

5 Consejos para administrar la seguridad en una recesión

A medida que la compañía ajusta el presupuesto severamente en una economía difícil, ¿puede la seguridad manejar los riesgos e incluso ser un facilitador de los negocios? Art Coviello, Presidente de RSA, le da a CSO algunos consejos.

En la actual economía en bajada, muchas compañías están recortando costos y los gastos de seguridad frecuentemente son parte de la ecuación cuando se considera donde ahorrar o gastar dinero. (Lea: IT Security Spending Up for Some) Un nuevo estudio publicado por RSA, la división de seguridad de EMC, reunió la experiencia de diez grandes compañías con ejecutivos dedicados a la seguridad y operaciones y les preguntó: ¿cómo se puede administrar la seguridad e incluso hacer que impulse la innovación con la actual economía en baja?

CSOs y CISOs de compañías tales como Cigna, eBay, Motorola y JP Morgan Chase dan su perspectiva de cómo abordar los desafíos de los costos y, en algunos casos, incluso sostener la inversión de seguridad cuando los negocios están hartos de gastar.

Art Coviello, presidente de RSA, nos da una visión general de los cinco puntos principales del estudio.

Priorizar basado en riesgo/beneficio En el actual clima económico. Algunos riesgos puede que no valgan la inversión, según el estudio, el cual aconseja a las empresas que sepan como priorizar. Las decisiones en los gastos no solo deben tener en cuenta donde están los mayores riesgos, sino también donde se pueden encontrar las mayores oportunidades.

El informe, titulado "Manejando rápido y hacia adelante: Administrando la Seguridad de la Información para una Ventaja Estratégica en una Economía Difícil," también sugiere que juicios difíciles serán inevitables a medida que las organizaciones resuelven que riesgos deben ser atendidos inmediatamente y cuales no vale la pena el costo. Coviello señaló como ejemplo a un gran banco cliente. El banco ha invertido en la adaptación de una solución de RSA para reducir el fraude, pero estaba costando 2 millones de dólares por año operarlo con todo lo que Coviello denomina "los detalles y opcionales posibles."

"La pregunta fue si valían la pena los 2 millones de dólares de costo por este riesgo y la respuesta fue no," dijo.

El informe también sugiere cambiar el foco de la implementación de las últimas tecnologías de seguridad hacia un enfoque de seguridad convergente en las áreas hacia donde van los negocios.

"Estará probablemente mucho más buscando fondos para sus esfuerzos de administración de riesgos si puede demostrar que sus controles de seguridad tratarán múltiples áreas de riesgo a la vez," afirma el informe. "Por ejemplo, conociendo quien accede a cuales sistemas puede ayudarlo a prevenir el fraude."

Tener la mezcla apropiada de gente en su equipo En la medida que los presupuestos son recortados, a menudo también se recorta el personal. Ahora, más que nunca, tener a los mejores es esencial.

"Tener a la gente correcta en el corazón del equipo de seguridad es más importante que nunca porque deberá apoyarse en ellos más aún," dice el informe. "Los miembros del equipo central de seguridad necesitan tener un estado de ánimo de premios y castigos y un conjunto de habilidades excepcionales."

Coviello también sugiere reutilizar gente para evitar despidos y para una estrategia más eficiente. Es fue recientemente el caso en RSA cuando un administrador de incidentes y eventos permitió mayor automatización de eventos. El personal que antes estaba a cargo de las tareas que ahora se automatizaron, fueron reasignados. "No despedimos a esa gente. En lugar de aumentar nuestro costo base en 25 por ciento pudimos mantenerlo plano.," dijo Coviello.

Construir procesos repetibles Crear formas estandarizadas de hacer las cosas puede ser el camino largo hacia crear eficiencias, dice el informe. Unidades de negocio diferentes suelen tener diferentes forma de hacer las mismas cosas. ¿No podría cambiarse para hacer que la seguridad funcione de forma más eficiente?

Coviello señaló que a lo que se refiere el informe es a "la fruta que está a la mano", para conseguir eficiencias más fácilmente, tales como en la administración de identidad y de acceso. ¿Necesita realmente cada división, por ejemplo, un mecanismo diferente de requerimiento de identificación, o un sistema diferente de administración de accesos privilegiados?

"Un punto clave es, no reinvente la rueda," dice Roland Cluthier, CSO de EMC Corp., en el resumen del estudio. "Hay oportunidades increíbles a lo ancho de toda empresa de aprovechar los recursos de otros grupos para reducir el costo de asegurar la protección de una compañía. Puede ser de TI, auditoría o del grupo de finanzas. Ocupe tiempo mirando que podría ya estar hecho en lugar de ir sencillamente a hacerlo de nuevo. Luego confíe y use la información de sus socios internos."

Cree una óptima estrategia de costos compartidos"Hoy en día todos están repartiendo costos compartidos y muchos salen golpeados," dijo Coviello. "Pero la idea aquí es que la seguridad necesita ser considerada en cualquier presupuesto y que no se debe depender constantemente en la organización central de seguridad para obtener esos fondos. Es fundamental para cualquier esfuerzo que tenga."

Según el estudio, hay tres categorías de actividades de seguridad, y típicamente cada una se paga de forma distinta. Las tres categorías son: Estrategia de seguridad y administración de conocimiento, operaciones críticas diarias, y compromiso con los proyectos. Determinar como compartir los costos puede ser difícil, pero es esencial.

"En una era donde el ambiente de negocios es muy dinámico, ¿cómo distribuye los recursos que necesita?" dice en el informe Bill Boni, vice presidente corporativo de seguridad de información y protección de Motorola. "¿Cómo estima el equipo de seguridad cuantos recursos van a necesitar para administrar todos los requerimientos de toda la organización? En lugar de construir un imperio de la seguridad, tiene la organización, haga que las organizaciones tengan gradualmente los recursos. La Seguridad provee los estándares y tiene un programa de gobierno.

Automatice y subcontrate sabiamente"El nombre del juego es eficacia de costos", dijo Coviello, quien aconseja a las compañías a considerar todas las implicancias de subcontratar antes de tomar una decisión. "Considerar las subcontratación debe ser resultado de una combinación de factores. Si es solo costos, está cometiendo un error."

En tanto subcontratar puede crear eficiencias y recorte de gastos, las compañías también deben considerar que aquello que se agrega a los riesgos de seguridad en algunas ocasiones, dice Coviello, ya que existe una potencial pérdida de información cuando uno le confía a un tercero información sensible de la organización.

Traducido para Blog de Segu-info por Raúl Batista

Autor: Joan Goodchild

Fuente: CSOnline