



Cyber

¿Es la cyber-seguridad más que solo protección?

Debido al aumento del tamaño de la amenaza, las organizaciones están gastando más en cyber-seguridad, dedicando recursos adicionales para mejorar sus defensas y trabajando más arduamente para integrar la seguridad por diseño. Como la agenda de transformación digital obliga a las organizaciones a abrazar Tecnologías emergentes y nuevos modelos de negocio, a menudo a ritmo. La cyber-seguridad debe ser un habilitador clave del crecimiento.

Todas las organizaciones de minería y metales son digitales por defecto: en un mundo cada vez más conectado, el panorama digital es muy amplio, ya que cada activo que posee o utiliza una organización representa otro posible punto de entrada. Al mismo tiempo, nunca ha sido más difícil para las organizaciones entender y asegurar el entorno digital en el que operan, o sus interacciones con él como resultado, la superficie de ataque solo se está haciendo más grande entre los activos físicos, la infraestructura digital y los procesos de negocios; e incluso puede extenderse a las conexiones de una empresa con proveedores y clientes.

Por ejemplo, la incorporación de internet de cosas en equipos por parte de los proveedores de ingeniería extiende y difumina la "red perímetro". Los ataques pueden ser maliciosos o involuntarios; sin embargo, los impactos resultantes pueden ser similares, independientemente de la intención. Estos impactos incluyen interrupciones prolongadas y generalizadas, incidentes de seguridad, reclamos de responsabilidad y costos legales asociados, costos de limpieza de datos, daños a la reputación, distracción de la administración y daños físicos. Daño a los bienes.

54%

de las empresas de minería y metales ha tenido un incidente en el último año significativo de cyber-seguridad"

.Fuente: EY Global Information Security Encuesta 2018–19

Una estrategia innovadora de cyber-seguridad Basados en buenos principios de gestión de riesgos deben ser aplicados.

El foco debe estar en cómo la cyber-seguridad apoyará y permitirá el crecimiento empresarial. El objetivo debe ser integrar la seguridad en los procesos empresariales y crear un entorno de trabajo más seguro para todos. Para lograr estos objetivos, las organizaciones necesitarán una estrategia innovadora de cyber-seguridad basada en principios de buena gestión de riesgos.

Las compañías mineras y metalúrgicas necesitan comprender los riesgos comerciales, los activos críticos y los escenarios que plantean un evento de riesgo cibernético.

La cyber-seguridad efectiva requiere, en primer lugar, que la organización realice una revisión cibernética de referencia. Controles de evaluación de madurez. Esto es apoyado por un enfoque basado en el riesgo para priorizar los ciberestratégicos, a largo plazo, inversión para la amenaza cibernética superior. Entonces, es esencial aplicar un marco de seguridad cibernética para identificar las brechas críticas de control cibernético que deben cerrarse.

Cada transformación de la cyber-seguridad debe promover tres principios clave a través de la cultura, la gobernanza y las capacidades:

1. Espere excelencia en los fundamentos de seguridad: sea altamente maduro en Los "conceptos básicos de seguridad", practican una buena higiene de seguridad y optimizan las capacidades actuales de la solución de seguridad de la información.
2. Establecer un programa de gobierno sólido y una cultura de responsabilidad: esto debería incluir un progreso adecuado y Las métricas de rendimiento, el desarrollo de una cultura de seguridad y un cambio en la cultura para garantizar prácticas de seguridad como parte de las responsabilidades diarias de las personas.
3. Construir un compromiso de mejora continua: adaptarse a los nuevos requisitos basados en amenazas y tendencias en evolución, evaluar periódicamente la seguridad, postura para remediar las brechas, y recuerde que los roles de la estrategia cibernética y las responsabilidades son para todos en el a organización no importa cuales sean sus roles.