Deloitte.

An integrated approach to combat cyber risk

Securing industrial operations in mining

Forward

Although numerous consumer companies have been thrust into the spotlight due to data breaches, the alarm bell has been slow to sound within the mining sector. For years, mining organizations largely had a false sense of security, believing they could operate under the radar of cyber criminals who had more lucrative targets to pursue. Why would malicious actors hack a mining operation when they could attack a consumer organization that moves financial data? Today, that reasoning has become as faulty as a patch on decades-old software.

The mining industry is moving into its next stage of evolution, which is sometimes referred to as "intelligent mining." As detailed in the recent Deloitte report, Intelligent Mining: Delivering real value, this entails—in addition to broader organizational change—rapidly integrating robotics, automation, and the Internet of Things (IoT) into the operational environment.[1] At the same time, the interest of cyber criminals in industrial operations has increased over the last decade, while the motives for their actions have become more diffuse. Malicious hacking, ransomware attacks, electronic fraud, data leaks and corporate espionage have become prevalent worldwide. These illicit activities are often driven by financial, political, or competitive objectives—or merely by the desire to cause disruption.

The combination of greater connectivity and proliferating threat vectors has already resulted in cyber attacks that have compromised both production and safety. These attacks have made cyber security a hot discussion topic within boardrooms around the globe, and now a growing number of organizations are developing transformation programs to address these new operational threats.

However, making operational processes secure, vigilant and resilient is a challenge. For example, deploying the organization's existing cyber capabilities within the operations environment requires harmonizing two cultures, which is challenging. In addition, the operations environment demands continuous availability, along with tailored technical solutions that are not always easy to secure.

Solving these challenges requires a good understanding of both engineering and information technology (IT) disciplines as well as leading, sector-specific cyber security practices. This paper shares the understanding we've culled from our field experience, including lessons learned in helping mining companies to go beyond safety in securing their industrial control systems (ICS).

Introduction

Critical infrastructure relies on Industrial Control Systems (ICS) to maintain safe and reliable operations. Engineers have successfully designed and deployed ICS with safety and reliability in mind, but not always security. Why? Originally, there was little need for it. Fit-for-purpose, isolated operational systems were the order of the day. Since these operational systems were not integrated to enterprise systems or even to each other, the risk of a large-scale cascading failure due to an attack—cyber or otherwise—was extremely remote.

Fast forward 20 years, and digitization and IoT has turned the most basic assumptions about operational security upside down. Today, all sorts of industrial facilities, including mine sites, mineral processing plants, and remote operations centers, are vulnerable to cyber attacks. These vulnerabilities span critical electrical infrastructure, connected distributed control systems, programmable logic controllers (PLCs), supply chain partners, and more. Even a shaft mine with little internet connectivity underground is vulnerable to cyber-attacks on the above-ground electrical system, which could put the mine's ventilation system at risk. Even more disconcerting, mitigating this type of cyber threat may be completely outside of the company's control if the mine is reliant on the broader electricity grid rather than on its own distributed energy resources, such as solar panels or diesel generator sets.

Across multiple vectors, operational systems can now be compromised by external or internal bad actors, causing safety or production failures and increasing commercial risk. Although ICS are typically designed to fail safe, the increasing sophistication of cyber criminals heightens the risk of catastrophic incidents, along with the magnitude of the impacts in terms of cost, safety, reputation and commercial or financial losses.

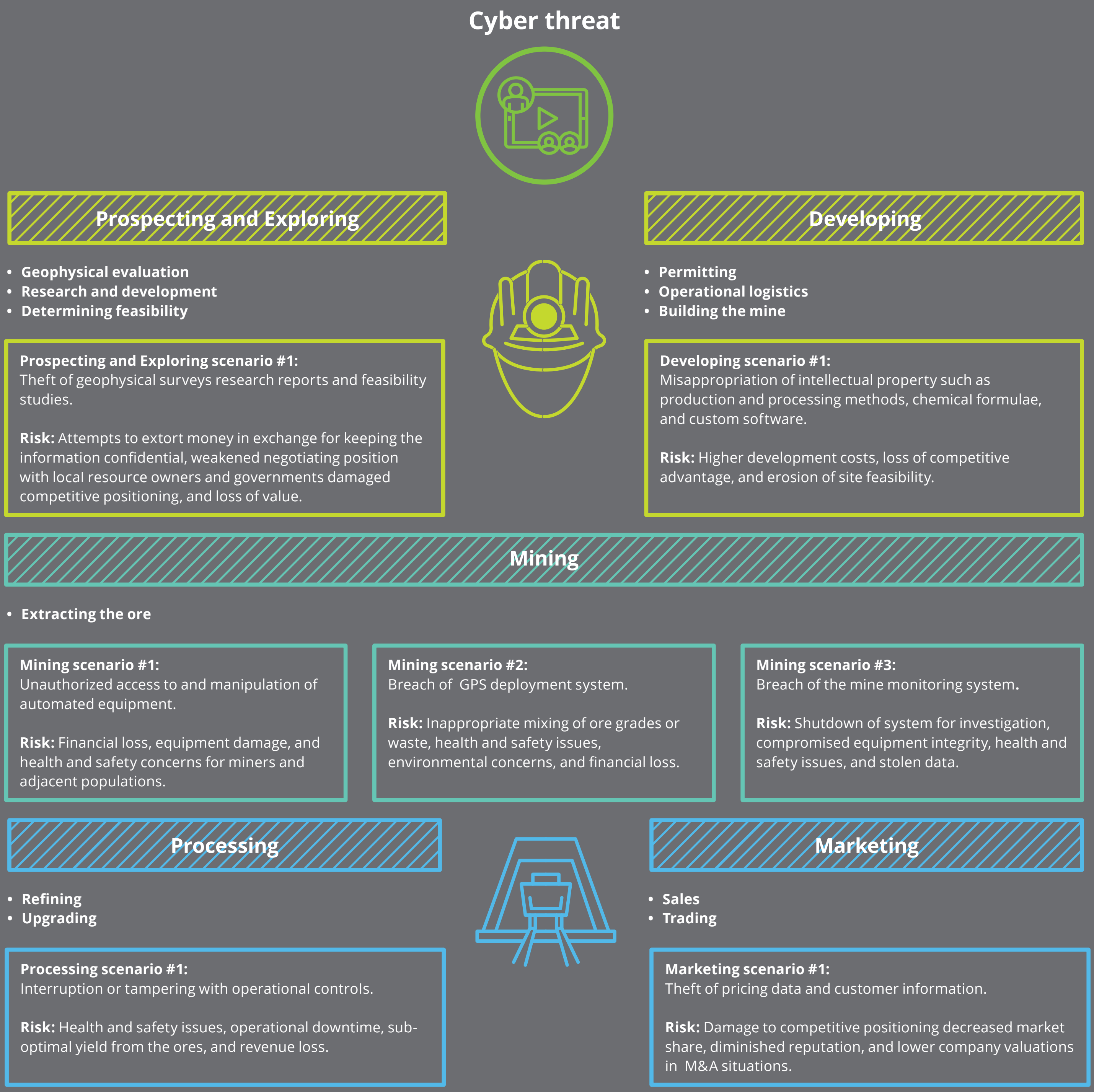
As mining companies begin to grapple with the implications of an inter-connected operational environment, their corporate back-office systems are simultaneously coming under fire. Nation states, local activist groups, and even competitors have shown a keen interest in stealing intellectual property and proprietary information, such as exploration data, company valuations and other information pertaining to mergers and acquisitions. Often the goal is to gain an edge in negotiations or to influence business dynamics.

Threats such as these have made cyber security a top concern among senior leadership and boards of directors, and like other industries, the Energy, Resources and Industrials (ER&I) industry has been working to shore up its defenses. Such incidents inspired a group of Canadian mining companies to start the Mining and Metals Information Sharing and Analysis Center (MM-ISAC).[2] Launched in April 2017, the non-profit, industry-owned Center is open to all companies in the mining and metals industry.[3] It allows member companies to share critical cyber security information through secure channels enabling them to benefit from this intelligence at a reasonable cost.[4] Importantly, the Center hints at the type of information sharing and resource pooling that could help the sector to combat cyber threats more effectively, similar to the collective approach taken by the financial sector.

While the mining industry has suffered data breaches and loss of intellectual property, it has escaped a major operational catastrophe thus far. However, this good fortune may not last unless mining companies expand their cyber security programs to protect operational as well as back-office systems and embrace the new level of intra-industry collaboration required to stay ahead of the rapidly evolving threat landscape. At a minimum, companies will need to think more broadly about what cyber security entails. To date, mining companies have been primarily focused on protecting corporate, as opposed to operational, systems and data. That's because the IoT—where production can be controlled from an iPad or a smart phone, for instance—is relatively new, gaining momentum over the last decade, and because operational systems are inherently different, requiring engineering know-how, in addition to IT expertise, in order to secure them appropriately.

Today, an approach is needed that brings together IT and engineering to address cyber security programmatically and sustainably. The following discusses the goals of such an approach as well as practical steps for getting started. But first, let's take a closer look at the types of cyber risks facing the mining sector, how they can disrupt the value chain, and what the consequences could be.

Figure 1. How cyber threats impact the mining value chain



Cyber threat

Prospecting and Exploring

- **Geophysical evaluation**
- **Research and development**
- **Determining feasibility**

Prospecting and Exploring scenario #1:
Theft of geophysical surveys research reports and feasibility studies.

Risk: Attempts to extort money in exchange for keeping the information confidential, weakened negotiating position with local resource owners and governments damaged competitive positioning, and loss of value.

Developing

- **Permitting**
- **Operational logistics**
- **Building the mine**

Developing scenario #1:
Misappropriation of intellectual property such as production and processing methods, chemical formulae, and custom software.

Risk: Higher development costs, loss of competitive advantage, and erosion of site feasibility.

Mining

- **Extracting the ore**

Mining scenario #1:
Unauthorized access to and manipulation of automated equipment.

Risk: Financial loss, equipment damage, and health and safety concerns for miners and adjacent populations.

Mining scenario #2:
Breach of GPS deployment system.

Risk: Inappropriate mixing of ore grades or waste, health and safety issues, environmental concerns, and financial loss.

Mining scenario #3:
Breach of the mine monitoring system.

Risk: Shutdown of system for investigation, compromised equipment integrity, health and safety issues, and stolen data.

Processing

- **Refining**
- **Upgrading**

Processing scenario #1:
Interruption or tampering with operational controls.

Risk: Health and safety issues, operational downtime, sub-optimal yield from the ores, and revenue loss.

Marketing

- **Sales**
- **Trading**

Marketing scenario #1:
Theft of pricing data and customer information.

Risk: Damage to competitive positioning decreased market share, diminished reputation, and lower company valuations in M&A situations.

Understanding the risks

One of the main factors that makes it so difficult to secure ICS is that they were not designed to be connected, yet today they are networked. Digitization of operational processes in the mining industry has led to new opportunities to improve productivity and to drive down costs. However, the convergence of operational and business systems has also opened up the enterprise to a whole new array of cyber risks. Consider the following scenarios, the possibility of which didn't even exist a few years ago:

- Lack of authentication in wireless communications allows a cyber criminal to hijack an autonomous hauling system, halting the movement of materials, damaging costly equipment, and putting people's lives at risk.

- Poor security practices by a third-party contractor allow a virus to migrate into the production environment, shutting down critical Supervisory Control and Data Acquisition (SCADA) systems and creating unsafe working conditions.

- Insufficient employee training about how to recognize spear phishing and social engineering attempts enables a competitor to circumvent the organization's security protocols and steal sensitive pricing data.

- Weaknesses within the supply chain allow ICS equipment to be intercepted and malware installed prior to delivery at a mining site. Improper testing of the components prior to deployment then allows the virus to proliferate undetected, resulting in a system crash, leading to disruption or shutdown of operations. This is indeed how the notorious Stuxnet virus is believed to have been introduced into Iran's nuclear infrastructure.[5]

- A commodity IT solution with open design protocols allows members of an adversarial community to gain remote access to PLCs, thus giving them the ability to disrupt the production process at will.

As these examples illustrate, cyber threats can come from many directions, including internal actors aiming to sabotage production, competitors seeking to cause brand damage, and external parties, such as activist groups, wanting to shut down operations.

However, not all vulnerabilities stem from the technologies themselves. Diverse mine types and locations, coupled with the decentralized structure of many companies, also pose a challenge. For instance, it is not uncommon for a mining organization to be running 10 different versions of an industrial control system across 10 different mines, each having greater or lesser degrees of internet connectivity. In this type of environment, it is not uncommon for the corporate Chief Information Security Officer (CISO) to have little control over site-specific security procedures.

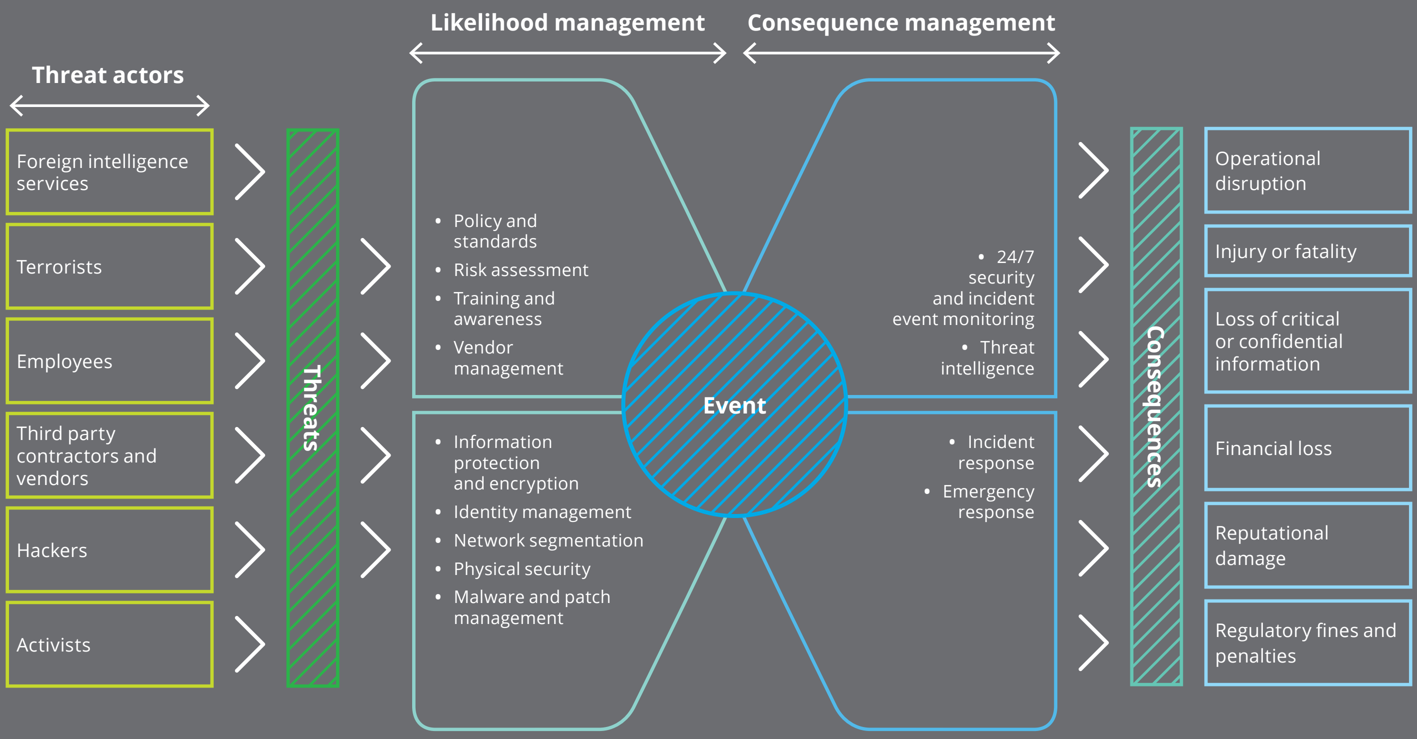
Behavioral aspects additionally come into play. For instance, sometimes a lack of security awareness within the organization can inadvertently expose systems to cyber attacks, such as when employees bring portable media that is infected with malware into the environment.

Furthermore, many operations employees simply believe that their systems are an unlikely target, thus they are reluctant to buy into the need to change their behaviors and implement new security protocols. After all, not long ago they could safely assume that all equipment components were trustworthy, which is no longer the case since digital sensors and controllers can be manipulated to provide false input and misguiding status information. Another outdated assumption is that process failures are mainly caused by weather conditions, human error and equipment fatigue, and not necessarily malicious manipulation of the system by those intending to inflict harm.

Whether a cyber breach is intentional or unintentional, the consequences can be grave, ranging from compromising confidential data to triggering system failure or shutdown. This can result in decreased revenue, reputational damage, environmental disaster, legal penalties, and in extreme cases, loss of life.

It’s easy to see why integrating effective and comprehensive cyber security controls into ICS is necessary, if not increasingly becoming mandatory. But to get there, companies must find a way to reconcile the divergent points of view of IT and operations: ICS specialists do not always fully understand modern IT security risks, just as IT security specialists often do not completely comprehend the industrial processes supported by ICS. In our experience, a bowtie analysis, a common concept used in engineering for failure mode analysis, can be a useful tool for bridging this gap. While any analysis will be company-specific, Figure 2 provides an example of how the “bowtie” might look for a mining company.

Figure 2. Example of a "Cyber Risk" bowtie analysis for a mining company



Source: Information adapted from Talbot, J, and Jakeman, M, 2008, 'Security Risk Management Body of Knowledge', RMIA, Carlton South

Conduct a maturity assessment

Once the risks are understood, a mining company should assess the maturity of its cyber security controls not only in a corporate context but also in an operational environment. While not every risk can be mitigated, it's important to know what type of controls are in place and where to focus improvement efforts. This means giving appropriate consideration to how potential security breaches within ICS link to business risks. Importantly, this can't be done by an engineering or IT group on its own: it requires a multi-disciplinary team of business, operations, engineering and IT security professionals to:

- Record assets and facilities and rank them in terms of criticality. This can involve asking questions such as: Are there factors that make a certain mine site or processing plant a particularly attractive target? Are corporate IT standards, governance and monitoring processes being applied to all ICS assets? Have the full range of cyber vulnerabilities been considered, and have the potential consequences been identified, and ideally quantified?

- Determine if critical assets and facilities have well-known and exploitable vulnerabilities. In the mining industry, these vulnerabilities differ somewhat according to where they fall within the value chain. For instance, corporate offices are commonly exposed to theft of proprietary exploration data, such as geophysical surveys, ore-body composition reports, feasibility studies, and strategic planning information—all of which can jeopardize competitive positioning. Back-office systems are also vulnerable to theft of sensitive data related to executive decision-making, payroll, company valuations, joint ventures, M&A, and pricing, which can weaken negotiations with governments and their constituents.

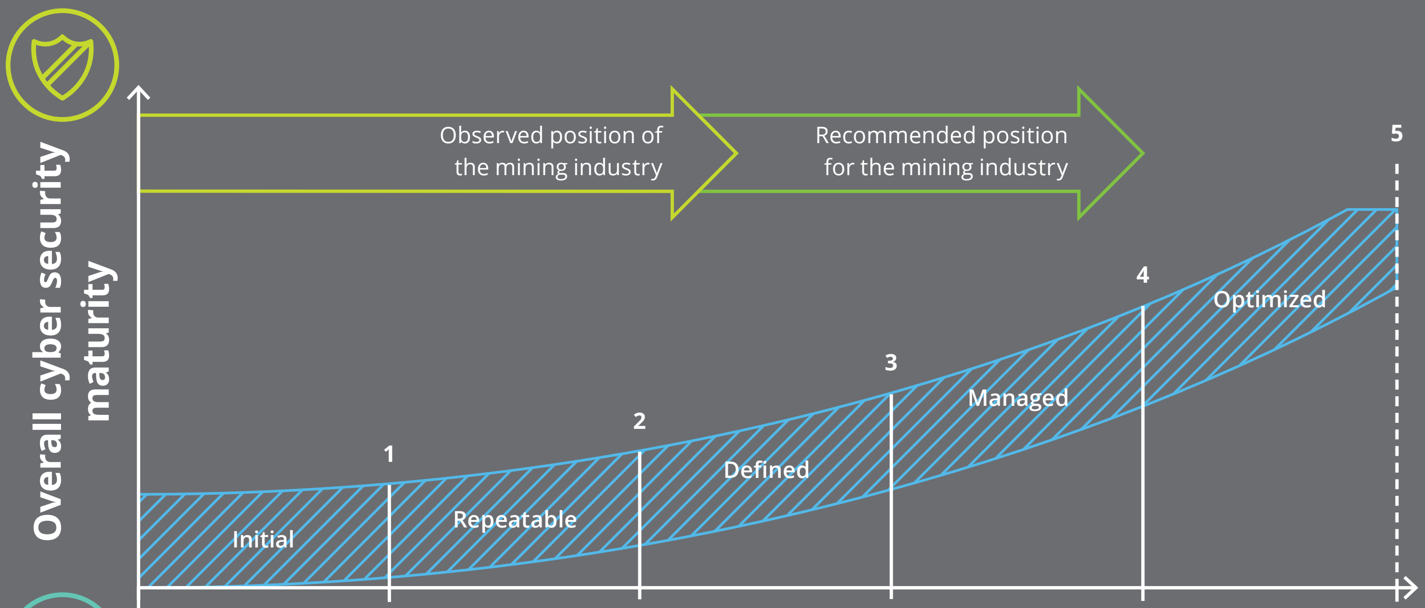
- Mine sites and processing plants on the other hand are vulnerable to the malicious manipulation of supervisory control and data acquisition (SCADA) and other operational systems; production shutdowns due to virus infections; and loss of communication to workers and remote operation centers.

Here, the consequences are more physical, potentially resulting in unsafe working conditions, environmental damage, and production downtime, which in turn could lead to human and financial loss and ultimately jeopardize the company's social license to operate. Similarly, cyber risks for remote operations centers also have both physical and financial implications, such as unsafe conditions within the mines, disruption to materials movement and communication, and improper handling of chemicals or other hazardous materials. This could result in revenue loss, brand damage, and regulatory and compliance violations.

- Assess the maturity of the controls environment for proactively managing these threats. In gauging the sophistication of governance and controls, it is often helpful to use an established framework such as the Deloitte cyber security maturity model, which is presented in Figure 3. In performing maturity assessments for a broad range of energy and resources companies, we've observed that the maturity of the mining industry as a whole is about 2.5 on this scale, whereas the recommended position is greater than 4.

Throughout the maturity assessment process, it is important to understand the difference between the security considerations for business systems versus industrial control systems. In today's integrated environment, IT security standards and processes must be capable of addressing both back-office systems and ICS in a manner that neither affects the performance of current systems nor interferes with existing mechanisms for protecting safety and reliability.

Figure 3. The Deloitte cyber security maturity model


Overall cyber security maturity
Observed position of the mining industry
Recommended position for the mining industry
1
2
3
4
5
Initial
Repeatable
Defined
Managed
Optimized

Behaviors	• Dependent primarily on individuals and isolated practices • New or relatively inexperienced security team	• Ad-hoc approach with some tools and documented procedures • Established security function	• Clearly defined strategy supported with tools and methods to manage risk • Security processes defined and in place • Established security function with integrated systems designed to predict, prevent, detect, and respond	• Established security capability, with defined processes and measures • Focused on risk management and business enablement • Two plus years operating with defined processes and practices	• Risk sensing and predictive analytics used to model threats • Highly automated • Five plus years operating without a significant failure • Board level engagement
Key controls	• General awareness of ICS cyber security needs but not considered a priority	• ICS cyber security strategy and policy established • Awareness and education • Segmentation of ICS and corporate networks • Annual risk assessment with identified gaps and remediation plan • Physical security	• Inventory of all cyber assets • Security standards developed • Annual vulnerability testing • 24/7 security monitoring • Incident response plan developed and tested • Virus and malware protection	• Industrial control systems secured according to security standards • Identity and access management for provisioning and authentication • End point security • Mobile protection • Third party security	• Cyber threat intelligence/sensing • Data loss prevention • Behavioral analytics

Build a unified program

For over 50 years, safety was the primary motivation behind designing and deploying controls for physical production processes. While this motivation is still there—keeping processes in a safe and operational state—the landscape of potential disruptions now encompasses the cyber domain. This now requires a unified program to address cyber security systematically across the business and operations. Although building and implementing a program of this nature is a multi-year, transformational effort, each phase of the initiative should have the same objective in mind: moving up the maturity scale to create an ICS environment that is secure, vigilant, and resilient.

Secure

Being secure is about preventing system breaches or compromises through effective, automated controls and monitoring. But, it's not feasible to secure everything equally. Critical assets and infrastructure and their associated ICS would obviously be at the top of the list, but it's important to remember that they're not isolated components. They're part of larger supply chains, so it's essential to shore up weaknesses throughout end-to-end processes. This can involve many layers and types of controls, ranging from installing firewalls to "hardening" sensors such as on drilling machines, excavators, earth movers, crushing and grinding equipment and processing plants. Systems need to be designed to consider that the entity operating an asset may not be the only organization with rights to data. Service and supply companies and equipment vendors may also be given visibility into operational and equipment performance data in order to improve the services they can offer. Unless properly structured, this might provide an opportunity for unforeseen data leakage or system weaknesses, which could be exploited by third parties. It is essential to build control and monitoring systems with clearly defined data access rights and the ability to identify when these are contravened.

Vigilant

Security alone is not enough. It must be accompanied by vigilance, or continuous monitoring to determine whether a system is still secure or has been compromised. Worthwhile efforts to be vigilant start with an understanding of what you need to defend against. There are discernable threat trends in the mining industry, which provide a good starting point for understanding the types of attacks being launched against ICS. These trends, however, need to be supplemented by an understanding of your organization's specific business risks in order to anticipate what might occur and design detection systems accordingly.

Resilient

A resilient organization should ensure that it has the plans and procedures in place to identify a cyber attack, contain or neutralize it, and rapidly restore normal operations. We can refer to these steps as "detect, respond and recover," and the protocols for ensuring successful outcomes will depend on the type of cyber issue identified.

At any stage of the mining value chain, whether it be exploration, development, extraction, processing, or delivery logistics, continuous automated monitoring of equipment should allow real-time detection of anomalies. This includes continually knowing the status of a diverse array of property, plant and equipment, spanning excavators and drag lines, drills and crushers, loaders and haul trucks, and everything in between—not to mention processing plants, tailings ponds and distributed energy resources. Ongoing visibility into these metrics should facilitate rapid reaction to eliminate environmental and safety hazards stemming from out-of-control operations, up to and including shutting down where necessary. It may be harder to detect the misappropriation or alteration of commercially sensitive data, such as degree of purity, dilution of ore, and waste volume. Therefore, it is even more important to build safeguards into the design of these data management systems.

Even if security controls fail and a cyber attack goes undetected, the ability to mount a strong response can help to contain production losses as well as financial, environmental and brand damage. The response and recovery phases will need to include not only immediate remediation of compromised equipment and systems but also in-depth analysis of where and how cyber attacks occurred, what system vulnerabilities allowed them to happen, and what mitigation measures should be implemented to prevent further risks.

Critically, it's not sufficient to just put playbooks and policies in place. Like a familiar fire drill, they should be rehearsed periodically through cyber war-gaming and simulations that bring together business and technology teams.

Implement key controls

While risk appetite and maturity levels will vary, there are a few pillars for cyber risk transformation in an ICS environment that nearly every mining company should have in place. Implementing these key controls can provide a starting point for a customized program aimed at achieving security, vigilance and resiliency.

- Awareness training: Cyber security awareness needs to be promoted among professionals in different roles in the organization, along with training to give them the necessary skills to interact with systems safely, securely and responsibly.

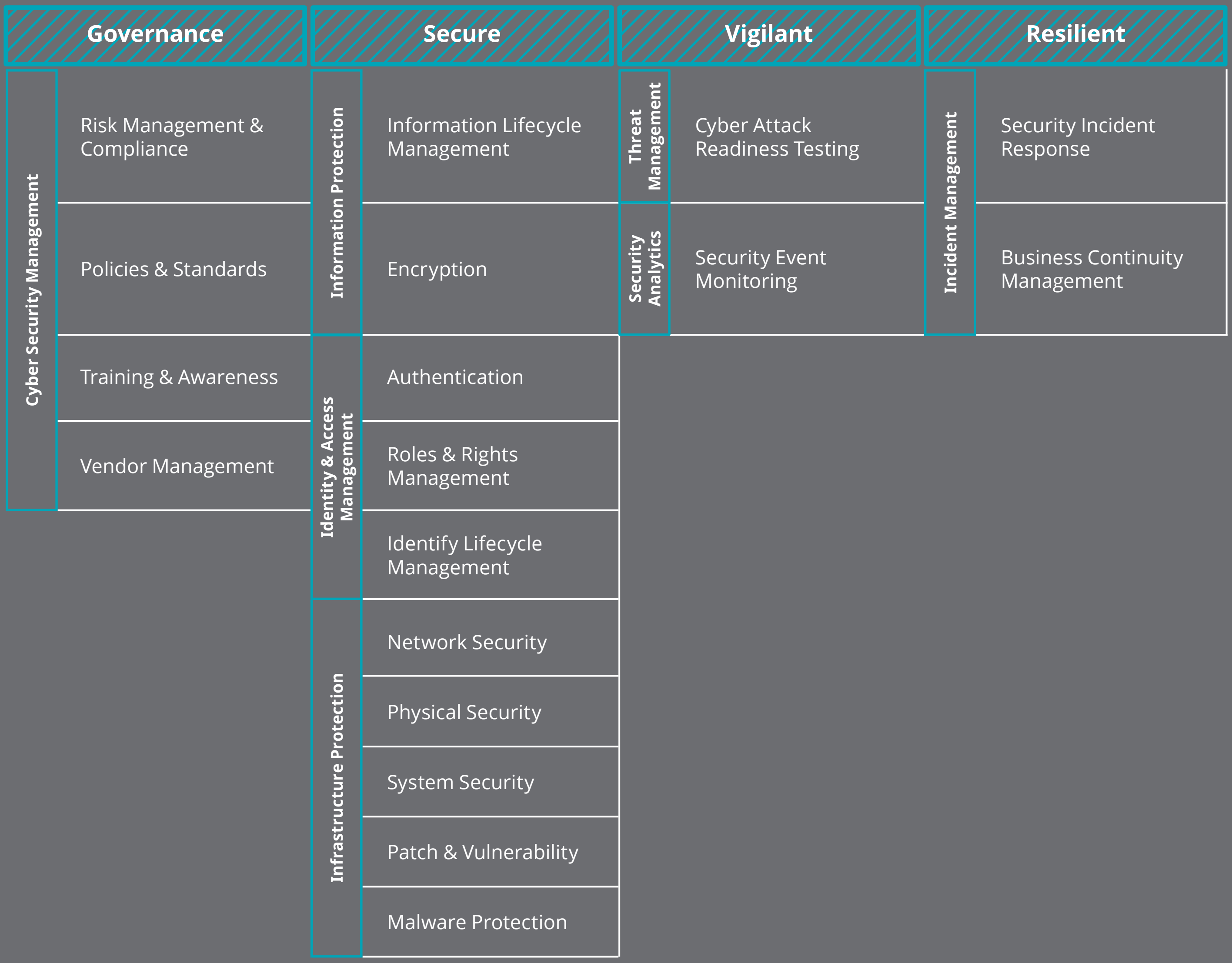
- Access control: ICS components, including hardware, applications and networks, are both physically and logically secured, with access only being granted after formal authentication and authorization.

- Network security: Access to wired and wireless networks within the ICS environment is limited and secured in accordance with leading identity and access management practices, including dynamic provisioning and authentication, 24/7 monitoring and end point security.

- Portable media: Use of portable media within the ICS environment is restricted and scanned for malicious software.

- Incident Response: Incident management policies and procedures are developed and periodically tested.

Figure 4. Key controls



Governance

Cyber Security Management

- Risk Management & Compliance
- Policies & Standards
- Training & Awareness
- Vendor Management

Secure

Information Protection

- Information Lifecycle Management
- Encryption

Identity & Access Management

- Authentication
- Roles & Rights Management
- Identify Lifecycle Management

Infrastructure Protection

- Network Security
- Physical Security
- System Security
- Patch & Vulnerability
- Malware Protection

Vigilant

Threat Management

- Cyber Attack Readiness Testing

Security Analytics

- Security Event Monitoring

Resilient

Incident Management

- Security Incident Response
- Business Continuity Management

Embrace good governance

Clear ownership of ICS security is crucial, and roles and responsibilities should be clearly defined for everyone involved, from managers to process operators to third parties. Ultimately, there must be a single line of accountability. Without one, it is challenging not only to define requirements that apply to the whole organization but also to identify where centralized versus local solutions are appropriate.

In the past, the manufacturing and engineering discipline owned the production environment, including ICS and related security mechanisms. Today, ICS security is increasingly becoming a part of the corporate organization, falling under the auspices of the CISO. Yet, this isn't about IT stepping in and running the mine site or the processing plant. Even with CISO accountability, the engineering organization is still responsible for developing the right solutions and deploying them at the sites.

Implementing a cyber security program within the ICS domain additionally poses some distinct talent management challenges. The job profile often requires people to be stationed at sites for a number of years. Without providing them with a clear career path, two things can happen:

1. IT professionals who are forced into an ICS security role will consider the program as merely a hobby and they will not actively contribute.

2. Security-savvy professionals will quickly reach their peak at a site and then will search for another organization.

Ideally, the organization should develop an awareness program to bridge the gap between IT and ICS professionals as well as a career development path for those wishing to specialize in ICS security. This path often starts with an entry-level site analyst position and progresses to a global security role within the organization.

Expand the conversation

It's easy to see how cyber risks can damage shareholder value, but managing these risks effectively can generate value as well. For instance, an organization can use a secure, vigilant and resilient cyber security program to provide stability and continuity, create a favorable environment for innovation and R&D, build confidence among business partners and resource owners, attract and retain talent, and preserve the company's social license to operate. Yet, many executives in the mining sector are focused on improving returns, and they don't necessarily recognize the connection between managing risk and increasing the value of the company. In our experience, this situation can create a precarious blind-spot for mining executives.

The most potent risk is often the one you don't know about. Time and again, executives go through the exercise of creating risk registers, which typically detail the most likely risks. Rather than limiting the conversation to common risks, it's often more productive to think about how much a potential incident could affect returns, even if it is highly unlikely. If a "black swan" does occur, how much value would it destroy? And, if it does not happen, how much value would it protect and create?

More expansive conversations are generally needed at the executive level to consider not only the likelihood but also the potential impact of an ever-evolving spectrum of cyber risks. By elevating the topic of cyber risk to the same level as the topic of returns in the executive suite, mining organizations can largely avoid what is perhaps the greatest danger of all: a false sense of security.

Conclusion

In the past few years, the mining industry has seen the traditional boundaries between corporate IT and ICS largely disappear. Today, the evolution continues with the pursuit of intelligent mining to tackle the dual sector challenges of declining ore grades and operating efficiency. Beyond digitizing mining operations, intelligent mining is about making informed decisions through accurate, complete and timely information, which requires forging new connections across previously isolated mines sites and functional business silos. As this interconnectedness marches on, so does the frequency and sophistication of cyber attacks. However, most companies have not kept pace in terms of their preparedness. The call to bridge the cyber-readiness gap has never been louder, with growing public awareness of cyber crime and the potentially disastrous impact it can have on critical infrastructure. The place to start is assessing the maturity of your cyber security controls environment. Going beyond traditional operational safety considerations to implement a secure, vigilant and resilient program is not only essential for enhancing a mining company's ability to protect operational integrity amid a growing range of cyber threats but also to achieve operational excellence by taking advantage of the productivity benefits offered by a digitized, fully integrated ICS environment.

Contacts

Authors

Sandeep Verma
Global Risk Advisory Leader - Mining & Metals
Deloitte US
sxverma@deloitte.com

Andrew Douglas
Managing Director – Risk Advisory
Deloitte US
andouglas@deloitte.com

Andrew Deas
Managing Director – Risk Advisory
Deloitte US
adeas@deloitte.com

Adriaan Davidse
Director – Consulting
Deloitte Canada
adavidse@deloitte.ca

Global contacts

Phil Hopwood
Global Leader – Mining & Metals
Deloitte Touche Tohmatsu Limited
pjhopwood@deloitte.ca

Paul Zonneveld
Global Risk Advisory Leader – Energy, Resources & Industrials
Deloitte Canada
pzonneveld@deloitte.ca

Rajeev Chopra
Global Leader – Energy, Resources & Industrials
Deloitte Touche Tohmatsu Limited
rchopra@deloitte.co.uk

Sandeep Verma
Global Risk Advisory Leader - Mining & Metals
Deloitte US
sxverma@deloitte.com

Country contacts

Africa
Andrew Lane
+27 11 517 4221
alane@deloitte.co.za

Americas
Glenn Ives
+1 416 874 3506
gives@deloitte.ca

Argentina
Edith Alvarez
+11 4320 2791
edalvarez@deloitte.com

Australia
Ian Sanders
+61 3 9671 7479
iasanders@deloitte.com.au

Brazil
Andre Joffily
+55 21 3981 0490
ajoffily@deloitte.com

Canada
Andrew Swart
+1 416 813 2335
aswart@deloitte.ca

Chile
Christian Duran
+56 22 729 8286
chrduran@deloitte.com

China
Kevin Xu
+86 10 85207147
kxu@deloitte.com.cn

Colombia
Julio Berrocal
+57 5 360 8306
jberrocal@deloitte.com

France
Damien Jacquart
+33 1 55 61 64 89
djacquart@deloitte.fr

India
Kalpana Jain
+91 11 4602 1406
kajain@deloitte.com

Mexico
Cesar Garza
+52 871 7474401 x4401
cgarza@deloittemx.com

Peru
Karla Velásquez
+51 1 211 8559
kvelasquez@deloitte.com

Poland
Zbig Majtyka
+48 32 508 0333
zmajtyka@deloittece.com

Russia – CIS
Igor Tokarev
+74 95 787 0600 x 8241
itokarev@deloitte.ru

Southeast Asia
Rick Carr
+65 623 27138
RickCarr@deloitte.com

Switzerland
David Quinlin
+41 58 279 6158
dquinlin@deloitte.ch

Turkey
Uygar Yörük
+90 312 295 4700
uyoruk@deloitte.com

United Arab Emirates
Salam Awawdeh
+971 4 376 8888
SAwawdeh@deloitte.com

United Kingdom
Tim Biggs
+44 20 7303 2366
tibiggs@deloitte.co.uk

United States
Amy Winsor
+1 303 312 4156
awinsor@deloitte.com

End Notes

1. “Intelligent Mining: Delivering Real Value,” Deloitte, 2018, https://www2.deloitte.com/global/en/pages/energy-and-resources/articles/intelligent-mining-deloitte.html.

2. Mining and Metals Information Analysis Centre, http://www.mmisac.org/, accessed July 17, 2018.

3. Ibid.

4. Ibid.

5. Mark Clayton, “Exclusive: New thesis on how Stuxnet infiltrated Iran nuclear facility,” Christian Science Monitor, February 25, 2014, https://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility, accessed July 18, 2018.

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see http://www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500®companies. Learn how Deloitte's approximately 264,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") 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 entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.