Rol del directorio en la gestión de los riesgos informáticos

Marcelo Zanotti
Socio líder de Consultoría en Riesgo de EY Chile

Es importante analizar los desafíos de los directorios en estos tiempos de ciberataques y delitos informáticos. Los directores deben involucrarse en las decisiones tecnológicas de sus empresas y contar con una visión crítica al respecto, no dejando toda la responsabilidad a sus CIO o gerentes de TI.

El mundo digital ofrece un potencial enorme para la creación de nuevos mercados y productos. Sin embargo, este nuevo escenario nos enfrenta a riesgos informáticos cada vez más complejos. Para cada organización los riesgos son distintos dependiendo del negocio, pero el efecto es el mismo; un daño reputacional y económico que puede afectar, incluso, la continuidad operativa de la empresa u organización. Es por este motivo que la seguridad cibernética se ha convertido en una prioridad para los directorios, que desean estar mejor informados, tener un rol activo en materias de ciber riesgos y saber las preguntas correctas que deben formularse para no quedarse atrás en materia digital.

Dada la frecuencia, magnitud y costo de los incidentes de seguridad cibernética, hoy se considera que es fundamental que las empresas y organizaciones tomen todas las medidas necesarias para informar a los inversionistas sobre los riesgos e incidentes de ciberseguridad de manera oportuna, sobre todo aquellas compañías que están sujetas a riesgos importantes de ciberseguridad por su core business o por la cantidad de información que manejan, pero que aún no hayan sido el objetivo de un ciberataque.

"Según nuestra perspectiva, existen dos tipos de empresas: las que serán atacadas en alguna medida por ciberdelincuentes y las que ya lo fueron. Esto es lo que sucede al integrarse de forma activa al mundo digital, por lo que el punto inicial para ganar esta batalla es entender cómo se ve la organización frente a un ciberatacante", explica Marcelo Zanotti, socio líder de Consultoría en Riesgo de EY Chile.

En la actualidad, prácticamente todas las empresas son digitales por defecto y, según los últimos estudios del Foro Económico Mundial, la brecha de ciberseguridad supone uno de los cinco mayores riesgos que afronta el mundo. Existen informes que estiman el costo global de la ciberseguridad en US$ 6 billones para 2021, el doble del registrado en 2015, y el impacto para las organizaciones es tanto económico como reputacional.

Lo anterior lo confirma el estudio Global Information Security Survey (GISS) de EY. El reporte, en el que han participado responsables de TI de aproximadamente 1.200 grandes empresas en todo el mundo, pone de manifiesto que la ciberseguridad debe ser una prioridad a todos los niveles y que la mayoría de las compañías considera que el riesgo de sufrir hoy un ciberataque es mayor que hace un año, ya que las técnicas de los ciberdelincuentes son más sofisticadas, mientras que las corporaciones están más conectadas que nunca. Las oportunidades que ofrece la digitalización son muy grandes a lo largo de la cadena de valor, pero también lo son los riesgos informáticos.

En nuestro país, los desafíos y riesgos en ciberseguridad son similares a los mencionados anteriormente a nivel mundial. Ya es conocido por todos que Chile es susceptible de sufrir ciberataques. En este contexto, y de acuerdo a la encuesta "Principales desafíos de las empresas en Chile" de EY Chile, realizada este año a más de 200 ejecutivos de las principales firmas nacionales, la seguridad cibernética se encuentra entre las tres tecnologías disruptivas a incorporar entre los próximos tres y cinco años. Las otras dos son e-commerce y Big Data.

LAS CINCO CLAVES DE LAS EMPRESAS EN CIBERSEGURIDAD

ROL DEL DIRECTORIO EN LA CIBERSEGURIDAD

Los directorios deben comprender los avances de la tecnología y digitalización dentro de las empresas y es por esto que deben estar al tanto de los factores claves que pueden tener un impacto en la estrategia corporativa, incluyendo cambio tecnológico, innovación y tecnologías emergentes. Por ejemplo: inteligencia artificial, automatización y blockchain. Al supervisar las estrategias digitales, los directorios también deben considerar cómo la tecnología está alineada con el propósito de la empresa y respaldar los objetivos del negocio y de los clientes e inversionistas, integrando la seguridad en cada etapa, con el fin de tener una modernización tecnológica, donde se consoliden todos los sistemas.

A medida que las empresas se alinean en base a un modelo tecnológico, frente a un propósito y a la experiencia del cliente, los directorios deben comprender de mejor manera la rápida evolución del escenario digital, para servir como un socio estratégico de la administración. Esto puede requerir un replanteamiento de la composición del directorio, además de su estructura y diseño y frecuencia de las reuniones.

Desde el punto de vista de EY, los directores deberían considerar los siguientes aspectos:

Directores digitales. Los directorios deben considerar la mejor forma de asegurarse de que los desafíos digitales y tecnológicos sean los adecuados a las circunstancias y características de su empresa, ya que cada empresa tiene sus particularidades y debilidades cibernéticas diferentes.

Comités de tecnología. Algunos expertos recomiendan la formación de comités formales, al interior del Directorio, que se reúnan sólo para ver iniciativas estratégicas centradas en la tecnología y los riesgos que puede sufrir la organización.

Aumento de la frecuencia de las reuniones y con foco en la estrategia. Los directorios deberían reunirse con mayor frecuencia con los CIO. En la actualidad deben ser un socio estratégico de la administración y para la supervisión de la estrategia digital de la empresa, hay que ir mucho más allá del cumplimiento, por lo que a veces se debe desafiar o tener una visión crítica de lo que está haciendo actualmente el departamento de TI y su CIO.

"En consecuencia, los directorios deben jugar un rol activo en la ciberseguridad de las empresas, contar con la información apropiada para supervisar los riesgos de ciberataques y analizarlos con la administración, incluyendo la forma en que estos riesgos son identificados, informados a inversionistas y autoridades y evaluados en el contexto de las actuales, y cada vez más complejas, amenazas de ciberseguridad, que cada día evolucionan y se perfeccionan en favor de los ciberdelincuentes", detalla el socio líder de Consultoría en Riesgo de EY Chile.

Para concluir, Marcelo Zanotti añade que "los directores deberían contar con algún conocimiento o expertise en los temas digitales para enfrentar de mejor manera los actuales desafíos y riesgos informáticos. Hoy no es común ver estas capacidades en la mayoría de los Directorios".

PREGUNTAS CLAVES PARA LOS DIRECTORIOS

Tips

¿Cuentan con los controles y procedimientos que proporcionen un "sistema de alerta temprana" que permita a la compañía identificar, evaluar, abordar y hacer divulgaciones oportunas sobre los riesgos e incidentes de ciberseguridad?

¿Ha considerado el consejo una evaluación independiente del proceso de gestión del riesgo de ciberseguridad de la compañía, y los informes relacionados para ayudar a garantizar que los procesos sean apropiados y sólidos?

¿El directorio entiende cómo se integra el programa de gestión de riesgos de ciberseguridad en el programa general de gestión de riesgos empresariales de la empresa¿ y ¿son adecuadas las líneas de denuncia para el personal de cumplimiento (por ejemplo, el director de seguridad de la información) que tienen la responsabilidad de supervisar los riesgos de ciberseguridad?

OPINIÓN

Fernando Larraín

Gerente general de la Asociación de AFP

"Una correcta estrategia es un proceso central para una compañía"

En un mundo complejo y dinámico, en donde los usuarios y clientes son cada vez más exigentes y desconfiados, el rol del directorio es clave. El desarrollo de una correcta estrategia es un proceso central para una compañía, no solo porque define su futuro sino también porque es un ejercicio que genera una cultura dentro de ella.

El directorio, entre otras funciones, debe tener la capacidad de identificar los puntos de conflicto entre los grupos de interés con el objeto de reducir el riesgo y construir una oferta de valor relevante. Considerar en las juntas de accionistas a los minoritarios y/o extranjeros para que puedan ejercer su opción de votación remota y que la información corporativa a la que se tenga acceso sea completa y oportuna, generando y construyendo un camino de confianza con los inversionistas es un proceso cada vez más necesario.

En este sentido la incorporación de directores independientes podría permitir la disminución de la acumulación de poder dentro de la empresa. Los directores independientes tienen como misión, al igual que cualquier otro director, trabajar en función de los objetivos y el bien de la compañía y al no tener compromisos o vínculos con ningún grupo específico de poder tiendan a actuar de manera más objetiva.

El desafío es llegar a no preocuparse únicamente de la última línea, sino que elaborar una hoja de ruta que permita lograr entornos estables, inclusivos y transparentes que aseguren una continuidad sana para los negocios, el mercado y las comunidades en el largo plazo.