Caso de estudio:
“El valor de negocio de ISO17799”

Abril 2006

Dr. Gary Hinson

CISA, CISSP, CISSM, CISA, MBA

Traducción de Javier Ruiz Spohr

CISA, Auditor BS7799

www.iso27000.es

Gary Hinson, consultor y experto en buen gobierno y seguridad de las tecnologías de la información, ha autorizado a www.iso27000.es a traducir su interesante caso de estudio “The business value of ISO17799”. En él analiza las ventajas y beneficios empresariales de implantar en una empresa de servicios informáticos la BS7799-2 (actual ISO27001) y el código de buenas prácticas asociado ISO17799.

Este tipo de empresas, al tener como objeto de su negocio los sistemas de información de sus clientes, obtienen una clara ventaja competitiva por medio de la implantación de estas normas, que dan una garantía a los usuarios de sus servicios de que la información es tratada con métodos procedimentados y directrices de seguridad claras.

Gary Hinson es máximo responsable de la empresa consultora IsecT Ltd. (www.isect.com), el servicio de información www.noticebored.com, y la web www.iso27001security.com.

Introducción

Este caso de estudio se refiere a una empresa de servicios informáticos que decidió implantar la ISO17799 -Código de buenas prácticas para la Gestión de la Seguridad de la Información-, obteniendo como resultado importantes ventajas de negocio.

El caso revela algunas conexiones sorprendentes entre la gestión de la seguridad de la información y la gestión empresarial en general, además de numerosas ventajas indirectas que no suelen mencionarse.

Situación de partida

"Servicios, S.A." -el nombre no es real- es un proveedor de servicios informáticos, hardware y software para clientes empresariales. Con su certificación ISO 9002 obtenida hacía casi diez años, la plantilla estaba acostumbrada a trabajar de forma consecuente con directrices y procedimientos documentados. Sin embargo, el ambiente en la empresa había empeorado de un par de años hacia acá. Las decisiones de la dirección se tomaban más bien de forma instintiva, con poco análisis real. Con una rotación de personal en aumento, la dirección se dio cuenta de la necesidad de cambiar y analizó en profundidad las fortalezas y debilidades de la organización.

La alta dirección de "Servicios, S.A." decidió implantar la ISO17799. Según uno de los directivos, "implantar la ISO17799 tenía sentido empresarial. Asegurar la información interna de "Servicios, S.A." reduciría el riesgo, y por tanto el coste, de brechas de seguridad importantes. ISO17799 es un marco de seguridad conocido, utilizado por algunas de las empresas líderes a nivel mundial (BT, HSBC, Shell International y Unilever, entre otras), lo que nos proporcionaba los medios para implementar controles de seguridad basados en las mejores prácticas."

Este directivo nos dijo que "la ISO17799 no trata sólo de seguridad de la información o de tecnologías de la información; realmente ayuda a la organización a ganar dinero." Enumeró las siguientes ventajas de la ISO17799:

Ventajas directas

Incremento de la fiabilidad y seguridad de los sistemas: "Como cualquier empresa, "Servicios, S.A." depende de los sistemas de información. La ISO17799 garantiza que ahora tengamos controles que mantengan la disponibilidad de los sistemas y reduzcan el riesgo de que las vulnerabilidades sean explotadas. Las auditorías internas de seguimiento y las externas de recertificación aseguran que la empresa se mantiene al día en el conocimiento de las vulnerabilidades y buenas prácticas más recientes."

Incremento de beneficios: "Las ventas y los márgenes se han incrementado y la percepción de nuestra empresa por parte de los clientes ha mejorado. Nuestra certificación BS7799-2 demuestra que se puede confiar en nosotros para asegurar los datos de nuestros clientes, así como los nuestros propios. Nuestros clientes no sólo entienden que nuestra inversión en la ISO17799 les ha proporcionado beneficios a ellos, sino que están dispuestos a pagar un poco más por una infraestructura de IT segura. Desde que obtuvimos la ISO17799, hemos constatado un incremento notable de nuestro beneficio final y algunos clientes nuevos nos han dicho que prefieren tratar con empresas que tienen una certificación de seguridad reconocida. Adicionalmente, recibimos más solicitudes de oferta de empresas que exigen como requisito previo la conformidad con ISO17799. Y, de paso, nuestros empleados pierden menos tiempo navegando en Internet por páginas no relacionadas con el trabajo."

Seguridad de la información rentable y coherente: "Hemos implementado una seguridad eficiente en costes y adecuada a nuestras necesidades de negocio. "Servicios, S.A." tenía muchas protecciones técnicas por toda la empresa, pero la evaluación de riesgos puso de manifiesto que algunas de nuestras protecciones o salvaguardas proporcionaban poco o ningún beneficio empresarial y que proporcionarían un mejor retorno de la inversión siendo reconfiguradas para proteger activos necesitados de un nivel de protección mayor. Todas las divisiones y departamentos de "Servicios, S.A." habían desarrollado hasta el momento sus propias directrices de seguridad. La ISO17799 nos ayudó a desarrollar un enfoque coherente de la seguridad por medio de unas políticas uniformes basadas en las mejores prácticas de la industria. Allí donde es necesario, el cumplimiento de las políticas por parte de los empleados está apoyado por procedimientos disciplinarios."

Racionalización de sistemas: "Analizar adecuadamente nuestros requerimientos de información y de seguridad de la misma significa que invertimos nuestro dinero inteligentemente. Fuimos capaces de recortar en cerca de un 50% nuestros sistemas y datos al darnos cuenta de que no merecía la pena mantenerlos, e incluso relajamos controles en algunos sistemas de bajo riesgo".

Conformidad con la legislación: "Implantar la ISO17799 nos obligó a cumplir con la legislación del Reino Unido en áreas como la protección de datos y el copyright de software."

Ventajas indirectas

Mejora del control por parte de la dirección: "La dirección tiene más control sobre la organización y mejor información de calidad para gestionar la misma; se reduce, por tanto, el esfuerzo de la dirección."

Mejores relaciones interpersonales: "Políticas claras, procedimientos y directrices le facilitan las cosas a nuestra plantilla. El ambiente de trabajo ha mejorado y la rotación de personal se ha reducido. La ISO17799 diferencia a "Servicios, S.A." de su competencia y le ha proporcionado un argumento de ventas único, procurando un mejor entorno laboral a nuestra plantilla. Los empleados comprenden ahora que su potencial salarial depende de cómo perciban los clientes la marca de la empresa y que cualquier publicidad negativa les puede afectar. La profesionalidad ha aumentado en toda la compañía. Dado que la seguridad depende en tan alto grado de los controles internos, necesitamos mirar con más cuidado a quién estamos contratando. Por medio de ISO17799, introdujimos más procesos de contratación que reducen el riesgo de emplear personas inadecuadas para el puesto o que pudieran suponer un riesgo potencial para nuestra empresa. Ahora sabemos quién trabaja para nosotros.

Mejor gestión del riesgo y planificación de contingencias: "A través del proceso de certificación de ISO17799, "Servicios, S.A." identificó sus vulnerabilidades, amenazas e impactos potenciales en el negocio. Como resultado de esto e implementando controles de ISO17799, "Servicios, S.A." tiene un enfoque más estructurado de la gestión del riesgo. Por ejemplo, ahora tenemos un proceso racional para decidir qué riesgos transferimos a nuestras aseguradoras. Ahora también tenemos un plan de continuidad de negocio que se ajusta a la empresa, no sólo al departamento de IT. En la evaluación de riesgos se identificaron los activos de información que son críticos para el éxito de la empresa. Esto nos permitió elaborar un plan de continuidad de negocio que priorizara dichos activos y redujera nuestra exposición potencial a pérdidas financieras o publicidad negativa."

Aumento de la confianza de clientes y socios comerciales: "La mayor sensibilización hacia las brechas de seguridad hacía buscar a socios comerciales y clientes evidencias de seguridad. La certificación ISO17799 ha aportado esa garantía. En cualquier negocio tienes que destacar sobre tu competencia. El haber sido el primer VAR -distribuidor de valor añadido- del mundo en obtener la ISO17799 es algo que siempre va a distinguir a "Servicios, S.A.". La inclusión de los logotipos de ISO17799 en todos nuestros impresos es un recordatorio constante a nuestros clientes actuales y potenciales de que somos una empresa gestionada profesionalmente, que toma muy en serio la confidencialidad, integridad y disponibilidad tanto de su información como de la nuestra."

Costes

"A pesar de lo que se dice, los costes de implantar la ISO17799 son muy moderados. El principal coste fue el esfuerzo del cambio cultural -tuvimos que "dejar irse" a alguna de nuestra gente por no cumplir con nuestras políticas y procedimientos-. Las revisiones regulares de conformidad para mantener nuestra certificación sólo nos cuestan unas 3.000 £ (4.500 €) al año, por lo que ISO17799 es muy efectiva en costes. Estamos en conversaciones con nuestros asesores para combinar las revisiones de ISO17799 e ISO 9002 para ahorrar tiempo y dinero."

Para más información

Para más información acerca de este caso de estudio o para ayuda en evaluar el valor de negocio de ISO17799 en su organización, contacte IsecT Ltd. (info@isect.com).

Nota final: El texto original en inglés de este caso de estudio se puede encontrar en:

http://www.isect.com/html/value_of_7799.html