Boardroom Questions

Seguridad cibernética: ¿qué significa para el Consejo?

¿Por qué el riesgo cibernético debe ser considerado diariamente en las organizaciones?

Las compañías se encuentran bajo una presión constante por **adoptar** y desarrollar **nuevas tecnologías** para seguir siendo competitivas en sus mercados, mediante oportunidades para **diferenciar la experiencia del cliente**, reducir **costos operativos** y aumentar su **ventaja competitiva**.

Al mismo tiempo, los **inversionistas, gobiernos** y **reguladores** están desafiando constantemente a los miembros del Consejo para **demostrar activamente su diligencia** en esta área. Los reguladores esperan que la i**nformación personal esté protegida** y que los **sistemas sean resistentes**, tanto a posibles **accidentes** como a **ataques deliberados**.

Las organizaciones no pueden darse el lujo de ser detenidas por los riesgos cibernéticos. El Consejo y la Alta Dirección deben tomar decisiones firmes y confiar en que su **estrategia cibernética**, sus **defensas** y **capacidades de recuperación** protegerán el negocio y respaldarán los objetivos sustentables de **crecimiento** de la compañía.

Cuestiones clave: ¿por qué las compañías deben considerar reevaluar su estrategia cibernética?

La presión por encontrar **nuevos clientes** y competir con **empresas disruptivas** da como resultado que la mayoría de las compañías estén implementando tecnología digital (robótica, inteligencia artificial, movilidad e introducción de nuevos sistemas), que **expone constantemente sus datos**

Ante un panorama de amenazas cambiante, en el que un creciente número de **atacantes profesionales están innovando más rápido que muchas compañías, las organizaciones podrían mejorar sus defensas**

Restaurar la confianza y minimizar posibles **daños a la reputación** de la empresa es clave para muchas industrias, pues una violación de los datos podría afectar ambos factores, así como el **valor de las acciones**

Impacto potencial y posibles implicaciones para el Consejo

Pérdidas de propiedad intelectual, que incluyen material patentado y de marca registrada, listas de clientes y datos comerciales sensibles.

Sanciones, que pueden ser legales o normativas, por violaciones a la privacidad de datos, compensación a los clientes y contractuales, o por demoras.

Pérdida de bienes en acciones o información que provoque demoras o fallas en su entrega.

Pérdida de reputación que provoca que el valor de mercado de la compañía disminuya; pérdida de plusvalía y confianza por parte de clientes y proveedores.

Tiempo desperdiciado en investigar las pérdidas, mantener a los accionistas informados y respaldar a las autoridades (financieras, fiscales y legales).

Recursos administrativos para corregir el impacto: restaurar la confianza del cliente, comunicación con las autoridades, reemplazar propiedades y restaurar la organización a sus niveles anteriores.

Boardroom Questions

El nivel de conciencia del Consejo sobre las amenazas cibernéticas crece, y su participación directa en la determinación de respuesta es crítica. La ciberinteligencia puede ayudar a las organizaciones a volverse más proactivas, enfocadas y preventivas para tomar el control del riesgo de una manera única y positiva.

1. ¿Cuáles son las **nuevas amenazas** y riesgos de ciberseguridad, y cómo afectan a la organización?
2. ¿**El programa de seguridad cibernética** de la empresa está listo para enfrentar las amenazas actuales y del mañana?
3. ¿Entendemos completamente nuestras **vulnerabilidades actuales** y qué **procesos** tenemos implementados para enfrentar las amenazas cibernéticas?
4. ¿Qué **indicadores clave** deben revisarse a nivel directivo y de Consejo para realizar una gestión de riesgos efectiva?
5. ¿La organización cumple con todas sus obligaciones y garantías sobre la **privacidad de la información**, tanto locales (LFPDPPP) como internacionales (GDPR)?
6. ¿La ciberseguridad forma parte de los **temas estratégicos** del Consejo? ¿Cuándo fue la última vez que se examinaron las amenazas cibernéticas que enfrenta el negocio?
7. ¿Cómo pasamos de **reaccionar a anticipar** los ataques cibernéticos?
8. ¿Nos lleva la delantera la **competencia**? Si es así, ¿les da esto una **ventaja competitiva**?

Preguntas para la Alta Dirección

1. ¿Cómo estamos **demostrando** el trabajo adecuado, la responsabilidad y la **gestión eficiente de los riesgos**?
2. ¿A qué nivel hemos creado una **cultura de seguridad** en la organización que **faculta y garantiza** al capital humano con habilidades y conocimientos adecuados para enfrentar amenazas cibernéticas?
3. ¿Qué tan efectivo es nuestro enfoque para lograr una **gestión de riesgo de la información integral y efectiva** en la compañía, considerando a los *stakeholders*?
4. ¿Estamos **preparados** para un suceso de ciberseguridad? ¿Cómo podemos **prevenir o minimizar el impacto** mediante gestión de crisis, incluyendo a los *stakeholders*?
5. ¿Qué **medidas de control** tenemos para afrontar los riesgos identificados y qué tan **efectivas** son para prevenir o minimizar el impacto?
6. ¿Tenemos un **entendimiento claro del entorno legal y normativo** en el que operamos? ¿Cómo demostramos efectivamente el **cumplimiento** en nuestra cadena de suministro, nuestros clientes y socios comerciales?

¿Qué acciones debe considerar el Consejo?

Es necesario desarrollar una estrategia que vaya más allá de la ciberseguridad, combinando el talento corporativo, la privacidad, el control de la información y la resiliencia comercial. Las preguntas propuestas en este documento contribuirán a identificar qué hace falta en la estrategia actual. El área de Cyber Maturity Assessment (CMA) de KPMG cuenta con profesionales especializados en proporcionar revisiones profundas con respecto a la capacidad y madurez de su organización para proteger los activos de información y conocer su nivel de preparación ante las ciberamenazas, incluyendo:

- Liderazgo y gobernabilidad
- Factores humanos
- Administración de riesgos de la información
- Continuidad del negocio
- Operaciones y tecnología
- Área legal y de cumplimiento

KPMG

BOARD LEADERSHIP CENTER MEXICO

Acerca de KPMG Board Leadership Center

Es un programa global con presencia local exclusivo para miembros del Consejo de Administración en México, que tiene como objetivo promover un gobierno corporativo efectivo para impulsar el valor de la empresa a corto, mediano y largo plazo, generando confianza en los *stakeholders* de las organizaciones.

kpmg.com.mx
01 800 292 KPMG (5764)
blc@kpmg.com.mx

KPMG MÉXICO @KPMGMEXICO KPMGMX KPMG MÉXICO