Deloitte.

5x5 series: Insights and actions

Protecting mining operations from cybersecurity events

While it may be tempting for organizations to leverage out-of-the-box information technology (IT) cybersecurity controls to protect their mining operations, these can often be difficult to implement or not fit for the purpose in operational environments. Cybersecurity for mining requires a tailored, programmatic approach and focused attention from multiple stakeholder groups across the organization. This is increasingly important as more network connected equipment is being introduced to mining operations to unlock more efficient and effective operations.

***5** things you should know*		***5** actions you can take*
Secure supply chain and vendor risk management including contractors and system integrators should be considered by organizations looking to minimize interruptions to operations.	1	Implementing a **customized cybersecurity framework** to enable supply chain resilience and maintain continuous operations is needed. Adopting broad **vendor risk management strategies** is essential in safeguarding against potential vulnerabilities introduced through your extended supply chain as discussed in the most recent mining trends release, *"gaining agility and competitive advantage through next-gen approaches to outsourcing".*[1]
Secure network architecture and segmentation efforts should be an ongoing focus as mining organizations continue to add connected systems and devices to the operations environment in an effort to unlock additional business value.	2	IT and operational technology (OT) networks should be segmented from one another **to help prevent attackers from moving freely throughout a mining network.** Deploying a **secure remote access solution** helps to improve security and efficiency in mining operations. This can provide increased control over employees, contractors, and other support personnel who are accessing the environment remotely and reduces the risk of unauthorized access using an existing insecure remote access solution as the entry point.
Cybersecurity controls should be considered during the design and implementation of connected machines and OT/industrial internet of things (IIoT) devices as organizations continue to accelerate their technology strategy efforts.	3	**Cyber security acceptance testing (CSAT)** should be performed on OT and IIoT systems to confirm that the implemented controls meet the security requirements of the company and align with industry standards and leading practices. Protecting connected devices by implementing standardized profiles like port security and device hardening are important control measures**.**
Asset visibility, data security and cybersecurity monitoring within OT networks is becoming a fundamental control for organizations looking to identify indicators of compromise more promptly and efficiently.	4	OT network monitoring capabilities should **passively collect information** and active scanning should only be enabled when these networks (and their components) are well understood. OT network monitoring and asset visibility capabilities also enable organizations to identify vulnerabilities/risks at the device level and better prioritize their mitigation as noted in the most recent mining trend, *unlocking new value in existing assets.*[2] Crown Jewels and critical assets should be defined through an asset classification process to enable the organization to focus on the protection of assets that are critical to operations. Identity management programs focused on managing powerful accounts should be extended to Crown Jewels within the OT environments (i.e., acknowledging cyberattacks are rooted in access control in some way).
OT specific response and recovery planning should be a focus of a Cybersecurity Program. This should include periodic exercises to test response and recovery plans.	5	Personnel at the mines **should know who to call and when** during business disruptions**.** Plans should be documented and tested at set intervals to confirm personnel understand their roles/responsibilities. Backups of critical systems should also be available to enable recovery in the event that those systems need to be restored. Solutions for enabling these backups should be made available to sites and regular testing of backup restore capabilities should occur as seen in the mining trends release discussing disruption, *"building capacity to thrive in disruption".*[3]

1. Deloitte's report: Tracking the trends 2024; navigating global challenges and opportunities in mining and metals
2. Ibid.
3. Ibid.

Explore our **Cyber-Physical Systems (CPS) Security** services or contact us to learn more:

BRIAN CLARK
Partner | Deloitte & Touche LLP
bclark@deloitte.com

JASON HUNT
Principal | Deloitte & Touche LLP
jashunt@deloitte.com

JAKE MORELLA
Senior Manager | Deloitte & Touche LLP
jmorella@deloitte.com

SAURABH LOKHANDE
AVP, Solution Delivery | Deloitte & Touche Assurance & Enterprise Risk Services (India) Private Limited
salokhande@deloitte.com