
# Cyber Protections for the Mining Sector: Best Practices

*Camara Minera de Chile, 12 May 2021*

**Michael Berk**
Chief Operating Officer
The ALRM Group

info@thealrmgroup.ca www.thealrmgroup.ca

# The ALRM Group Inc.

- El **Grupo ALRM** se fundó en 2015, con oficinas en Ottawa / Canadá y Santiago / Chile.
- Al combinar el diseño de proyectos, la experiencia técnica y las herramientas, y las mejores prácticas de clase mundial, ayudamos a:
  - Clientes gubernamentales mejorando la confianza pública en los servicios gubernamentales prestados por personal eficiente mediante la adopción de procesos efectivos en un entorno más seguro;
  - Clientes corporativos mediante la transición hacia la adopción de una postura de seguridad más resistente lograda mediante la incorporación de medidas de seguridad holísticas y proactivas, soluciones tecnológicas avanzadas y los mejores estándares de la industria.
- El **Grupo ALRM Chile** implementa proyectos de colaboración con el Gobierno de Chile en los sectores de defensa y seguridad on un enfoque en:
  - Soluciones cibernéticas de detección y respuesta gestionadas,
  - Soluciones de seguridad pública a través de un sistema de despacho asistido por computadora,
  - Soluciones de inteligencia de código abierto (OSINT),
  - Diseño integral de programas y soluciones de seguridad.

THE ALRM GROUP
CANADIAN EXCELLENCE IN BUILDING INTELLIGENT CAPACITY

# Cyber threats in the Mining Sector

- Digital transformation, automation and IIoT devices = operational efficiencies. BUT, the increased connectivity in operational technology (OT) environments expands the threat surface.
- If not protected, these devices are vulnerable to cyber attacks and negative consequences: operational disruptions, downtime, equipment malfunction, loss of access to equipment and data, theft of intellectual property and corporate secrets, and financial losses.
- **PROBLEM**: OT networks and industrial control systems (ICS) that rely on IIoT devices are not well integrated with existing IT structures: installed on legacy devices that lack appropriate cybersecurity controls.
- For example, the ICS advisories issued by the Canadian Center for Cyber Security in:

| 2019 | 2020 | 2021 (Jan-May) |
|---|---|---|
| 44 | 183 (Jan-May = 48) | 78 |

- The affected ICSs included: **Cassia Networks, ABB, Schneider Electric, Siemens, Rockwell Automation, Avantech, GE, Honeywell** and many other system providers.
- According to Accenture, the average annual cost of cybercrime to a Canadian mining company was over $12 million in 2018 (Source: Canadian Mining Journal, April 2020)

THE ALRM GROUP
CANADIAN EXCELLENCE IN BUILDING INTELLIGENT CAPACITY

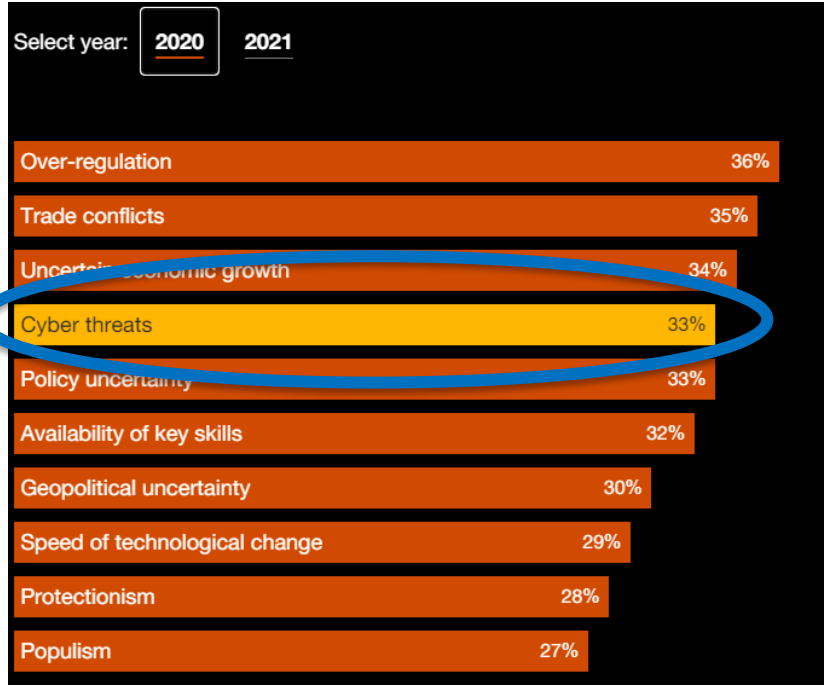
# Actores de Amenazas y Sus Motivaciones

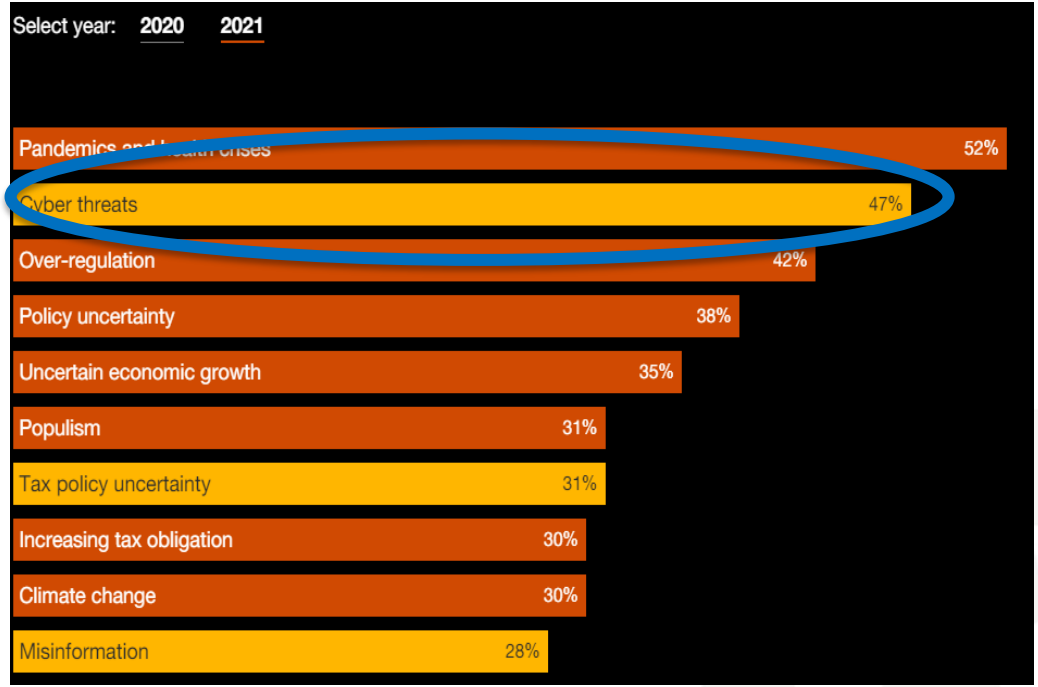
| Actor | Objetivo |
|---|---|
| Estados Naciones | ✓ Recolectar inteligencia<br>✓ Extraer datos de Exploración<br>✓ Interrumpir Operaciones<br>✓ Adquirir Activos Depreciados |
| Organized Cybercriminal Syndicates | ✓ Extraer y Vender Informacion Sensible y Confidencial<br>✓ Cifrar Archivos Sensibles para pedir Rescate (Ransomware)<br>✓ Cyber Ataques con motivacion Politica<br>✓ Agentes de Estados Naciones (desvinculacion plausible) |
| Competitors | ✓ Campañas de Cyber Ataques Destructivos<br>✓ Obtener una Mayor Participación en el Mercado<br>✓ Obtener Acceso a Propiedad Intelectual<br>✓ Extraer Datos de Exploración y Planes Futuros |
| Hacktivists | ✓ Demostrar capacidades técnicas en la comunidad y obtener reconocimiento<br>✓ Obtener beneficio económico |

# CEO concerns (1)

## How concerned are you about these potential threats?

(top 10 “extremely concerned” answers)



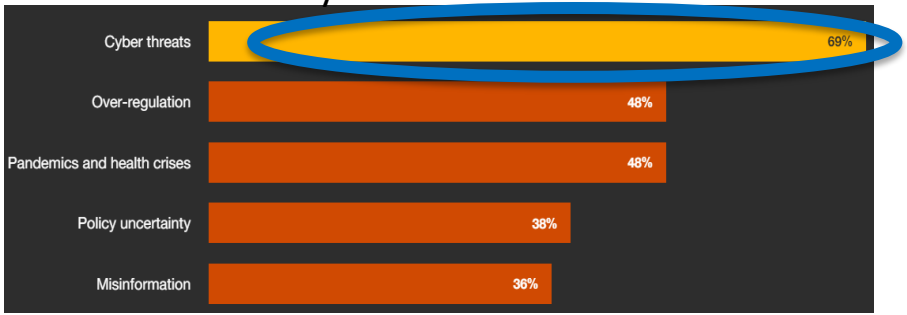

Source: PwC 24th Annual Global CEO Survey

# CEO concerns (2)

## How concerned are you about these potential threats?

(only “extremely concerned” answers)

North America: cyber threats = 69%




Asia-Pacific: 40%


Western Europe: 44%


Africa: 54%


Source: PwC 24th Annual Global CEO Survey

# CEO concerns (3)

## How concerned are you about these potential threats?

(only “extremely concerned” answers)


Source: PwC 24th Annual Global CEO Survey

# CEO Testimony

CEO David Rae: "…the mining industry hasn't traditionally considered the risks posed by threats on their IT systems or operational processes.

We realised how narrow our view was in terms of the risk and how much greater our response needed to be. As we began to understand the risks better, we undertook a cybersecurity maturity assessment that identified around 20 different items, filtered that down to eight priority areas, and then put together a plan to address them."

(Source: comments during a panel discussion, November 2020)

Dundee PRECIOUS METALS

# Mejorar la Postura de Cyber Seguridad (1)

1. La Alta Gerencia debe reconocer que las Cyber Amenazas representan un riesgo importante para la Organización
2. Formular un plan claro y preciso para administrar Cyber riesgos
3. Formular y dar prioridad a inversiones estratégicas de largo plazo para minimizar las amenazas mas importantes para la organización
4. Aplicar un marco de referencia reconocido para identificar las deficiencias de controles de cyber seguridad
5. Acelerar la creación de conciencia de los temas relacionados con el reconocimiento y adopción de procesos para la administración de cyber riesgos

# Mejorar la Postura de Cyber Seguridad (2)

- Engage cybersecurity services at the same time as buying cyber-physical equipment. Make cybersecurity part of the procurement process.
- Identify potential problems ahead by conducting vulnerability assessments. Do them regularly so that you can prioritize the mitigation of attack paths to critical assets and procedures.
- Look for cybersecurity solutions with real-time monitoring capabilities to detect malware, malfunctioning devices, and neglected firmware updates – as they happen.
- Cybersecurity solutions must offer operational visibility -- you can't secure what you can't see. Best solutions will offer a system inventory of all networked devices and ICS being monitored so that Corporate Security can determine what facilities are connected to their networks and who is active on their networks.
- A key step is to adopt a comprehensive cyber risk management program that addresses specific risks and includes a tested cyber-incident response plan.

THE ALRM GROUP

CANADIAN EXCELLENCE IN BUILDING INTELLIGENT CAPACITY

# Thank You!

info@thealrmgroup.ca www.thealrmgroup.ca