MINING AND METALS ISAC

MM-ISAC

Why Can’t We Be Friends

Healing the Rift Between the Business and Cyber

TLP: CLEAR

Rob Labbé

CISO-in-Residence
CEO

Safety Share – Responder Burnout

Major incidents are significant stressors. Your incident response plan must:

- Ensure sustainable hours with adequate rest (12 hours max, 16 potentially for short periods)
- Ensure sufficient food and beverages are available
- Positive management support
- Monitoring of employee mental health
- Ensure employee safety (Uber/Taxi home after long work periods)

Agenda

- cISO or CISO
- There is no “healthy tension”
- Building a Trusted Relationship

cISO or CISO

An Incident Review

cISO or CISO

- In many organizations, the CSIO is not like the other C-level executives
  - Struggle to get a seat at the executive and board table
  - Further down in the org chart
  - Not a part of the senior management team
  - Not an officer of the corporation
  - Less financial autonomy and decision-making
  - Not listed in D&O policy

- From the position of the executive team CISOs
  - Possesses deep technical expertise
  - Possesses risk assessment expertise
- But….
  - Struggle to communicate value of cyber investment
  - Struggle with aligning objectives to the rest of the company
  - Implementing controls and control frameworks with unexpected and unbudgeted business impact
  - Struggle to contribute to 80% of the conversations at the SMT

Examples - $5M project

VS

CYBERARK®

TLP
CLEAR

Justification

Truck @$5M

Truck Capacity (Short Tonnes)	380
Loads per day	4
Ore moved/day (Short Tonnes)	1520
Gold Recovered (4g/tonne) (oz)	195
Revenue ($2450/oz)	$ 478,917.52
Increased AISC ($1500/oz)	$ 293,214.81
Net Daily	$ 185,702.71
Annual (250 operating days)	$ 46,425,678.09

CyberArk

Licencing First Year	$ 1,500,000.00
Deployment Project	$ 1,000,000.00
Total Capital	$ 2,500,000.00
Ongoing Costs	
Annual Licence	$ 1,500,000.00
1.5 FTE $ $110,000	$ 165,000.00
Total Annual costs	$ 1,665,000.00
Total 3 year costs	$ 5,830,000.00

It is actually worse than that

Each of 12 mines experienced 3000 oz of lost production due to unplanned outage extensions caused by people not being able to access systems remotely quickly.

Cost = 3000* $2450 = $7,350,000 per site

= $88,200,000 in additional AISC

If the vulnerability were to be exploited – would it have cost $88M?

Licencing First Year	$ 1,500,000.00
Deployment Project	$ 1,000,000.00
Total Capital	$ 2,500,000.00
Ongoing Costs	
Annual Licence	$ 1,500,000.00
1.5 FTE $ $110,000	$ 165,000.00
Total Annual costs	$ 1,665,000.00
Total 3 year costs	$ 5,830,000.00

There is no such thing as “healthy Tension”

Don’t let a good incident go to waste

“Unhealthy Tension”

There is no healthy tension – only tension.

Erodes trust – Are operators likely to call you back?

Security Awareness – Fault and blame for engineering weaknesses

Excess process and fear – Restricts innovation

Objective and Values Mismatch

The root cause of this tension is objective values mismatch.

We behave according to our values first

- Ethics
- Trust
- Safety

We behave according to our objectives second

- Sense of accomplishment
- Supporting our boss/team
- Career Advancement
- Compensation

How bad can it get?

TLP
CLEAR

Building a Healthy Relationship

It starts with trust

Why are we here?

Resilience Prerequisites

Business/Cyber/IT objective and values alignment

A CISO that can function across Sectors – Owns Cyber Security but coordinates operational resilience and communications

Risk quantification and accounting of all losses due to security incidents, outages, and delay

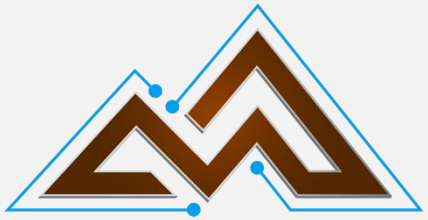
Resilient Cyber Security

- Control frameworks are guidance, not instructions
- Controls can, at best reduce the odds of an insurable cyber incident to 50%
- Blame and lack of accountability
- Account for and own all costs
- Work with how people naturally work
- Security is the CISO's responsibility, but we need everyone's help
- Policies that are outcome-based, not convenience based
- Resilience tied closely with operational resilience
- Solid, tested, rehearsed incident response plan.
- Backed by actionable intelligence

Operational Resilience

- The single biggest impact on risk reduction
  - The operation can continue for a period despite a cyber incident (or outage)
    - Can continue for 2x the estimated time to recover
    - Assumes failure of networks, applications and/or external services
    - Plan is documented and tested annually

Resilient Communication

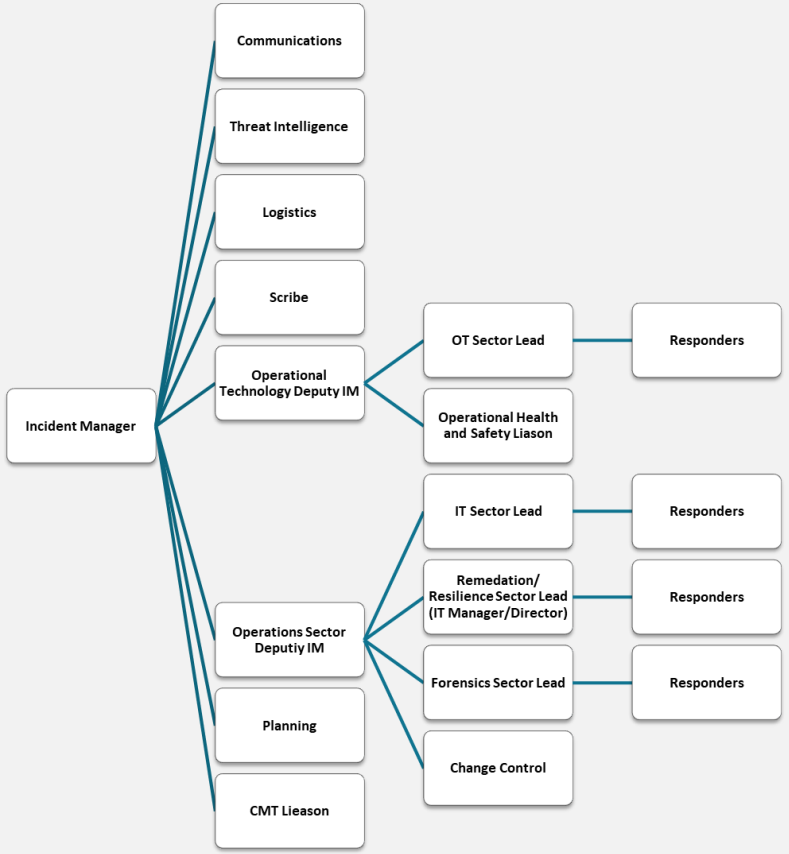


Have plans for how security will be communicated to all stakeholders

Have plans for incident disclosures

Effective Incident Response Plans

- Scale up to large global incidents and down to small incidents
- Provide for unity of command, clear communication and rapid decision-making
- Manageable span of control
- Clear roles and responsibilities
- But – only if people are trained and it is rehearsed

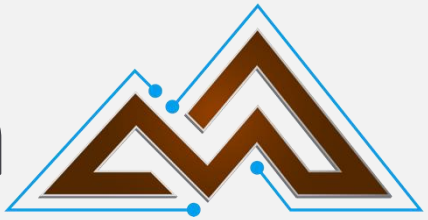


TLP CLEAR

Getting Started

Where do I start?

Build a Resilience Based Program

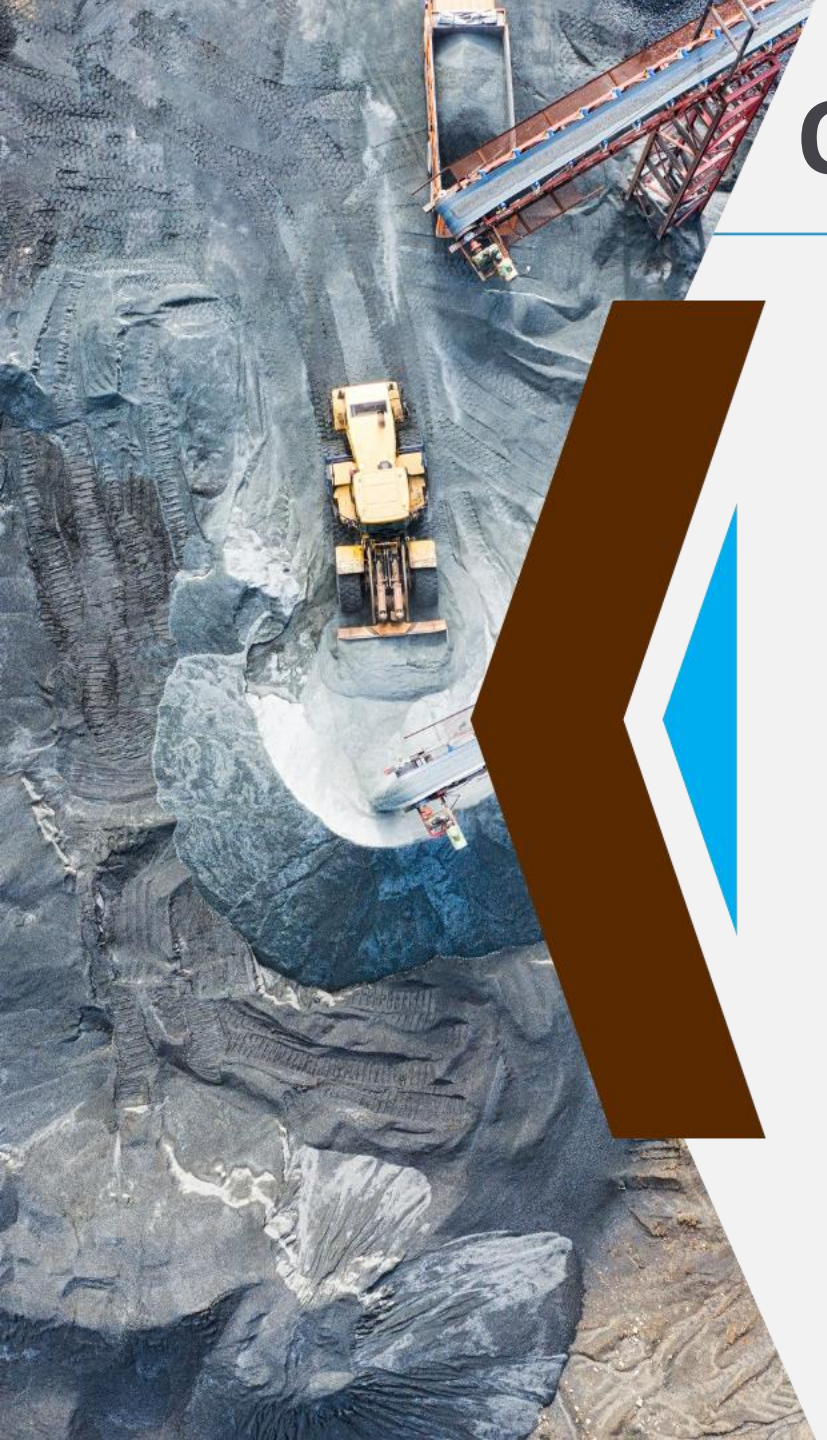


- Ensure airtight alignment between the cyber objectives and overall business objectives
- Fully cost the impacts of policies and controls
- Focus first on helping with operational resilience, as this will have the biggest risk impact.
- Build a rock-solid IRP that ties into BCPs, Communications, and Crisis plans.

Turn your c into a C

For a seat at the SMT – You need to contribute to 80% of the conversation.

- Most conversations have nothing to do with cyber risk
- Speak finance and business as a native speaker, not a tourist
- Learn the business domain



Questions

rlabbe@mmisac.org