www.mexis.net

HABLANDO DE RIESGOS OPERATIVOS Y TECNOLÓGICOS PODEMOS JUSTIFICAR GASTOS EN CIBERSEGURIDAD

mexis aggity

Últimamente he escuchado que, con implementar tecnología, es suficiente para poder evitar un ciberataque; sin embargo, no se considera que, por más tecnología, si no contamos con procedimientos claros y auditados, aún así puede pasar.

Cuando se ha tenido un incidente en temas de ciberseguridad, después de atenderlo, se busca si fue un problema técnico o de operación.

Dos términos que a menudo surgen en las estrategias de defensa corporativa son **“riesgo operativo” y “riesgo tecnológico”**. Comprender cómo cada uno afecta a nuestra organización es crucial para más que la simple protección de activos: **es fundamental para la supervivencia y el crecimiento estratégico.**

El riesgo operativo encapsula las **pérdidas potenciales derivadas de fallos en procesos internos, errores humanos y cualquier evento que pueda perturbar las operaciones diarias.** Consideremos el caso de un empleado en una organización que, por un descuido, envía información sensible a un contacto incorrecto.

Este error, aparentemente menor, puede desencadenar consecuencias devastadoras, como la **exposición de datos confidenciales o personales, acciones legales severas y un deterioro significativo en la confianza del cliente** que puede ser difícil, si no imposible, de recuperar.

Por otro lado, **el riesgo tecnológico se centra en las amenazas vinculadas con fallos o mal uso de la tecnología** que respalda las operaciones de la empresa. Un ejemplo de esto es un ataque de ransomware que paralizó los sistemas de una importante empresa de logística, deteniendo la distribución de mercancías y generando pérdidas económicas astronómicas. Este tipo de riesgo hace hincapié en la **importancia de mantener sistemas actualizados y protegidos contra cualquier forma de vulnerabilidad cibernética.**

La complejidad del riesgo tecnológico y operativo se puso de manifiesto en el caso de Target en 2013, cuando un código malicioso instalado en los sistemas de punto de venta de la cadena permitió a ciberatacantes acceder a los datos de 40 millones de tarjetas de crédito y débito.

A pesar de recibir múltiples alertas de seguridad que indicaban la presencia del código malicioso, estas fueron inicialmente descartadas como falsos positivos. **Este error crítico de evaluación permitió que el problema escalara enormemente, transformando un riesgo tecnológico inicial en un desastre operativo** al impactar directamente las operaciones de la empresa y su reputación en el mercado.

Entender la distinción y la interrelación entre estos riesgos es invaluable para cualquier director o consejero. **Al comprender que los riesgos tecnológicos pueden manifestarse rápidamente como riesgos operativos si no se gestionan adecuadamente,** los líderes pueden abogar por y asignar recursos a programas de ciberseguridad más robustos.

La claridad en estos términos permite a los ejecutivos de alto nivel priorizar la ciberseguridad no solo como una necesidad técnica, sino como una imperativa estratégica de negocio.

Para un CISO o un responsable de ciberseguridad, utilizar estos términos en comunicaciones con la alta administración puede ayudar a clarificar por qué la inversión en tecnología y en prácticas de seguridad es crucial. Al enmarcar los riesgos tecnológicos y operativos en términos de impacto potencial sobre la continuidad del negocio y la reputación corporativa, el CISO puede hacer que la ciberseguridad resuene como una prioridad en la agenda de la dirección.

Esta estrategia de comunicación no solo asegura la atención de la alta dirección, sino que facilita la obtención de los recursos necesarios para fortalecer la postura de seguridad de la empresa.

A todo esto, no olvidemos que, aunque podemos hacer todos los esfuerzos para prevenir, también es importante saber cómo reaccionar. En algunos de los **Tabletops Ejecutivos de Ciberseguridad (Simulaciones de Ciberataques)** que son ejecutados con los directores de la organización, es muy común que se piense que, ante un ciberataque, es responsabilidad completamente de TI y ciberseguridad.

Agradezco que estos ejercicios que hemos ejecutado permiten concientizar a la alta administración de la responsabilidad operativa cuando no está disponible un sistema de información y de que se puede trabajar de forma proactiva para que ese momento esté coordinado de tal forma que se regrese a la operación lo antes posible.

Hablar de riesgo operativo y riesgo tecnológico puede ayudar a toda la organización a ser coparticipe de las actividades para evitar que algo malo suceda.

Autor: Andrés Velázquez
Fuente de información: www.forbes.com.mx