

Conseguir fondos para la seguridad es más duro que vender seguros

Artículo original en inglés: <http://blogs.techrepublic.com.com/tech-manager/?p=293>

Traducción: Angel Gottfriedt (F{-NixARg)

Adaptación y publicación: Lic. Cristian Borghello Director de www.segu-info.com.ar

En el proceso del preparativo para una reunión de seguridad de la información la semana entrante, me he estado preguntando, "¿por qué es tan difícil convencer a aquellos que controlan los gastos para gastar dinero en seguridad?" Si se habla sobre la seguridad de la información, la mayoría de las personas estarán de acuerdo que es un asunto importante, pero si usted les insiste en políticas o presupuestos se encontrará con una pared. ¿Por qué es esto?

La respuesta a esta pregunta es que la seguridad de la información (o su falta) no proporcionan una amenaza inmediata de activos tangible. Es cuando son directamente afectados que esto se convierte en un asunto abrasador para ellos.

Las personas a menudo se refieren a las medidas de seguridad como "seguro" y usan el término "análisis de riesgo" al hablar de seguridad. Sin embargo la falta de pérdida personal hace que la venta de seguridad sea más dura que la de seguros de vida! Al menos cuando una persona empieza a considerar un seguro de vida, sabe que va a morir en cierto momento. Es una certeza. El mismo podría ser antes mencionado para seguros de hogares (los que lo compran saben que necesitan asegurarse que su inversión más grande esta cubierta en caso de un desastre, y la mayoría consideraría la destrucción de su casa una pérdida personal).

¿Pero quien se ve afectado en una empresa cuando la seguridad de la información se ve comprometida? El CIO, el encargado de seguridad (si existe uno), y quizá el CEO, dependiendo del tamaño de la brecha de seguridad; las víctimas por supuesto (o quizás nadie!). Nosotros hemos visto, a través de los años, que las repercusiones por la perdida de los datos no son normalmente tan severas en muchas organizaciones.

Esto lleva a por supuesto al juego conocido como análisis de riesgos -donde unos o más individuos en una organización llegan a decidir si pagar por protección e imponer políticas y procedimientos es de "valor". Comparan los riesgos de una posible brecha de seguridad contra las posibles repercusiones de esa brecha.

Frecuentemente, no es el CIO o personal de seguridad quienes toman la decisión. Sin embargo, ellos son los responsables si un evento ocurre. Esta es porque la seguridad de datos es a menudo manejada por IT, aunque otras áreas de la organización realmente deberían defenderlo.

¿Entonces como hacemos, el personal de IT, para conseguir fondos adecuados? creo existe varias vías de acción:

1. Comunicar. Asegure de señalar otras organizaciones que experimentan (o experimentaron) brechas de seguridad que apuntan a sus objetivos. Cuanto más a menudo usted pueda poner el asunto delante de ellos, más se adaptaran a ello,

particularmente si las brechas son en la misma industria que su propia organización.

2. Lleve a su equipo de IT en esto. Esto no es un asunto en el que deba estar solo. Consiga ayuda del resto de su organización.

3. Hazlo particular. La seguridad es "comportamiento" tanto como es tecnología. Escriba normas y procedimientos sobre seguridad de datos que sean agresivas. Ciertas personas son concienzudas por naturaleza; otros consecuentemente necesitan motivarse.

4. Eduque. De nuevo, atee al comportamiento y comunicación, tenemos que conseguir que la palabra salga. Tal como con el acoso sexual y diversos entrenamientos a través de los años, los empleados de nuestra organización necesitan ser continuamente expuestos a los temas de seguridad, la política y procedimientos que los gobiernan.

5. Legisle. Comunique a sus superiores, en todos los niveles, con respecto a las penas existentes por pérdida información personal. Déjeles saber que las penas necesitan ser significativas para que las personas estén alerta y tomen nota. ¿Por qué piensa usted que existía tal ferviente actividad con respecto al acto de Sarbanes-Oxley? La legislación "tiene dientes" y los CEOs de las organizaciones impactadas por estas leyes deben firmar que los reportes financieros de la organización son "sonantes".

6. Incremento del trabajo. A menos que una organización experimente una brecha que le cause cierto dolor, la seguridad de la información es algo que va a tener que incrementar. Construya un marco de lo que quiere ser y trabaje su proyecto sobre este marco. Es difícil trabajar en seguridad en el vacío.

7. Hazlo parte de la conformidad. Podría sonar como romper un record, pero existe una razón de que me mantenga nombrando los beneficios de escoger un marco de IT y conformidad y certificación. Si la seguridad es parte de su "store-card" es fácil de vender si usted está siendo "instado" por eso.

8. Los auditores son sus amigos. Ayúdeles para ayudarle a armar su caso.

9. Ejecute el análisis de riesgo usted mismo y arme su caso. Como probablemente usted será el sacrificado en caso de una brecha significativa, haga un análisis de riesgo completo. El suyo probablemente será más comprensivo que alguien no familiarizado con IT.

10. Piense fuera de la caja. Existen vías creativas de mitigar el riesgo, que probablemente usted todavía no ha considerado, en una organización. Mire a otras industrias y vea lo que están haciendo y si esto se ajustaría a su organización.

Mientras que puede ser frustrante para nosotros porque pensamos que la seguridad de la información es pan comido, esto no es diferente de las otras cosas en IT en que tenemos que trabajar para conseguir fondos.

Hacer las cosas antes mencionada ayuda a cambiar mentes, dentro y fuera de su organización, y al final del día, preferiría venderle seguridad a mi organización que venderle un seguro de vida a usted. Para mí, IT es mucho más divertido.