Does cyber risk only become a priority once you've been attacked?

Mining and metals

The better the question. The better the answer.
The better the world works.

Building a better working world

The frequency and impact of cyber threats are increasing

Cyber threats are growing at an exponential rate globally with more than half of energy and resources participants in EY's latest *Global Information Security Survey* having experienced a significant cybersecurity incident in the last year. These threats are evolving and escalating at an especially alarming rate for asset-intensive industries such as mining and metals.

Today, all mining organizations are digital by default – in an increasingly connected world, the digital landscape is vast, with every asset owned or used by an organization representing another node in the network. Organizations are increasingly reliant on technology, automation and operations data to drive productivity gains, margin improvement and cost containment goals. At the same time, it has never been more difficult for organizations to understand and secure the digital environment in which they operate, or their interactions with it:

- **Every organization's technology landscape is both bespoke and complex:** They span multiple accountable teams for strategic planning, budgeting and support; and encompass multiple networks and infrastructure that may be on-premises, in the cloud or owned and managed by a third party.
- **Defining an "organization" is difficult:** Blurring the security perimeter further, there has been a proliferation of devices belonging to employees, customers and suppliers (including laptops, tablets, smartphones, edge computing solutions, smart sensors and more) with access to the organization's systems.
- **Increased connectivity between Information Technology (IT) and less mature Operational Technology (OT) environments widens the "attack surface":** A cyber incident has the potential to disrupt production or processing, safety and cost efficiency and have a direct impact on business strategies and goals.

Cyber incidents can be malicious or unintentional. They range from business service interruptions, large-scale data breaches of commercial, personal and customer information, to cyber fraud and ransomware (such as WannaCry and NotPetya) and advanced persistence threat campaigns on strategic targets.

1 The frequency of cyber attacks are continuing to increase rapidly around the globe

+

2 Digital innovation has drastically increased the "attack surface" within the mining sector

+

3 Reliance on technology has significantly increased the impacts of a cyber incident

"There is potential for cyber risk to be the downfall of a mining and metals organization's productivity gains and digital advancement aspirations."

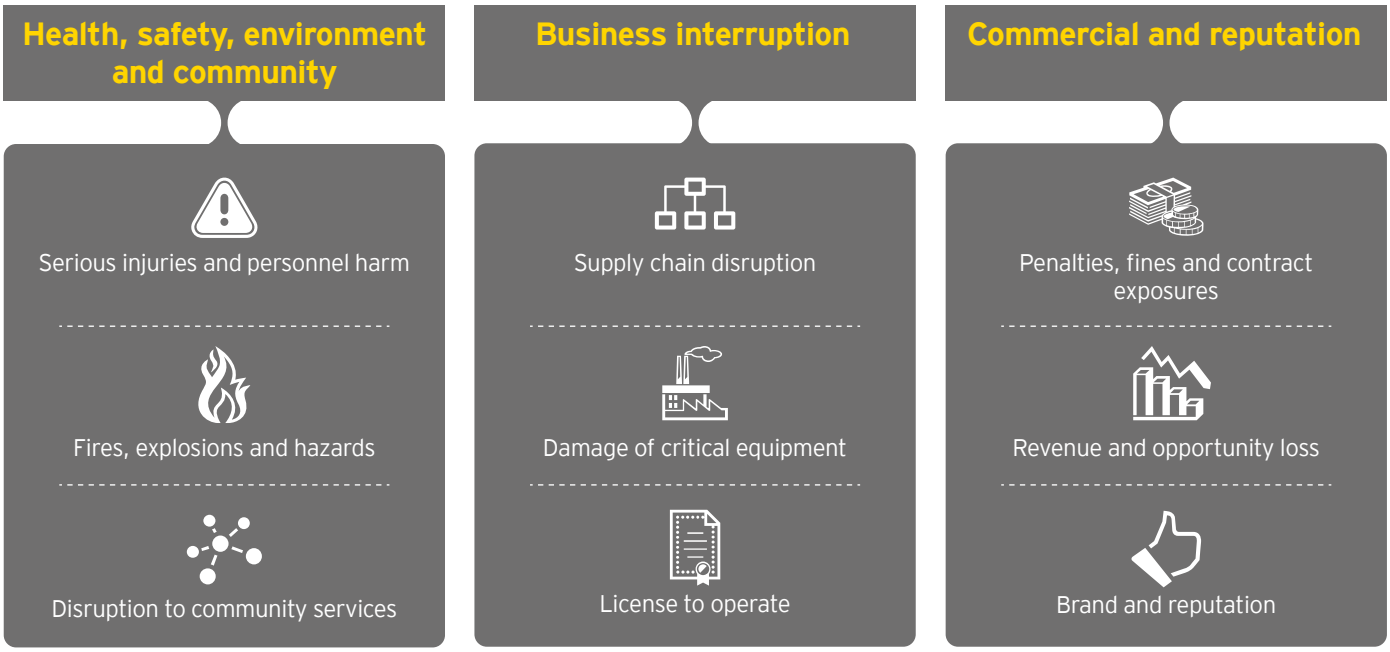
Mike Rundus
EY Global Mining & Metals Cybersecurity Leader

Share on social media

What is the cost of cyber threats?

By 2021, the global cost of cybersecurity breaches is expected to reach US$6 trillion, double the total for 2015.[1] The World Economic Forum now rates a large-scale breach of cybersecurity as one of the five most serious risks facing the world today.[2]

There can be significant consequences, as depicted below, should a cyber attack occur within an operational facility or affect operational assets.



The cyber threat landscape is complex and spans IT and OT

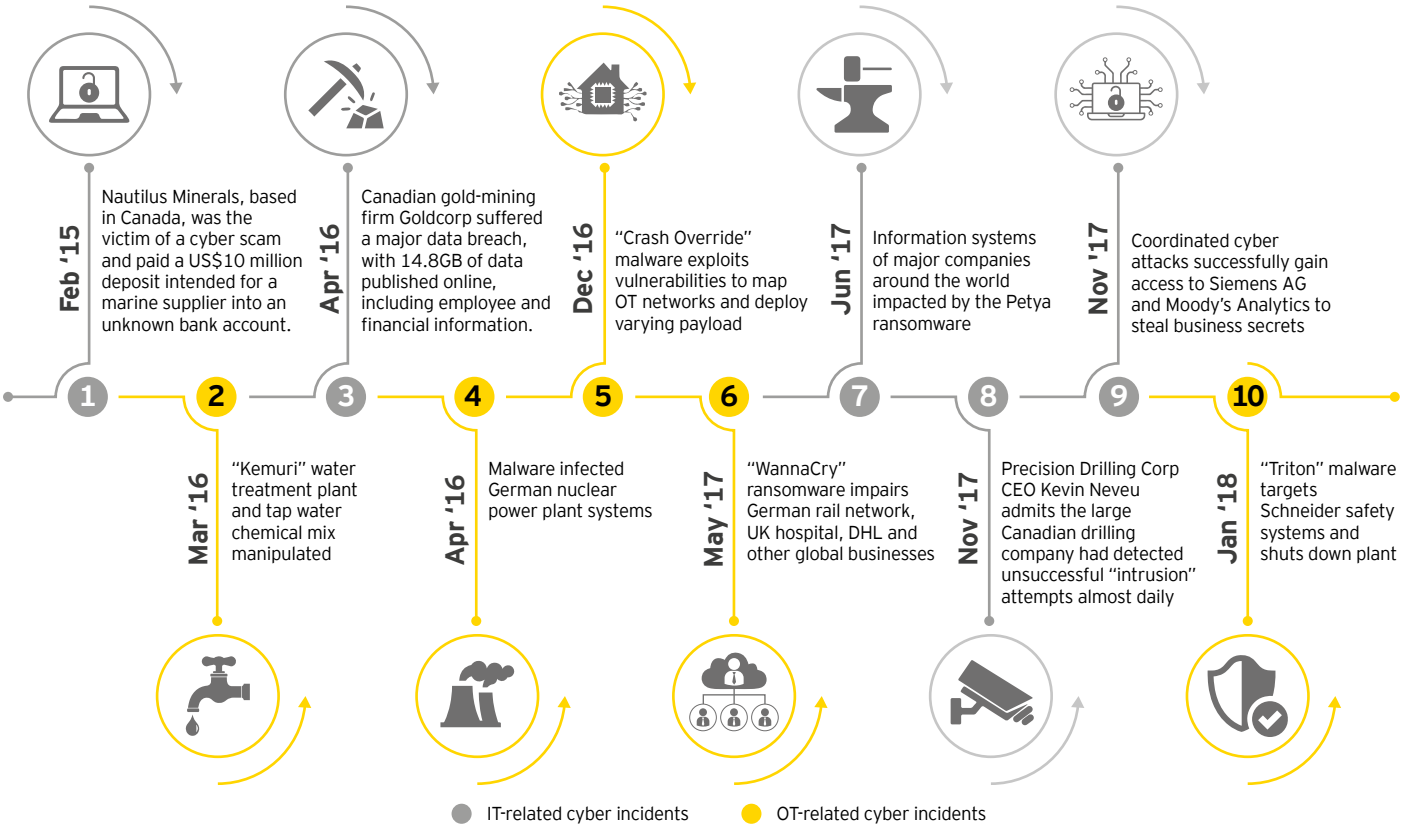
Historically, OT environments were isolated with limited connectivity to external networks beyond the physical site, and utilized vendor-specific protocols and proprietary technologies. This often allowed asset owners to adopt a "security by obscurity" approach. However, this approach is no longer viable within modern OT environments as they are highly connected and increasingly leverage infrastructure, protocols and operating systems that are also common within enterprise IT. As such, vulnerabilities associated with technologies utilized within enterprise IT are often equally applicable for critical OT.

Further threats are also fueled by the prominence of malware that targets OT environments. In December 2015, Ukraine's power grid was crippled by a cyber attack that utilized malware (BlackEnergy and KillDisk) and targeted OT and industrial control systems. Since this time, the malware has become more commoditized and widely available.

[1] "Cybercrime Report 2017 Edition," *Cyber security Ventures*, 19 October 2017.

[2] "Global Risks Report 2017," *World Economic Forum*, 11 January 2017.

The more prominent IT- and OT-related cyber events



Note: Sources in footnote[3,4,5,6,7,8,9]

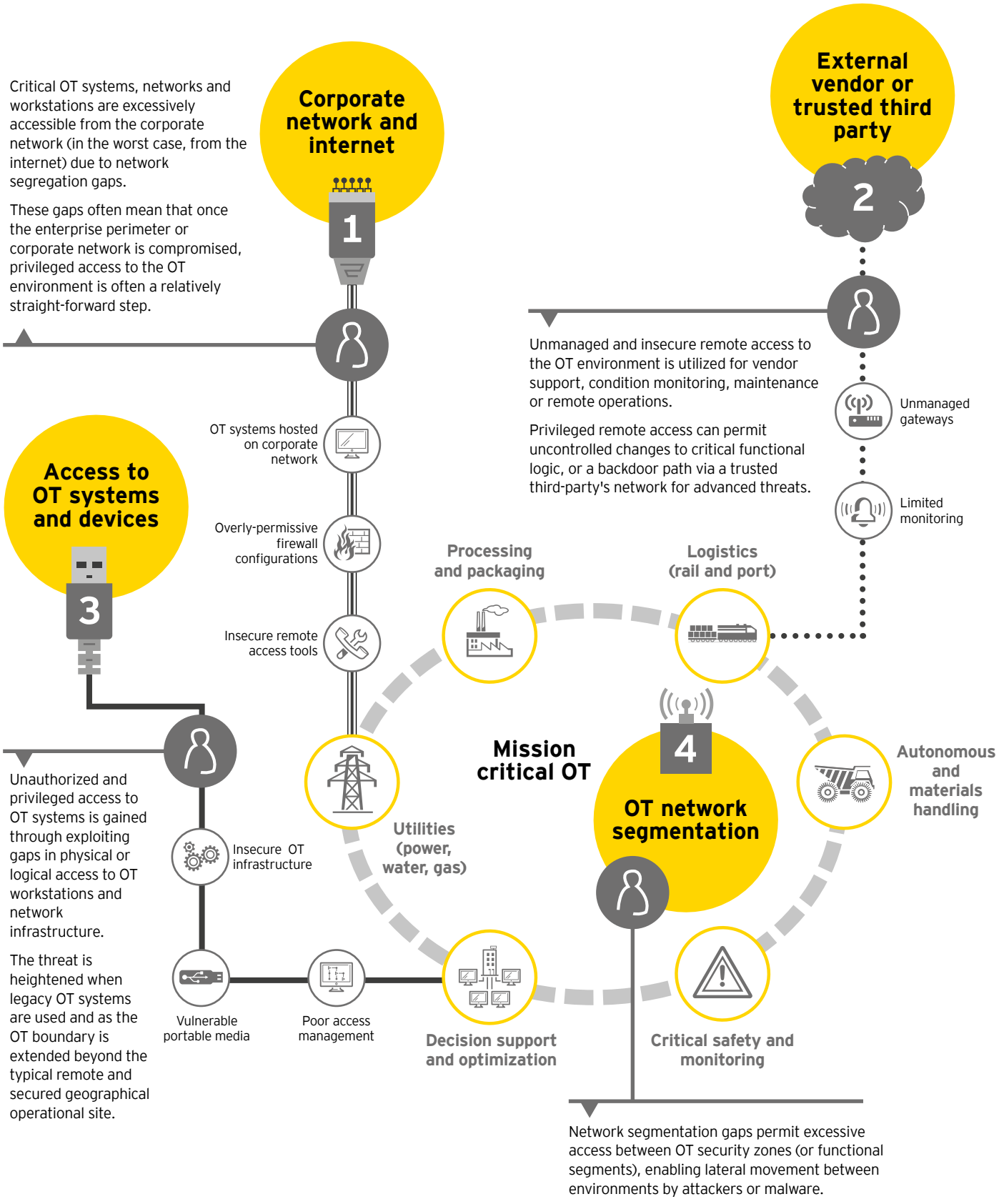
The large number of connected devices across operating environments is also contributing to the growing threat. With increasing investment in digital, reliance on automation systems, remote monitoring of infrastructure for long-term cost efficiency and near real-time decision-making across the value chain, it is the norm for mining and metals companies to have thousands of OT devices connected across geographical environments. However, the increased connectivity of these devices, and by extension the increased attack surface, means that the physical security of remote mining and metals operations is no longer sufficient.

Additionally, equipment and infrastructure that have traditionally been disconnected (e.g., autonomous drills, trucks and trains) are now integrated to provide greater control of operations. This combination of events, coupled with system complexity and third-party risks have led to a further expansion of the "attack paths" that may be used in cyber incidents.

For mining and metals organizations, there are four primary "attack paths" that can be used to compromise and impact operations across the value chain (e.g., extraction, processing/refinement, stock management and shipping). Hackers who exploit these paths frequently utilize a number of common weaknesses found within network architecture, legacy industrial technologies, basic access controls and security configurations, maintenance processes, remote staff and third-party access, and security awareness.

[3] "Cyber threats to the mining industry," *TrendMicro*, 28 June 2016.
[4] "Petya Cyber Attack: List of affected companies shows scale of hack," *Independent*, 27 June 2017.
[5] "Cyberattacks pose serious threat to Canada's automated resource firms," *Globe & Mail*, 26 November 2017.
[6] "Siemens, Trimble, Moody's breached by Chinese hackers, U.S. charges," *CNBC*, 29 November 2017.
[7] "Attackers alter water treatment systems in utility hack," *Securityweek.com*, 22 March 2016.
[8] "German nuclear plant infected with computer viruses," *Reuters*, 26 April 2016.
[9] "Unprecedented malware targets industrial safety systems in the Middle East," *Wired*, 14 December 2017.

EY point-of-view on common cyber attack paths for asset-intensive sectors such as resources



As a result, the entire supply chain is now at risk, which is not limited to the potential of causing disruptions to operations, but worse, significant health and safety consequences (e.g., resulting from shutdown or overriding of fail-safe systems, physical failure of infrastructure, equipment operating outside of expected parameters etc.). If these risks are not being effectively identified, tracked and monitored, it is likely that the organization and its employees will be left significantly exposed. Some of our clients with strong security event monitoring solutions are seeing a rapid increase in the number of new attacks on operational systems, including viruses that are specifically designed to attack these environments.

The challenge

Mounting threat levels now require a more robust response. Our 2017 *Global Information Security Survey* revealed that 53% of energy and resources organizations have increased their spend on cybersecurity over the last 12 months.

Cybersecurity budgets are increasing, but are not enough to effectively manage risk, particularly to mission critical OT.[10] As mining and metals companies continue to move into the digital age, current budgets may not be enough to manage risk, particularly in regard to the growing threat to OT.

97%

say their cybersecurity function does not fully meet their organization's needs.

48%

believe its unlikely their organization will be able to detect a sophisticated cyber attack.

53%

increased their cybersecurity budget over the last 12 months.

Also, too many mining and metals companies are taking an ad hoc approach or acting when it is already too late to manage their risks and vulnerabilities. This approach unnecessarily exposes the enterprise to greater threats.

The responsibility of managing exposure to cybersecurity risks is not one that can be delegated to one or two individuals. Rather, a broad range of individual responsibilities should be brought together to form a single coherent and accessible view of the threat environment.

For example, OT cyber risks may require different technology, engineering, maintenance and process control teams to be responsible and consulted to establish the critical cyber controls and security awareness. However, an accountable owner, such as a Chief Operating Officer or Site General Manager, is needed to drive the change and priority, and sustain ongoing OT cyber risk management.

> "We used to think we were not reliant on technology," he said. But ventilation and conveyor systems are managed by Supervisory Control and Data Acquisition (SCADA) systems. Even new hauling trucks come with 100 wireless sensors to be used. "Our dependence on technology means if access to the internet is shut for a week the company will come to a halt." The hack was "a wake-up call for us," he said, which resulted in a tripling of cybersecurity spend"
>
> **Luis Canepari**
> Goldcorp Vice-President of IT[11]

[10] "2017 EY Global Information Security Survey," *EY*, 2017.

[11] "Canadian cyber attack led to new mining industry threat sharing center," *IT World Canada*, 9 June 2017.

Being ahead of the cyber threats

A step-change in the culture and awareness of the cyber risk within the mining and metals sector is needed to resolve the gaping hole that the "human factor" exposes to cyber resilience and preparedness. The urgency becomes more critical when you accept the ideology that it is no longer "if" but "when."

Organizations need to apply good risk management principles; and this starts with thinking about the issue such as cyber risk, just like a business risk. Understanding the cyber threat landscape is the first and vital foundation step in the change to improve the cyber maturity. In order to address the step-change needed, mining and metals companies need to have a clear plan that forms part of their digital road map and risk management plan. The first step is to establish a baseline of basic cyber controls. This baseline, supported by a risk-based approach to prioritize strategic and long-term cyber investment, should be aligned with the organizations' top cyber threat scenarios.

Four key cyber threats are ever-present within mining and metals organizations that can significantly impact your operations:

1 Enterprise IT and business applications

Threats associated with the global IT network, IT managed services provider, ERP, and key on-premise or cloud-based solutions that enable end user productivity, data storage and compute. Compromises in these systems often lead to "priority one" incidents that need immediate attention and/or recovery.

2 Treasury, financial and commodity trading

Significant cash disbursements (by value and volume) to JV partners, suppliers, government agencies, inter/intra companies and commodity customers are synonymous with the mining industry. With the rise in CEO/CFO/AP-scams and spear-phishing, the occurrence of cyber-enabled crime or fraudulent payments is a real threat.

3 Commercially sensitive and personal data

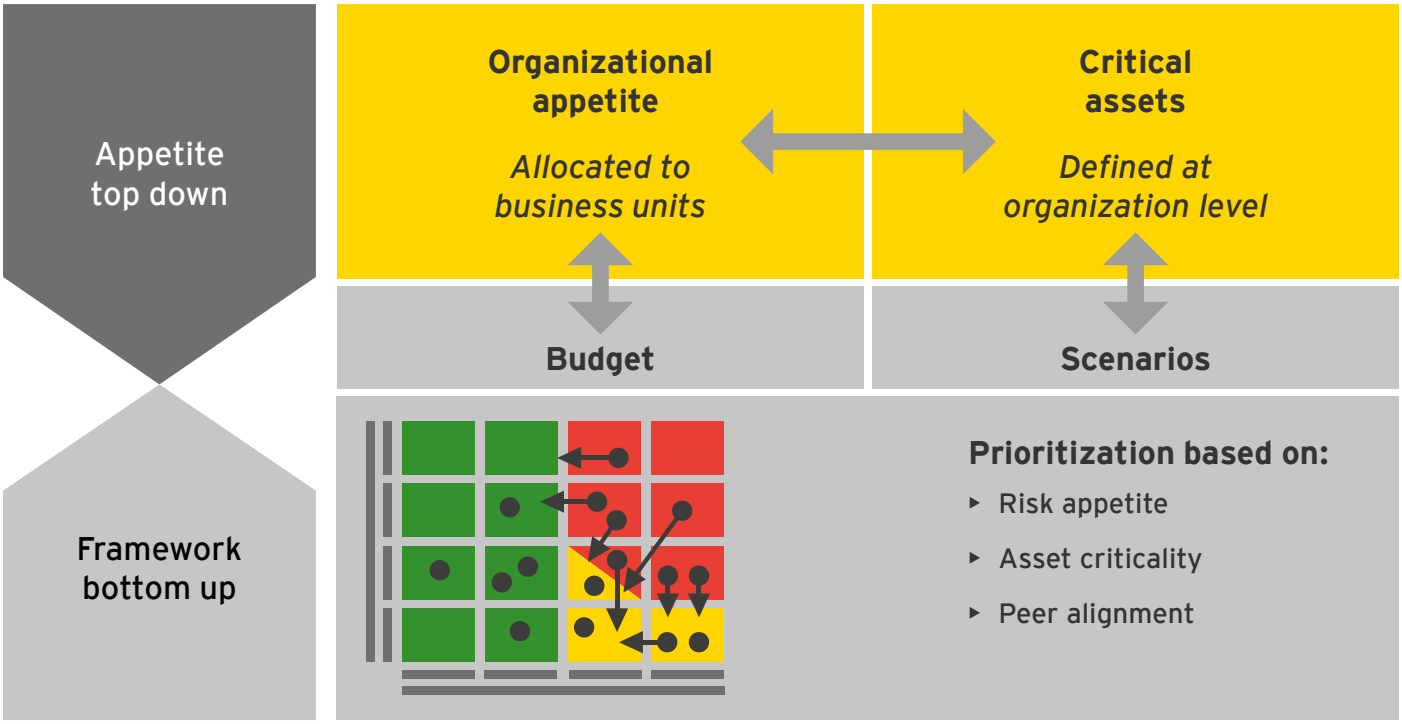
The increase in data breach notification requirements and the rapid pace of online media reporting has meant that all businesses need to pay greater attention to protect sensitive and personal data. For the mining and metals sector, this often translates to personal information within HR, medical hygiene, HSE and contractor management systems, and commercially-sensitive information on senior end-user devices and cloud-based data repositories.

4 Operational technology

The emerging OT cyber threats are evolving and at the forefront of boards, executives and regulators for asset intensive industries. This typically starts with the mission critical OT systems at operational sites, processing plants, and utilities; followed by key IT/OT networks and systems enabling integrated operations, remote monitoring and control, and production sensitive planning and decision support.

To enable this, organizations should adopt a cybersecurity framework for the consistent identification of critical cyber control gaps, threats and actions required to achieve the target risk profile. We believe that irrespectively of the framework adopted, a risk-based approach should be taken, which is fit for purpose, adopts a balance between "protect" and "react," and meets the operational requirements of an organization.

The following is a robust cyber threat approach:



- **Identify the real risks:** map out critical assets across systems and businesses
- **Prioritize what matters most:** assume breaches will occur and improve controls and processes to identify, protect, detect, respond and recover from attacks
- **Govern and monitor performance:** regularly assess performance and residual risk position
- **Optimize investments:** accept manageable risks where budget is not available
- **Enable business performance:** make security everyone's responsibility

An industry-wide approach to the solution

Following the high profile Goldcorp cyber attack and data breach in 2016, a consortium of Canadian miners set up a mining industry threat sharing center. This initiative is aimed at helping companies to collectively deal with cyber-related vulnerabilities to prevent similar attacks from reoccurring. According to Rob Labbe, Director of Information Security at Teck Resources, the mining sector has realized that not sharing threat information made it vulnerable. "In five to seven years it will become impossible to run a safe and environmentally sustainable mine – let alone a productive one – unless it's also secure,"... "I think the industry has started to realize that."

– "Canadian cyber attack led to new mining industry threat sharing center," IT World Canada, 9 June 2017.[12]

[12] "Canadian cyber attack led to new mining industry threat sharing center," *IT World Canada*, 9 June 2017.

Focus on boards

Board level leadership and governance around cyber risk management is lacking[13]

35%

of boards have sufficient cybersecurity knowledge for effective oversight of cyber risks.

10%

say the person with responsibility for cybersecurity sits on their board.

Boards are taking an increasingly active role in addressing the risks that cybersecurity risks posed to their business. There is an increasing demand on management to generate reporting, metrics and insight that provide visibility and assurance over the management of cybersecurity risks.

Most organizations struggle with understanding what to report to the board. This is indicative of the traditional reporting mindset that tends to focus on informing tactical decision-making and reporting on current progress. Instead, board reporting should seek to combine tangible and quantifiable metrics that demonstrate the outcomes resulting from recent key decisions and the performance of the current control environment. Ultimately, to enable effective decision-making, a successful cybersecurity reporting framework must provide the board with a clear and continuous view of the organization's current cyber risk exposure.

To encourage this paradigm shift, boards should apply a risk-focused mindset to transform the questions they ask of management.

Traditional mindset	Risk-focused mindset
What is the status of our cybersecurity improvement initiatives?	How are we measuring the effects of recent initiatives on improving our cybersecurity control frameworks and maturity?
Will implementing a two-factor authentication solution address the findings identified during our last audit?	How does our cybersecurity strategy align with our IT and cloud strategy?
What technologies are we yet to implement that will help us to detect and respond to cyber threats?	What assurance do we have to suggest our current efforts to detect and respond to cyber threats are working effectively?
What do the metrics reported by our firewalls and anti-virus solutions say about our overall level of protection against a cyber threat?	Have we evaluated the effectiveness of our cybersecurity controls to understand how effectively they are protecting our high-value data and critical business systems?

[13] "2017 EY Global Information Security Survey," *EY*, November 2017.

Cybersecurity contacts

Global and Oceania

Michael Rundus
+61 8 9429 2179
Michael.Rundus@au.ey.com

Africa

Wim Hoogedeure
+27 11 772 5200
Wim.Hoogedeure@za.ey.com

Samresh Ramjith
+27 11 772 3000
Samresh.Ramjith@za.ey.com

Argentina

Antonio Ramos
+54 11 4510 2222
antonio.ramos@ar.ey.com

Asia-Pacific

Clement Soh
+61 8 9429 2335
Clement.Soh@au.ey.com

Brazil

Afonso Sartorio
+55 21 3263 7423
Afonso.Sartorio@br.ey.com

Clarissa Ferreira
+55 21 3263 7172
clarissa.ferreira@br.ey.com

Canada

Iain Thompson
+1 604 891 8378
Iain.Thompson@ca.ey.com

Vitaly Sokolov
+1 403 206 5150
Vitaly.Sokolov@ca.ey.com

Chile

Eduardo Valente
+56 2 916 2997
Eduardo.Valente@cl.ey.com

India

Burgess Cooper
+ 91 22 61920000
Burgess.Cooper@in.ey.com

Japan

Dillon Dieffenbach
+81 3 3503 1110
Dillon.Dieffenbach@jp.ey.com

Nordics

Tim Best
+46 31 637 786
Tim.Best@se.ey.com

US

Joshua Axelrod
+1 541 760 8395
joshua.axelrod@ey.com

Western Europe and Maghreb

Marc Ayadi
+33 1 46 93 73 92
Marc.Ayadi@fr.ey.com

Fabrice Groseil
+33 1 46 93 71 65
Fabrice.Groseil@fr.ey.com

How EY's Global Mining & Metals Network can help your business

The sector is returning to growth but mining and metals (M&M) companies face a transformed competitive and operating landscape. The need to improve shareholder returns will drive bold strategies to accelerate productivity, improve margins and better allocate capital to achieve long-term growth. Digital innovation will be a key enabler but the industry must overcome a poor track record of technology implementations. If M&M companies are to survive and thrive in a new energy world, they must embrace digital to optimize productivity from market to mine.

EY takes a whole-of-value-chain approach to support each client to help seize the potential of digital to fast-track productivity, balance portfolios and set a clear roadmap for their new energy future.

EY area contacts

EY Global Mining & Metals Leader
Miguel Zweig
+55 11 2573 3363
miguel.zweig@br.ey.com

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

Brazil
Afonso Sartorio
+55 21 3263 7423
afonso.sartorio@br.ey.com

Canada
Jim MacLean
+1 416 943 3674
jim.d.maclean@ca.ey.com

Chile
María Javiera Contreras
+56 2 676 1492
maria.javiera.contreras@cl.ey.com

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

Commonwealth of Independent States
Boris Yatsenko
+7 495 755 98 60
boris.yatsenko@ru.ey.com

France, Luxembourg, Maghreb, MENA
Christian Mion
+33 1 46 93 65 47
christian.mion@fr.ey.com

Japan
Andrew Cowell
+81 80 2276 4048
andrew.cowell@jp.ey.com

India
Anjani Agrawal
+91 22 6192 0150
anjani.agrawal@in.ey.com

Nordics
Lasse Laurio
+35 8 405 616 140
lasse.laurio@fi.ey.com

Oceania
Scott Grimley
+61 8 9429 2409
scott.grimley@au.ey.com

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

United States
Bob Stall
+1 404 817 5474
robert.stall@ey.com

Service line contacts

EY Global Advisory Leader
Paul Mitchell
+61 2 9248 5110
paul.mitchell@au.ey.com

EY Global Assurance Leader
Alexei Ivanov
+7 495 228 36 61
alexei.ivanov@ru.ey.com

EY Global IFRS Leader
Tracey Waring
+61 3 9288 8638
tracey.waring@au.ey.com

EY Global Tax Leader
Andrew van Dinter
+61 3 8650 7589
andrew.van.dinter@au.ey.com

EY Global Transactions Leader
Lee Downham
+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.

EYG no. 01664-184GBL

BMC Agency
GA 1007086

ED None.

ey.com/miningmetals