Control del Ciberriesgo:

Principios clave y orientaciones prácticas para los Consejos de Administración de las empresas en Europa

Resumen

La ciberseguridad es la amenaza que más rápido crece, y quizás la más peligrosa, a la que se enfrentan las organizaciones actualmente. En los Consejos de Administración se está prestando cada vez más atención a la lucha contra estas amenazas.

Los manuales de la ASI sobre ciberriesgo (también disponibles en EE.UU., Reino Unido, Japón y Latinoamérica) tienen por objeto proporcionar a los miembros del Consejo un marco sencillo y coherente para comprender el ciberriesgo, así como una serie de preguntas sencillas para que los Consejos puedan plantear a la Dirección con el fin de garantizar que su organización aborde adecuadamente su postura específica en materia de ciberriesgo.

El manual, el cual ha sido elaborado conjuntamente por la ASI, Ecoda y AIG, promoverá la aplicación permanente de principios de ciberseguridad homogéneos en los Consejos de Administración de las empresas, no solo en Europa sino en todo el mundo. A continuación, se muestra un resumen de los cinco principios para la gestión del ciberriesgo, junto con las principales recomendaciones y enlaces a herramientas prácticas.

Puede consultar el manual completo aquí

Principio 1

Los administradores deben entender y enfocar la ciberseguridad como una cuestión de gestión de riesgos en toda la empresa, no solo como una cuestión de TI.

Recomendaciones clave:

- La seguridad de la información no debe considerarse como una cuestión puramente técnica a cargo del departamento de informática;
- La ciberseguridad debe concebirse como una cuestión de gestión de riesgos en toda la empresa durante todo su ciclo de vida;
- El control de los riesgos debería ser una función de todo el Consejo;
- El Consejo no debe basarse en un enfoque único, sino que debe definir sus propios planes específicos;
- El Consejo debe implementar una cultura adecuada dentro de la empresa para garantizar que todos los empleados consideren la ciberseguridad como una cuestión importante;
- La Dirección debe poner a disposición del Consejo de Administración toda la información relativa a la capacidad de prevención, detección y respuesta, así como el grado de madurez en el que opera la empresa. Al hacerlo, la Dirección no debe considerar solo las propias redes de la organización, sino su entorno exterior.

Herramientas

Kit de herramientas A para las preguntas recomendadas que deben incluirse en la revisión y autoevaluación del Consejo con el fin de ayudar a evaluar el nivel de comprensión del Consejo sobre las cuestiones de ciberseguridad o cultura cibernética

Kit de herramientas B para una lista de preguntas de ciberseguridad que los administradores pueden plantear a la Dirección sobre temas como la estrategia, la evaluación de riesgos, las medidas de prevención, los incidentes, la respuesta a los incidentes y la respuesta y comunicación posteriores a las infracciones

Kit de herramientas C para las preguntas pertinentes que los administradores pueden hacer para promover una medición óptima del rendimiento y la presentación de informes

Kit de herramientas D para las consideraciones de ciberseguridad relacionadas con las fusiones y adquisiciones

Kit de herramientas E para las referencias a las normativas internacionales

Principio 2

Los administradores deben entender las implicaciones legales y para la reputación que conllevan los ciberriesgos, en lo que se refiere a las circunstancias específicas de su empresa.

Recomendaciones clave:

- La ciberseguridad no solo se refiere a cuestiones ligadas a la reputación, sino también a la responsabilidad de los miembros del Consejo;
- Los miembros del Consejo deben conocer en profundidad las legislaciones existentes a nivel europeo o nacional, o incluso las específicas de la industria, para poder ejercer adecuadamente su deber de cuidado.

Principio 3

El Consejo de Administración debe garantizar un acceso adecuado a los conocimientos técnicos en materia de ciberseguridad, así como la presentación oportuna de informes, tanto a nivel del Consejo como de los Comités.

Recomendaciones clave:

- Los miembros del Consejo deben aplicar los mismos principios de investigación y reto constructivo que en el caso de las decisiones estratégicas;
- El Consejo debe especificar con precisión sus expectativas a la Dirección y orientar sobre el tipo de información que desea recibir;
- Incluso si la ciberseguridad se confía a un Comité específico, el Consejo en su totalidad debe involucrarse y obtener, al menos, informes trimestrales de la Dirección;
- La seguridad cibernética no debe tratarse como un tema aislado, sino que tiene que estar integrada en todas las dimensiones de la estrategia de la empresa.

Herramientas

Kit de herramientas B para los aspectos sobre las organizaciones y el equipo de gestión de ciberriesgos

Kit de herramientas C para posibles preguntas y ejemplos de métricas de informes e indicadores sobre ciberriesgos

Principio 4

El Consejo de Administración debe asegurarse de que la Dirección establezca un marco de gestión del ciberriesgo en toda la empresa que abarque la cultura, la capacidad de prevención, detección y respuesta, el control y la comunicación a todos los niveles.

Los recursos deben ser adecuados y se deben asignar apropiadamente mediante las estrategias adoptadas.

Recomendaciones clave:

- La Dirección debe establecer tanto un marco técnico para toda la empresa (dispositivos móviles, IA, ...) como un marco sistemático (con un enfoque de futuro) que facilite el control del ciberriesgo por parte del Consejo;
- La Dirección debe adoptar un enfoque integrado del ciberriesgo a fin de establecer un marco claro de responsabilidades, así como procesos bien definidos y directrices de comunicación;
- La Dirección debe optar por un enfoque de agregación ascendente;
- El Consejo y la Dirección deben marcar el ritmo al más alto nivel e implementar una cultura adecuada, así como aumentar la concienciación, para lograr la ciberresiliencia.

Principio 5

La deliberación del Consejo sobre el ciberriesgo debe incluir las estrategias para su gestión (mitigación, transferencia a través de seguros o asociaciones, etc.).

Recomendaciones clave:

- El Consejo debe considerar el rendimiento de las inversiones cibernéticas y adoptar un enfoque basado en el riesgo;
- La ciberseguridad debe ser conceptualizada como una forma de medir las pérdidas futuras.

Para obtener más información sobre el manual, póngase en contacto con Internet Security Alliance o sus contactos locales de AIG.

Mark Camillo
Head of Cyber, EMEA
AIG
T +44 (0)20 7651 6304
M +44 (0)78 6026 1692
mark.camillo@aig.com

Sebastian Hess
Cyber Risk Advisor, EMEA
AIG
T +49 69 97113-572
M +49 159 04611288
sebastian.hess@aig.com

Larry Clinton
President
Internet Security Alliance
T (001) 703-907-7090
lclinton@isalliance.org

Béatrice Richez-Baum
Director General
ecoDa
T +32 2 231 58 11
M +32 498 502687
beatrice.richez-baum@ecoda.org