Concientización en Seguridad de la Información en Siete Pasos

Autor: Gary Hinson, IsecT Ltd. (20 de Diciembre de 2005)

http://www.noticebored.com/html/7_steps.html

Traducción para Segu-Info: Alejandra Stolk y Fernando Spettoli

Revisión: Lic. Cristian Borghello, CISSP

Fecha Publicación: 20 de julio de 2008

Introducción

¿Está Ud. pensando en realizar un programa de concientización pero no está seguro por dónde empezar? Este artículo le ofrece algunas claves y tips pragmáticos de cómo aplicar siete pasos claves en un proceso típico de Tecnología de información desde el proceso de selección y el lanzamiento de un programa de concientización. Está basado en nuestra experiencia en la que ocasionalmente hemos sido el motor del proceso y en otras hemos sido conducidos por el mismo.

Hemos tratado de generalizar lo más posible este artículo para hacerlo de utilidad y evitar que el mismo quede como artículo para una cartelera y dejar al juicio del lector cómo adaptarlo a circunstancias específicas. Cómo en otros artículos de cartelera en sitios web, este está siempre trabajándose.

Gracias a las maravillas de la web revisamos el artículo de tiempo en tiempo y aprovechamos nuevas ondas de inspiración. Si queda alguna duda, pregunta o sugerencia sobre el artículo por favor ponte en contacto. Estaremos muy contentos de saber de tí. Especialmente, si hemos dejado por fuera algo importante para tí.

1. Especifica tus requerimientos

El primer paso es establecer las necesidades. Piensa con cuidado qué estás tratando de lograr con un programa de concientización. Hasta que tus objetivos no estén claros, tendrás problemas planificando y organizando un plan de concientización, mucho más evaluando y escogiendo productos y servicios que puedas necesitar para ello.

Podrías empezar por revisar nuestro artículo sobre el valor de la concientización de seguridad, y luego preguntarte algunas preguntas retóricas:

- ¿Tienes actualmente un plan de concientización ejecutándose? ¿Es este un nuevo concepto para la organización? Si no es sobre seguridad de la información, ¿Existen otros planes de concientización en tu organización?
- ¿Este plan incluye concientización, entrenamiento y educación o sólo alguna de ellas?
- ¿Qué tópicos o asuntos cubrirá este plan? ¿Existen otros aspectos importantes sobre seguridad de información en tu organización?

- ¿Qué tan seguido debería este programa llevarse a los individuos? Es lo suficientemente seguido cómo para mantener la seguridad de información en su agenda?
- ¿Debería este programa tener cierto nivel de profundidad para otorgar consejos útiles, guías y asesoría en dónde sea necesario, o está concebido para dar un resumen superficial?
- ¿Debería este programa aplicarse a todos los empleados desde el primer día hasta el último día de su trabajo? ¿Debería extenderse a los socios y terceras partes en puestos similares, Por ejemplo: consultores, contratistas y otros asociados trabajando en sitio?

Ahora trata de soñar un poco - Imagínate a tí mismo en el futuro - trata de imaginarte cómo han salido las cosas cuando el plan de concientización está ejecutándose. Podrías considerar algunos aspectos más complejos:

1. Quieres simplemente que las personas estén más conscientes sobre las seguridad o quieres que actúen de forma diferente como resultado de estar conscientes? La concientización es significativa por sí misma, pero hemos notado, que no es normalmente el objetivo final, y por ello un plan necesita continuar más allá de una simple mejora en los niveles de concientización, necesita incluir técnicas motivacionales y de control...
2. A quienes estás tratando de llegar con tu campaña? ¿Son éstas personas similares o son de hecho audiencias o grupos separados con diferentes necesidades de información? En tu jerarquía gerencial el personal supervisorio de tu audiencia entiende y apoya los que estás tratando de hacer o por el contrario también necesitan ser atendidos? Existen equipos con requerimientos más específicos y particulares? (como los de Operaciones y el centro de asistencia al usuario)
3. ¿Estás viendo una campaña general sobre la concientización de seguridad, o un entrenamiento específico para un problema en particular, o ambas? ¿De qué tipo de asuntos quieres que esté la gente consciente? Es una lista fija de cosas o una lista dinámica que cambiará con el tiempo y los meses y años por venir? Responder esta pregunta puede ayudarte a decidir si es factible cubrir completamente la materia en una sola entrega o si necesitas pensar una forma de hacerlo a largo plazo y evitar sobrecargar con información a tu audiencia...
4. ...Esto nos trae a: ¿Este plan de concientización va a ser una campaña continua o estás buscando una iniciativa de corto plazo? Ambas estrategias son válidas en las circunstancias adecuadas, algunas veces una combinación de ambas es necesaria.
5. Existe una cultura de seguridad informática en tu organización, o estás continuamente peleando para que cualquiera se tome el tema con seriedad? En otras palabras, ¿Qué tan madura es tu organización en términos de seguridad? Si la seguridad está bien arraigada en la organización, su gente y sus procesos (por ejemplo, en la mayoría de los bancos) tendrás un trabajo más fácil si el tema de concientización

de seguridad informática no es un concepto totalmente extraño. Ya existe un conjunto de políticas de seguridad informática establecido? Se encuentran actualizadas? O necesitará tu programa el establecimiento de las mismas así como promoverlas. Se realista en la planificación acerca del tiempo y el esfuerzo que probablemente tomará llegar a la meta: recuerda, es mejor prometer menos y obtener mayores resultados que viceversa!

6. ¿Será la campaña una actividad financiada y ejecutada por el negocio o liderada por Tecnología de Información? ¿Quien la ejecutará? ¿Qué experiencia/conocimiento tienen en seguridad de información y campañas/entrenamiento/educación de concientización en seguridad para equiparlos para la tarea? Es bastante común el proyecto sea tu bebé, entonces podrías obtener entrenamiento o asesoría adicional para dar poder despegar la campaña. Un poco de asistencia concentrada en la planificación y las primeras fases podrá ayudarte a evitar perder tiempo, esfuerzo y empeorar después.

NIST Special Publication 800-50 es una excelente fuente de consejos imparciales en concientización de seguridad. Si los aspectos mencionados anteriormente te dejaron pensando en el tema, revisa el SP 800-50 para ampliar tus horizontes y profundizar en el análisis.

2. Prepara un plan y evalúa una lista de productos

Los programas de concientización no se ejecutan por sí mismos, especialmente porque muchas organizaciones comienzan con una posición un poco negativa. Tomará un gran esfuerzo superar esa inercia, y conseguir que el plan se mantenga con el tiempo. En otras palabras, es necesario desarrollar un plan para establecer el programa y luego administrarlo en forma permanente con el fin de entregar los beneficios proyectados.

Si usted tiene una gran cantidad de terreno a cubrir (por ejemplo, "Todo lo que concierne a la seguridad de información"!), sin duda le recomendamos la planificación para cubrir en secciones o trozos a lo largo del tiempo, y siempre que sea posible la elaboración de esos trozos en términos que tengan sentido a su audiencia/s. Tomemos, por ejemplo, el problema del virus: toda persona que utiliza un sistema de TI debe tener una comprensión básica de los virus. Al explicar acerca de los virus, es posible que quieras hablar de cuestiones como la gestión de la configuración, sistemas y redes de acceso y así sucesivamente, pero no es necesario entrar en profundidad en todos los temas al mismo tiempo.

Es perfectamente aceptable decir "Le diremos más sobre esto más tarde" o incluso "Llame al Help Desk o el Administrador de Seguridad de Información para obtener más información". De esta forma puede mantener un enfoque en los mensajes clave sin sobrecargar de información a las personas.

Una forma ideal de cristalizar sus pensamientos desde el paso 1 mencionado anteriormente, en paralelo con el desarrollo de su plan y hacer frente a todas las partes de tu mapa mental, es preparar una lista de productos de evaluación que contenga:

- Filas para cada uno de los criterios que son importantes para usted;
- Columnas de los criterios y su ponderación (por ejemplo, 3 = vital, 2 = importante, 1 = sería-bueno-tener) y más columnas para las observaciones y resultados respecto a cada uno de los productos que está evaluando.

A medida que se trabaja en la lista, usted, en efecto irá refinando y definiendo sus requisitos para el programa, lo que hará más fácil desarrollar el correspondiente plan. Es por eso que tratamos a estas dos actividades como un solo paso.

3. Asegurar el financiamiento y el apoyo de la gerencia

Colocar a la directiva de la organización en el mismo barco con la idea de la campaña de concientización es, en mi humilde criterio, sin dudas, es el logro más importante que podrás alcanzar en los próximos meses y pagará grandes dividendos en el largo plazo. ¿Cómo lograr esto? te lo dejo a tí: sólo podemos darte pistas en las cosas que han funcionado para nosotros y nuestros clientes.

Dependiendo de la corporación, usted puede o no tener la necesidad de hacer una propuesta fuerte para el compromiso financiero qué representará la inversión - algunos altos directivos responden mejor su presentimiento que a los números crudos. Nuestro artículo sobre un modelo de negocio genérico puede ser un buen insumo si usted necesita persuadir a su gestión para financiar y apoyar la campaña de sensibilización (si necesita la versión editable MS Word del documento en caso de que ahorrará tiempo no duden en contactarnos).

Trabaja con tu CIO o el director de TI y si se puede con algunos otros gerentes de influencia que tendrán algún interés en que la campaña sea un éxito. Siempre encontrarás amigos en los departamentos de Auditoría Interna, Cumplimiento de las Normas, Servicios, jurídico, gestión de riesgos, recursos humanos y finanzas. El tiempo transcurrido privada y pacientemente para explicar tus planes a las principales partes interesadas ayudará (a) definir su plan, (b) identificar cualquier preocupación; (c) desviar las críticas y (d) la línea hacia arriba para apoyar abiertamente su programa, especialmente durante las primeras fases de la entrega. Esta es su inversión en el programa de concienciación!

Por cierto, a menudo vale la pena hacer explícito el apoyo de la gerencia a la gestión de la seguridad de la información durante este proceso, es decir, al menos una cita de un alto directivo que de manera inequívoca solicite el cumplimiento de los mandatos. Puede que necesites redactar un borrador para una declaración del CEO, pero su firma en la parte inferior va a añadir peso a su programa de concienciación mucho más allá de su valor aparente. Créanme, el peso funciona!

Durante el paso 3, no tenga miedo de seguir perfeccionando su plan y las necesidades. Todo el tiempo, usted está pensando en él y aprender acerca de las posibilidades. No pierdas la energía que el cerebro te está dando!

4. Identifica y genera listas de posibles soluciones

Ahora estás en una buena posición para ir en busca de lo que realmente puedes ser que necesites. Para empezar, busca dentro de su propia organización de los recursos adecuados, por ejemplo en TI, recursos humanos, Comunicaciones Corporativas, Capacitación y Desarrollo de funciones. Tome el consejo de otros colegas de funcionamiento interno de sensibilización / formación / programas educativos (tales como salud y seguridad o de formación en TI). Sólo con preguntar a tus colegas por consejo vale la pena, ya que puede ayudar a obtener su apoyo para entregar el programa más adelante, mientras que no preguntarles a ellos puede que involuntariamente terminen en contra de los planes de concientización.

Cuando se trata de encontrar pública libre y las ofertas comerciales, Google es tu amigo! Busca términos tales como: "conciencia de seguridad", "conciencia de seguridad de la información", "carteles de sensibilización a la seguridad" y así sucesivamente. Echa un vistazo a las revistas, publicaciones y sociedades profesionales para obtener ayuda y consejos. Únete al foro de sensibilización del Foro de Seguridad (Security Awareness Forum) en Yahoo! y revisas sus archivos. Rápidamente, habrás acumulado una interesante lista de productos y servicios. Se sistemático sobre la forma en que reúnes y evalúas la información y se te hará más fácil el resto de los pasos.

Ahora ve a través de tu lista de recursos internos y externos, verifica aquellas cosas realizadas en la empresa y en las partes que crees que pueden satisfacer sus necesidades. Por todos los medios descartar el material que no te sea útil, pero ten cuidado - es fácil pasar por alto los recursos útiles que son mal comercializados, incompletos o simplemente desconocidos (a menudo porque son nuevos). Si tienes el tiempo y la energía, puede ser más seguro que hagas una lista de contactos y potenciales proveedores en esta etapa y recortarla más tarde. No hay daño en contactar a las empresas para solicitar información inicial en esta etapa, pero desconfía de las ofertas y vendedores que quieran resolver las cosas rápidamente. El siguiente paso funciona mejor si se enfoque de forma objetiva en tus términos, no los suyos.

5. Evalúa soluciones potenciales

Para ofertas comerciales, este es el convencional sub-proceso de licitación:

- Preparar una solicitud formal de las propuestas que contiene sus exigencias derivadas de tus sueños, planificación, necesidades y criterios de evaluación (que es probable que no quieras dar a conocer a los ofertantes);
- Enviarás la solicitud de ofertas a cada uno de los posibles licitadores, sin más identificación que se está invitado a la oferta, junto con un plazo para responder;
- Recibirás las preguntas y solicitudes de aclaración de algunos oferentes, responder con rapidez a todos los ofertantes sin revelar quien originó la formulación de preguntas;
- Cuando el vence el plazo, rechazarás cualquier otra ofertas o propuestas y empezarás a evaluar sistemáticamente las ofertas.

Colocarás la puntuación utilizando una lista de criterios de evaluación que debes tener por escrito antes de comience la licitación (te recomendamos asignar un porcentaje de peso a cada resultado contra cada uno de los criterios);

- Centrarse en los requisitos esenciales primero - puedes ser capaz de excluir a algunos oferentes de inmediato en caso de que simplemente no satisfacen tus necesidades esenciales;

- No olvides las ofertas adicionales realizadas por los ofertantes - a veces, ellos sugieren ideas útiles, valiosas ideas que has pasado por alto, y que pueden ayudar a llegar a una decisión definitiva si los resultados están cercanos entre una o más ofertas;
- Examina la calidad de las ofertas o propuestas, así como cualquier muestra de los sistemas de conocimiento o materiales enviados para su evaluación - todos estos son indicadores válidos de la profesionalidad y la calidad de los ofertantes;
- Haga sus cálculos: Resultado final de cada ofertante = (suma de (puntuación para cada criterio de ponderación para x ese criterio)) dividido por puntuación máxima posible x 100 por ciento.

El personal del departamento de compras estará gustoso de ayudarte con el proceso de licitación, sobre todo si existen grandes sumas de dinero en juego. Ellos quieren asegurarse de que el proceso sea justo, objetivo y totalmente por encima de a bordo. Esta es su profesión: ten en cuenta sus consejos!

Para ofertas hechas en casa y gratis, haz de igual forma listas, criterios de evaluación similares a los de una licitación comercial. Es muy posible que tal vez desees tomar ventaja de las comunicaciones y materiales de libre distribución y por ejemplo: combinarlos con los recursos internos y comerciarles. Es tu elección.

6. Selecciona y compra la solución escogida

El resultado final del paso 5 normalmente termina con un ganador pero no siempre es así. Algunas veces puedes seleccionar distintos ofertantes para dedicarse a partes separadas de tus requerimientos. Algunas veces no podrás decidirte entre un par de ofertantes. El paso 6 generalmente requiere de negociaciones con los proveedores, aclaraciones de precios, términos de la oferta y algunos otros puntos que puedan no estar claros. Finalmente, tomarás tu decisión, prepararás la compra y estarás listo. Esto se conoce como hacer negocios.

Un comentario complementario desde el otro lado de la cerca: por favor trata de hacer tiempo para contactar a aquellos proveedores que no ganaron la oferta o al menos invítalos a una ronda de preguntas. Preparar una propuesta formal requiere tiempo y esfuerzo de su parte. Si sientes que algunos aspectos te decepcionaron, comunícalo siempre ayuda saber donde fallaste para hacerlo mejor la siguiente vez. [Si ellos no quieren si quiera oír de ti, sabrás que tomaste la decisión correcta!]

7. Implementa y lanza la campaña de concientización

Ahora deja que la diversión comience! Mientras que los 6 pasos anteriores parecían burocráticos y sin diversión, puede que encuentres lo contrario en la práctica! De igual forma que con el desarrollo de software el tiempo que se gasta en decidir los requerimientos, diseño de la solución y pruebas del sistema es más fácil con un final más suave y una implementación más efectiva.

Si has escrito un buen plan, con el apoyo de la gerencia y los recursos necesarios para ejecutarlo. Ahora es tiempo de llamar a tus colegas internos y tus proveedores y construir y entregar el plan de concientización que soñaste! Buena Suerte!

Conclusión

En este artículo, te hemos dado un pequeño sabor de lo que normalmente incluye el lanzamiento de un programa estructurado de concientización de seguridad. Tu kilometraje podrá variar pero esperamos que te ayude a tornar un proceso confuso en un las lista de pasos secuenciales.