goals and compete more effectively.

© 2013 EYGM Limited.
All Rights Reserved.

EYG no. ER0113
CSG/GSC2013/1172589
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/miningmetals