RISK DOCTOR PARTNERSHIP BRIEFING

GESTIONAR EL RIESGO DE LA CIBERDELINCUENCIA

© Mayo 2014, Ben Rendle

ben.rendle@rioscaconsulting.co.uk

La ciberdelincuencia está creciendo rápidamente amenazando a la economía global. Pero no está bien definida, y a menudo se confunde con la ciberguerra o el ciberterrorismo. Los profesionales del riesgo necesitan entender que la ciberdelincuencia está relacionada con la gestión de riesgos, tanto en cuanto nosotros podemos proporcionar una ayuda valiosa haciendo frente a esta amenaza significativa para el negocio y para la sociedad.

Algunos profesionales del riesgo piensan que la ciberdelincuencia es solo relevante para las personas técnicas y que debería ser abordado por los departamentos de TI. Pero la ciberdelincuencia representa un riesgo significativo para las organizaciones porque afecta a su habilidad para alcanzar objetivos estratégicos y operativos. Desafortunadamente muchos negocios no saben lo que significa la ciberdelincuencia, cómo es de probable que sean afectados, cuál podría ser la extensión del impacto, o cómo gestionarlo mejor.

La ciberdelincuencia puede afectar a una organización de muchas formas diferentes, incluyendo:

- robo o fraude en línea
- robo de identidad
- extorsión
- robo de datos de cliente
- robo de propiedad intelectual
- espionaje industrial

La exposición a la ciberdelincuencia está relacionada con el nivel de actividades “on-line” llevadas a cabo por una organización, incluyendo el alcance de su presencia ”on-line”, el grado en el que activos valiosos e información son almacenados “on-line”, la fortaleza de la seguridad ”on-line”, y el grado de concienciación del riesgo en la cultura organizativa.

Para gestionar el riesgo de la ciberdelincuencia, debemos primero identificar el nivel de nuestras actividades “on-line”, y determinar qué activos y actividades podrían ser afectados. Entonces podemos empezar a identificar, evaluar y gestionar nuestros ciberriesgos. Los pasos siguientes serán de ayuda:

- **Entender y definir claramente los objetivos organizativos para las actividades ”on-line”.** Reconocer los entornos diferentes y específicos “on-line” de nuestros interesados, y evaluar sus apetitos de riesgo.
- **Direccionar factores tanto culturales como técnicos**. Estos incluyen barreras culturales, dificultades en la comunicación, y los efectos de los prejuicios en las percepciones del ciberriesgo.
- **Reconocer las amenazas del ciberdelito tanto internas como externas.** Las amenazas internas pueden surgir de los errores de los empleados, de la pérdida accidental de datos, o de filtraciones maliciosas de datos corporativos confidenciales. Las amenazas externas podrían venir de piratas informáticos, grupos de presión, competidores o incluso gobiernos extranjeros hostiles, así como virus, infiltraciones, troyanos etc.
- **Establecer responsabilidad, control e incentivos para direccionar ciberriesgos.** Todo el personal senior debería de ser responsable de gestionar el riesgo cibernético en su área de responsabilidad, y deberíamos desafiar a los interesados que “no lo ven como su problema”.
- **Gestionar los ciberriesgos dentro del marco (ERM).** Los ciberriesgos pueden afectar a la empresa entera en áreas tales como la reputación, la continuidad del negocio y el efecto “edad” de las delegaciones y suministradores, de forma que necesite enfrentarse de *una forma coherente como parte de nuestra respuesta global al riesgo.*
- **Desarrollar una perspectiva global del impacto del riesgo de los delitos informáticos.** Muchas organizaciones dependen de la economía del extranjero para el comercio, las exportaciones y la generación de salud, y esto les expone a los delitos informáticos en el extranjero que no se pueden ignorar.

Como profesionales del riesgo, necesitamos incluir el ciberdelito en nuestro pensamiento y práctica, de forma que podamos ofrecer un consejo práctico a nuestras organizaciones para reducir la amenaza y proteger nuestro negocio.
