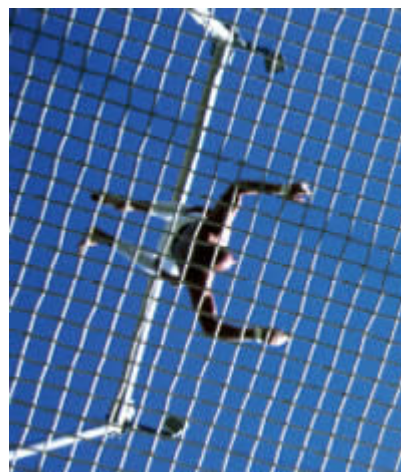


¿Cómo gestionar el riesgo en TI?

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.

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.

Empresas protegidas: cuatro visiones del riesgo en TI

¿Cómo afronta el mundo empresarial la identificación y el control de los riesgos en TI? Así ven el reto cuatro asesores de Executive Circle: Gerard Johnson, director de Tecnología en HSN.com; Tom Guthrie, vicepresidente de Operaciones de Cox Communications; Karl Mudra, CIO de Delta Dental, y Merl Waschler, vicepresidente ejecutivo y director de Operaciones de Valley of the Sun United Way.

Executive Circle: ¿Cuáles son las mayores fuentes de riesgo de TI en su empresa?

Johnson: Es una respuesta impopular pero, en mi opinión, el factor de riesgo más significativo lo constituyen las personas. En este sentido, hemos de hacer dos consideraciones. La primera en cuanto al fracaso en la disciplina de algunos empleados, que obvian la aplicación de parches de seguridad en el tratamiento de las vulnerabilidades de la compañía. La segunda, es la salvaguarda de toda información confidencial de clientes y socios. En este punto, el personal ha de estar plenamente concienciado de su responsabilidad.

Mudra: Nuestra organización hace frente a dos riesgos muy importantes: por un lado, necesitamos cumplir requisitos financieros para poder asegurar una protección adecuada de los activos de información; por otro, apostamos por la obtención de unos determinados niveles de rendimiento. En la práctica, si acuerdo un nivel de servicio con un cliente en concreto y no puedo satisfacerlo, me veo obligado a compensarlo económicamente.

Waschler: El punto de partida para cualquier actuación en nuestra compañía es el control de la información con la que trabajamos. La confidencialidad de los datos es crítica para nuestras relaciones de negocio. Pero esta tarea se ha vuelto cada vez más compleja, tanto desde un punto de vista puramente tecnológico, como en términos de legislación.

EC: ¿Cómo han influido las reformas legislativas el modo en el que su firma enfoca el tema de la gestión del riesgo?

Johnson: Dentro de la filosofía de HSN.com destaca la concienciación con la reciente ley CAN-SPAM (que controla el envío masivo de publicidad por e-mail). Una de las maneras más recurrentes de mantener informados a los clientes de la compañía es a través del correo electrónico, pero nuestra actuación ha sido siempre muy clara y cuidada, comprometiéndonos en todo momento con no efectuar ningún tipo de práctica de spam. Nuestro departamento de Marketing vigila todos y cada uno de los pasos que damos en este camino, en constante comunicación con el equipo de TI, y no pierde de vista ninguna de las nuevas regulaciones que afectan a nuestra actividad empresarial.

Waschler: Sarbanes-Oxley (la ley de protección a la inversión y reforma de la contabilidad de la empresa pública de 2002) es una legislación originariamente enfocada a las corporaciones de índole público que ha terminado afectando la actividad de empresas sin ánimo de lucro. Para nosotros, también esta ley define la forma en la que hemos de trabajar. Esto nos ha llevado a revisar la manera en la que gestionamos y manejamos la información. En este sentido, evaluamos el riesgo comercial con un enfoque diferente del que veníamos utilizando hasta ahora.

Guthrie: Como forma de regular el negocio, estamos acostumbrados a conservar, durante largos periodos de tiempo, información relativa al trato con nuestros clientes (datos confidenciales, llamadas telefónicas, etcétera). En la actualidad aún nos encontramos bajo el influjo de la ley Sarbanes-Oxley, que nos ha conminado a revisar nuestros procesos y procedimientos actuales. Con todo, hemos detectado que parte importante del riesgo se halla en la interpretación. Es importante ser justo para poder cumplir con la ley, pero, en ocasiones, los requisitos son menos específicos que las leyes que para definirlos.

Mudra: Tanto la ley HIPAA como la Sarbanes-Oxley dejan muchos aspectos a la libre interpretación. Entre éstos, cómo transmitir las comunicaciones; qué profesional está acreditado o qué entidad está facultada para acceder a la información; qué acuerdos de negocio han de asumirse... Nuestro lema reza, simplemente: "hazlo ahora". Aunque, claro, después de evaluar los riesgos de la divulgación de información confidencial.

EC: ¿Cómo garantizar que la gestión del riesgo no afectará la innovación en TI?

Mudra: Hemos creado un comité de seguridad y privacidad de la información que analiza todas las iniciativas innovadoras que podrían tener un impacto en términos de seguridad y política de privacidad. Si identificamos un producto que está acarreado algún problema, solicitamos al fabricante un servicio de garantía del que nos podamos fiar.

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

Waschler: Llegados a este punto, hemos de revisar algunos de los fundamentos relativos a la gestión del proyecto. Necesitamos casos de negocio sólidos, cuantificar los resultados, y tener un claro entendimiento de éstos. Y es que, en este tipo de entornos, en los que las reglas de juego empiezan a ser cada vez más complejas, los problemas históricos de la gestión del proyecto empiezan a ser más importantes.

Johnson: Un gran negocio con una mínima apuesta: esto es lo que haces cuando implantas nuevas tecnologías en áreas críticas. Pero antes, debes someter dicha implantación a distintas pruebas en escenarios de bajo riesgo, con el fin de poder evaluar su impacto en todos los aspectos.

EC: Con respecto a la seguridad, ¿cuál es el mayor riesgo al que se enfrenta su empresa y de qué manera lo encara?

Guthrie: La cantidad de riesgo que proviene de fuera de la empresa se ha multiplicado por cien. No podemos permitirnos un ataque a nuestros sistemas o la infección de un virus informático que debilite los servidores, por lo que debemos encarar una protección rigurosa de nuestro perímetro. Así, contamos con soluciones de detección de intrusiones, antivirus y anti spam, entre otras.

Johnson: Las empresas punto.com son cada vez más populares y captan cada vez a más clientes, así que sólo podemos ser competitivos en la medida en que nosotros también optemos por esta modalidad de negocio. Por todo ello, además de las medidas de seguridad internas, recurrimos a agentes de auditoría externa que chequean continuamente el funcionamiento de nuestros sistemas.

EC: ¿Cómo sabe que está siguiendo el camino correcto en la gestión del riesgo?

Guthrie: Para mí, un indicador es, precisamente, el hecho de hallarme gestionando el riesgo y no el efecto de los fallos en la gestión del mismo. Si estás invirtiendo todo tu tiempo en gestionar un fallo de esta índole, ¿cómo puedes decir que estás siguiendo las pautas de seguridad adecuadas?

Mudra: Utilizo una tarjeta de puntuación en la que anoto las contingencias ocurridas durante un intervalo de tiempo determinado. Si hay alguna incidencia que consigo solventar, marco la columna del sí; en caso contrario, marco un no y, posteriormente, procedo a analizar qué es lo que ha fallado y cómo podemos actualizar nuestros recursos.

EC: ¿Cuál es el aspecto con el que hay que ser más cuidadoso en la gestión del riesgo en TI?

Mudra: Esta cuestión toca los procesos estratégicos de planificación, que para nosotros se engloban en cuatro categorías: recursos; productos y servicios; estabilidad financiera, y clientes y mercados. Analizo el riesgo en TI a través de cada una de las áreas que componen dicho plan, y estudio de qué manera afectarían las innovaciones cada una de estas categorías.

Johnson: La gestión del riesgo y la seguridad han de estar presentes en cada una de las actividades que realicemos. Así, uno de los primeros pasos consiste en cerciorarnos de que el desarrollador es consciente de los agujeros de seguridad que podría abrir una determinada línea de código. Por ello, estamos invirtiendo ingentes recursos en la formación de nuestros departamentos de desarrollo.