

¿Cómo gestionar el riesgo en TI?

Las grandes compañías se han concienciado de la estrecha relación entre la innovación tecnológica y de negocio, y las oportunidades y riesgos que supone. Por ello, han comenzado a diseñar planes de seguridad para seguir avanzando sobre terreno firme.

Texto: Executive Circle

En el último año, la gestión de los riesgos del negocio — incluidos los derivados de las inversiones tecnológicas— se ha ubicado en el puesto número cuatro de la lista de prioridades de las empresas, cuando hasta hace poco se encontraba en una posición que ni siquiera se acercaba al top ten, según un estudio de la consultora Gartner, que analizó las opiniones de unos 880 CIOs. "Los riesgos de las inversiones tecnológicas son hoy contingencias de nivel empresarial y, por tanto, no puedes hablar de ningún elemento de riesgo de negocio sin haber contemplado antes estos mismos peligros para las TI", apunta el vicepresidente de la firma de investigación Stamford, Richard Hunter.



Internet y otras tecnologías de comunicación como la inalámbrica, han permitido a las empresas compartir, libremente y sin costes muy elevados, todo tipo de información con clientes y socios de negocio. No obstante, estos vínculos estratégicos son susceptibles de abrir agujeros de seguridad que pueden llegar a ser catastróficos para la empresa y acarrear consecuencias legales.

Providence Health Plans es una compañía de Oregón sin ánimo de lucro, financiada por Providence Health System, que utiliza Internet, el e-mail y las posibilidades del EDI (tecnología de Intercambio Electrónico de Datos) para compartir información con clientes, proveedores y distintos organismos. Sus conexiones están hoy en día aseguradas con tecnología de encriptación y autenticación, pero la compañía continúa investigando nuevas medidas de seguridad. "La posibilidad de vernos involucrados en un caso de divulgación de información confidencial nos preocupa tanto como las consecuencias financieras de un litigio", afirma Chris Apgar, asesor jurídico de Providence Health Plans.

"Este problema no sólo afecta a grandes corporaciones financieras y entidades de carácter público", apunta el vicepresidente senior de Chubb Group of Insurance Companies, James West: "En realidad, cualquier negocio que trabaje con información confidencial de clientes o usuarios ha de estar alerta ante esta situación". Algunos directivos pueden verse tentados a actuar sobre seguro para solventar los problemas de la gestión del riesgo, es decir, abandonar los proyectos de innovación en TI, una alternativa claramente desacertada en tiempos de globalización. En lugar de intentar evitar los riesgos relativos a la tecnología, las empresas más aventajadas están

aprendiendo a manejarlos para que su negocio avance, apoyándose en innovaciones estratégicas en materia de seguridad.

La planificación es la clave

La consolidación de una efectiva gestión de riesgos de TI requiere de un continuo ciclo de valoración y reevaluación. En este sentido, la planificación proactiva determina qué recursos necesitan ser protegidos, cuáles son exactamente las amenazas que acechan al sistema y qué puede hacer la compañía para mitigar el peligro.

"En Providence Health Plans continuamos trabajando para incluir las valoraciones de mitigación de riesgos como parte de los procesos de desarrollo", afirma Apgar. "Desde nuestro punto de vista, es vital realizar una valoración del riesgo en el conjunto de la compañía una vez al año, así como en el momento en el que se incorpore cualquier modificación en los entornos de TI", añade.

Una vez identificados los puntos débiles, es necesario recurrir al plan reactivo. "En este punto necesitamos contar con un equipo de profesionales capaz de responder a cada posible emergencia en TI con planes de contingencia eficaces, ya se trate de un ataque terrorista, un virus informático o la acción malintencionada de un empleado", explica el director de la estrategia Informática de Confianza de Microsoft, Scott Charney.

Todo documento ha de estar adaptado para dar respuesta a un posible incidente. "Estos registros podrían necesitarse para demostrar que la empresa ha cumplido con las regulaciones gubernamentales en materia de prevención; poner en marcha de nuevo la estrategia de seguridad después de haberse producido un ataque; formalizar el aviso a las autoridades y, si cabe, reclamar daños y perjuicios", añade Charney.

La forma en la que una compañía evalúa y enfoca su riesgo en TI puede variar considerablemente de unos casos peligrosos a otros. Por ejemplo, un sistema de detección de intrusión de red de 10.000 dólares podría tener sentido en un gran hospital en el que las personas circulan libremente, pero en el caso de una pequeña clínica, un armario de archivo franqueado por una llave puede ser suficiente.

Finalmente, todas las planificaciones han de ser tratadas en el marco de un proceso continuado. "Si alguien entra en tu red, necesitas volver al origen para determinar por qué tus medidas proactivas no funcionaron", afirma Charney.

Con un 20 por ciento más de esfuerzo en materia de seguridad, las organizaciones pueden obtener un 80 por ciento más de beneficio

Compartir el riesgo

Para aquellas compañías que no están en condiciones de eliminar o mitigar los posibles riesgos, pero que encuentran inaceptable convivir con ellos, existe otra alternativa: compartir el riesgo con una tercera firma. Aseguradoras como Chubb ofrecen pólizas especiales que cubren riesgos en TI, incluyendo los referidos al

fracaso en la protección de la información confidencial de los clientes, la transmisión de virus informáticos y la infracción de los derechos de propiedad intelectual. El vicepresidente senior de

Chubb Group asegura que el pasado año se registró un incremento de más del 400 por ciento en las demandas empresariales de cobertura para los riesgos de la seguridad de la información, y pronostica un incremento para el próximo año que podría igualar, o incluso superar, este porcentaje.

En el marco de esta alternativa, que apunta a la externalización de la gestión del riesgo, proliferan los acuerdos de niveles de servicio que son ofrecidos por proveedores financieramente solventes. Estas prácticas pueden también recoger una cláusula que garantice que el proveedor asume los daños en el sistema si la seguridad presenta brechas por alguna negligencia en su actuación.

Centralización y control de calidad

Un número creciente de compañías está apostando por una gestión del riesgo basada en políticas corporativas gestionadas de forma centralizada. Algunas organizaciones públicas, incluso, han puesto en marcha un mecanismo aún más estructurado para todos los proyectos de TI nuevos, con chequeos constantes a lo largo de todo el proceso. En este escenario, los sistemas han de ser diseñados para que los datos personales no estén expuestos —ni interna ni externamente— a personal no autorizado, a través de prácticas de autenticación y de usuario registrado.

El control de calidad es otra de las herramientas básicas en cualquier cuadro de innovación. Sin embargo, la toma de control no siempre requiere de una completa y costosa modernización de las infraestructuras y prácticas de TI. En opinión de Hunter, analista de Gartner, "está comprobado que con un 20 por ciento más de esfuerzo en sus políticas de seguridad, las organizaciones pueden obtener un 80 por ciento más de beneficios"..

También es importante poner a alguien preparado frente al timón, como un director de Seguridad de la Información, o CISO (Chief Information Security Officer). Este directivo es el máximo garante de la estrategia de seguridad en el área de TI para el conjunto de la compañía.

Pero unas rigurosas medidas de protección de la intimidad resultan ineficaces si los empleados no las cumplen. "El personal de la compañía necesita un constante entrenamiento en las últimas políticas corporativas emprendidas en estos campos, y un exhaustivo conocimiento de las regulaciones gubernamentales específicas y de las implicaciones derivadas de su incumplimiento", apunta el directivo de Chubb Group.

"En este punto hay que ser especialmente firme", señala John Voeller, director de Tecnologías de Información de la constructora Black & Veatch y asesor del Gobierno Federal de EE UU en el desarrollo de estrategias para proteger sus infraestructuras críticas: "Necesitas que todos tus empleados entiendan que hay ciertas cosas que no se pueden hacer, y que la información no debe ser transmitida ni expandida".

Las claves de la LOPD

La ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) impone diversas obligaciones a todas las empresas y profesionales que posean bases de datos con información de carácter personal. Básicamente se trata de tres compromisos: notificar ante la Agencia de Protección de Datos todos los ficheros que contengan información de carácter personal (de clientes, proveedores, asociados, etcétera); adecuar la actividad de la empresa a las obligaciones establecidas para recabar, tratar y comunicar datos de carácter personal, y elaborar un Documento de Seguridad obligatorio, según los requerimientos del Real Decreto 994/1999.

En este sentido, y de acuerdo con el artículo 4 de esta normativa, "los datos de carácter personal sólo se podrán recoger y someter para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". La Ley fija también la condición de que una vez desaparezca la necesidad de su manipulación, los datos han de ser cancelados por el responsable del fichero.

El artículo 6 de la LOPD señala además que el tratamiento de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa. Así, aquellos a quienes se les soliciten datos personales deberán ser previamente informados de la existencia de un fichero, así como de la finalidad de la recogida de los datos, de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta, de la identidad y dirección del responsable del tratamiento y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, entre otros. Si los datos figuran en fuentes accesibles al público (como las guías telefónicas o los listados de colegios profesionales) es posible su tratamiento sin el consentimiento de los titulares.

Respecto de la utilización de los datos del censo electoral, la Ley Orgánica 5/1985 de 19 de junio de Régimen Electoral General prohíbe cualquier información particularizada sobre los datos personales contenidos en el censo, a excepción de los que se soliciten por vía judicial.