2. Serie de consejo comercial

No ponga en peligro su empresa

Cómo asegurar que el software tiene licencia

BSA
Business Software Alliance

¿Qué riesgos está corriendo su empresa?

En 2007, la Business Software Alliance (BSA) encargó a la firma de estudios independiente GfK NOP que investigara las actitudes de las pequeñas y medianas empresas (PYME) de Europa en relación con su percepción de los riesgos asociados con la utilización de software sin licencia (incluyendo copias falsificadas). Los resultados revelaron que un 95% de las PYMEs afirmaban tener "confianza" en que todo el software instalado tenía una licencia completa. Sin embargo, un análisis detenido de la consultora IDC muestra que la piratería de software a través de Europa permanece elevada, con unos índices en Europa occidental que llegan al 34% y en Europa central y oriental al 68%.

Esta discrepancia entre la situación percibida y la realidad sugiere una falta de concienciación entre los ejecutivos de las empresas en lo concerniente al software y la gestión del mismo. Esta situación es peligrosa. El software se ha convertido rápidamente en uno de los activos comerciales más valiosos y críticos que poseen las empresas y si éstas no invierten en sus activos de software y los protegen y gestionan adecuadamente, se quedan expuestas a numerosos riesgos comerciales que pueden tener implicaciones financieras sustanciales.

La BSA ha elaborado esta guía para esbozar los riesgos reales del software sin licencia (pirateado, con licencia inapropiada o con menos licencias de las utilizadas), cómo se puede proteger la empresa y cómo conseguir el máximo beneficio del software utilizado.

Definiciones:

Software sin licencia: cualquier producto de software que se haya instalado en un PC cuando el contrato de licencia no permita o soporte dicha instalación o no se haya realizado un contrato de licencia / uso con el propietario de los derechos de autor. En este documento, el término "software sin licencia" se utiliza para hacer referencia a las tres formas de infracción de derechos de autor de software que se listan a continuación.

Software con menos licencias de las utilizadas: software que se ha instalado en más ordenadores de los permitidos por el contrato de licencia. Por ejemplo, una licencia puede permitir que el software se instale en 20 ordenadores. Si dicho software se ha instalado en 30 ordenadores, las diez instalaciones adicionales se consideran "sin licencia".

Software con licencia inapropiada: software que se utiliza para fines no permitidos de acuerdo con el contrato de licencia. Por ejemplo, software con licencia para uso académico que se utiliza con fines comerciales.

Software pirata: cualquier software que haya sido copiado deliberadamente (en un volumen sustancial) para defraudar a los propietarios de los derechos de autor mediante la distribución ilegal, bien por medio de CD o a través de sitios de descarga en Internet. Esto incluye el "software falsificado".

Introducción

Para muchas PYMEs, el mundo de la gestión de los riesgos está cambiando con gran rapidez y centrándose más en la administración y la transparencia y en un aparente empuje implacable hacia una regulación más estricta. Muchos se sienten bombardeados por el flujo continuo de mensajes que animan a mejorar la gestión de riesgos. Pero, ¿cuáles son los beneficios comerciales?, ¿por qué se debería prestar atención a aspectos de gestión de riesgos como la administración del capital de software y la seguridad de la información?

Las PYMEs constituyen la inmensa mayoría de las compañías de todo el mundo. En Europa representan bastante más de la mitad de la riqueza generada anualmente y emplean a la inmensa mayoría de los trabajadores de los países. Resistirse a admitir o a prepararse para una interrupción importante en las operaciones deja a muchas firmas en situación potencialmente vulnerable incluso a una interrupción de menor cuantía, poniendo a riesgo, de manera colectiva, decenas de miles de puestos de trabajo y amenazando a las otras numerosas empresas con las que interactúan en calidad de proveedores o clientes.

Los directivos de las PYMEs están acostumbrados a abordar los retos comerciales que suponen el cambio de precios de suministro, los nuevos competidores y las exigencias de los clientes. La familiaridad con tales desafíos cotidianos puede engendrar un exceso de confianza en la capacidad de la empresa a hacer frente al desastre, incluso si es a pequeña escala.

Tampoco se puede subestimar el impacto total de un incidente de interrupción comercial. Un estudio realizado por Gartner Consultants sugiere que el 40% de las empresas fracasan en el plazo de cinco años siguiente a sobrevivir una interrupción importante de las operaciones comerciales. En un estudio anexo, se sugiere que las empresas que tardan más de treinta días en recuperar las operaciones comerciales normales tienen una “gran probabilidad” de quebrar.

Dada la acrecentada concienciación que existe hoy en día acerca de la vulnerabilidad, tal vez resulte sorprendente que haya tantas empresas que no estén preparadas para las interrupciones comerciales. Este hecho generalmente se reconoce, pero apenas se habla de ello.

Nuestra investigación en Henley muestra que un factor significativo para las compañías que eligen invertir en actividades de gestión de riesgos es el peso de las fuentes de amenaza que perciben. No obstante, y como los directivos de las PYMEs saben bien, los beneficios son las recompensas de la exitosa toma de riesgos comerciales. El riesgo comercial, como un componente esencial de las ganancias, resulta inevitable.

Gestionar los riesgos no se trata simplemente de reducir los mismos. También implica comprender el apetito de la firma por los riesgos y mitigar los mismos mediante la reducción de su probabilidad y/o impacto en la medida de lo posible sin inhibir los negocios de la firma. Con los riesgos gestionados de una manera óptima, la firma puede tolerar con seguridad la exposición, incrementando las ganancias potenciales sin exceder el apetito de riesgos. La buena gestión de los riesgos incrementa la resistencia de la firma.

Muchas firmas no saben reconocer el papel que desempeña el riesgo en las operaciones comerciales. Las empresas mayores tienen un enfoque estructurado a la inversión en nuevos proyectos, factorizando el riesgo en expectativas de beneficios. Sin embargo, las firmas más pequeñas no pueden aplicar siempre unos métodos tan rígidos, dejándoles potencialmente con un exceso de exposición a medida que van creciendo.

Ya se trate del resultado de un enfoque del director gerente en el flujo de dinero o del deseo de escalar, las firmas más pequeñas podrían estar arriesgando el sustento de toda la empresa al crecer sin tener en cuenta la gestión de los riesgos.

Esto está teniendo impacto en la gestión de riesgos de la seguridad de la información y el escenario se complicará más en un futuro cercano con la emergencia de tecnologías nuevas. El desarrollo y la implementación de tipos nuevos de mecanismos de distribución de informática y software tendrán un impacto importante en los requisitos exigidos en los enfoques de valoración de riesgos.

Lo último, pero no por ello lo menos importante, es que no deberíamos olvidar que son los riesgos percibidos directamente los que se abordan usando el juicio (riesgos como, por ejemplo, cruzar de acera). Desgraciadamente, demasiados de los riesgos asociados con el software se siguen percibiendo como “virtuales”. Si bien la mayoría de los directores de las PYMEs habrán experimentado un disco duro averiado o un virus informático, pocos habrán tenido que afrontar consecuencias de gran gravedad. Si bien pocos de los desastres importantes se pueden ligar con el software, sí han sucedido en organizaciones tanto grandes como pequeñas.

Las implicaciones legales de operar con software sin licencia pueden ser sustanciales pero lo que tal vez se divulgue menos es que operar con software con licencia significa el tener acceso a asistencia técnica, mayor protección contra virus o malware y, consecuentemente, menos interrupciones. En un mundo en el que la continuidad comercial es un factor clave, las PYMEs tienen menos capacidad que las grandes empresas para capear el temporal de las interrupciones comerciales. Por lo general, no tienen la misma resistencia inherente que las organizaciones grandes, las cuales poseen varios locales, reservas de efectivo y fuentes de asesoría externa. Como muestra la investigación y el consejo dados en este informe, a menudo son las firmas pequeñas de rápido crecimiento las que no prestan la atención debida a las actividades de gestión de riesgos importantes, como las auditorías de licencias de software. Sin embargo, son las más vulnerables.

Como se indica en esta guía, el incremento en el reconocimiento de esta vulnerabilidad parece ser lento, según se deduce de la falta de actividad y preparación reportada. ¿Qué se puede hacer al respecto? y ¿qué se debería hacer? Yo sugiero que necesitamos mostrarnos más abiertos con respecto a las consecuencias de la mala gestión de los riesgos y de los beneficios de una buena gestión de los riesgos.

Con demasiada frecuencia ocultamos los problemas porque tememos que vayan a tener un impacto negativo en nuestra reputación. Sin embargo, solamente comunicándonos con nuestros colegas podemos desarrollar estrategias eficaces de gestión de los riesgos en los que la atención de gestión recaiga en aquellas pocas actividades verdaderamente importantes y asegurar que sigamos cosechando los frutos de la toma de riesgos comerciales y evitar los peligros de una toma de riesgos desacertada.

Esta guía contribuye a este esfuerzo de comunicación. En lo que se refiere a la licencia de software, la ecuación riesgo-recompensa en realidad es muy simple.

Las ventajas de la licencia completa de software son muy elevadas en lo concerniente a la operación y reputación. Las recompensas de las licencias inadecuadas no sólo son muy reducidas sino que son ingestionables y se encuentran en la raíz de un riesgo incluso mayor.

Jean-Noel Ezingeard,
Henley Management School.

Software y riesgo comercial

El software es uno de los activos más valiosos que posee una empresa. Estudios realizados recientemente por la BSA revelaron que el 94% de las empresas de Europa citan las tecnologías de la informacións como una parte esencial de la operación exitosa de sus empresas.[1] El software especializado permite que empresas de arquitectura, ingeniería, financieras y de diseño compitan e innoven. Pero incluso en las prácticas comerciales cotidianas casi todas las empresas confían en hojas de cálculo para administrar las actividades financieras; bases de datos para guardar información crucial; correo electrónico para comunicarse (con colegas, clientes y proveedores), y paquetes de autoedición para crear presentaciones y material de marketing colateral.

Por lo que resulta sorprendente enterarse de que el 36% del software de las empresas de la Unión Europea se utiliza sin una licencia válida.[2]

La ignorancia del estado de las licencias de software de una empresa no sirve como defensa, por lo que resulta crucial que las organizaciones conozcan perfectamente tanto los riesgos que representa para sus empresas la piratería de software como los pasos que pueden tomar para evitar dichos riesgos y asegurar que actúan legítimamente.

Al igual que una empresa tiene que administrar adecuadamente a sus empleados en cierto marco legislativo, lo mismo sucede con el software que utiliza. Si bien la mayoría de las empresas están al tanto de –y disponen de procesos para abordarlos– los reglamentos financieros y las directivas de RRHH, también son responsables ante sí mismos y ante los accionistas de administrar cuidadosamente su capital de software y fomentar un nivel apropiado de concienciación en sus empresas.

[1] Fuente: Estudio de "Riesgo comercial" de GfK NOP, 2007
[2] Fuente: Estudio de "Piratería de software" de IDC, 2007

Esto puede resultar un reto al principio, especialmente si la organización crece rápidamente o se dan cambios sustanciales en la estructura de la empresa. No obstante, y conjuntamente a la toma en consideración de cómo trabajar y comunicarse con los accionistas y los empleados, analizar cambios potenciales del estado financiero y revisar contratos con proveedores y clientes, también se debe emplear tiempo en requisitos relativos a la gestión de software. A largo plazo, se comprobará que este tiempo estuvo bien empleado.

La gestión de software bien implementada no es sólo cuestión de evitar los riesgos que pueda ocasionar a la empresa el uso de software sin licencia, sino que también puede aportar ganancias de eficacia y ahorros de costes y no exclusivamente en cuanto al gasto directo en software sino también en los costes de proceso e infraestructura relacionados.

Los beneficios de una gestión eficaz del software son amplios: puede colocarle en una posición mejor cuando negocia con proveedores de software y le asegura que dispone de la información necesaria para sentirse con confianza cuando realice contratos de compra de software.

Una correcta gestión del software permite una planificación más estratégica, al tiempo que reduce la tarea administrativa del Departamento de TI y la carga en servicios de soporte con costes asociados.

El Departamento de TI o los servicios de soporte disponen de más capacidad para controlar a qué software tienen acceso los empleados, incluyendo la capacidad de los mismos de introducir software no autorizado en la red.

El impacto económico

La piratería de software no sólo tiene un impacto negativo en el entorno comercial, sino que existen implicaciones de mucho mayor alcance para la economía en general. La piratería frena ingresos que los proveedores de software invertirían en investigación y desarrollo, así como en puestos de trabajo. Dado que el software desempeña un papel crucial en la economía de la información, esto crea un efecto residual e impacta en otras partes del sector informático y en la economía general.

La industria de las tecnologías de la información no sólo da empleo a cientos de miles de personas y contribuye sustancialmente al PIB, sino que también estimula la productividad en la mayoría de las empresas. Consecuentemente, resulta crucial que las empresas reconozcan el valor del software y aseguren que cada pieza del mismo sea legal y posea una licencia adecuada.

La mejor práctica y un enfoque experto en la responsabilidad social corporativa fomentan la idea de juego justo y comportamiento ético de las empresas, así como la necesidad de proteger a todas las partes interesadas de éstas, incluyendo aquellas compañías que desarrollan el software que resulta vital para ellas.

Software sin licencia: ¿cuáles son los riesgos?

Una quinta parte de las PYMEs de Europa creen que "no existe riesgo" en instalar, descargar o utilizar software sin licencia, de acuerdo con un estudio encargado por la BSA[3]. Sin embargo, esta práctica conlleva muchos riesgos comerciales inherentes y la presunción de que no existe riesgo, así como la creencia de que utilizar software sin licenciar no sea algo por lo que haya que preocuparse, constituye una tendencia preocupante. El hecho de no entender los riesgos asociados al software sin licencia puede exponer la empresa a numerosos peligros.

Las consecuencias de utilizar software sin licencia para una empresa pueden ser de carácter operacional, técnico, financiero y legal.

[3] Fuente: Estudio de "Riesgo comercial" de GfK NOP, 2007

Riesgos operacionales y técnicos

Pérdida y corrupción de datos

Estudios realizados por IDC[4] han revelado que el software pirateado adquirido mediante descargas ilegales o CDs falsificados tienen un cincuenta por ciento de posibilidades de contener "código adicional" como troyanos, virus o spyware, que puede hacer fallar los sistemas informáticos o exponer datos comerciales confidenciales a intrusos. Además, el software pirateado podría no ofrecer parches de seguridad. Sólo en algunos casos, al software sin licencia se le puede aplicar parches críticos. Los tiempos de inactividad y las infracciones de seguridad pueden tener efectos negativos inmediatos en el saldo final.

Pérdida de funcionalidad

Además de los riesgos de seguridad de utilizar software pirateado descargado de sitios web o redes P2P, dicho software suele ser subestándar o puede provocar pérdida de funcionalidad y problemas de compatibilidad que no se encontrarían en versiones legales con licencia. Las copias sin licencia podrían no recibir todas las actualizaciones de los proveedores. Esto significa que sus empleados no serán capaces de utilizar el software en toda su capacidad, dando ventaja a los competidores, ya que pueden responder más rápida, completa o eficazmente porque poseen las herramientas que requieren. También existe el riesgo de que los datos se corrompan o no se guarden correctamente, conduciendo a una pérdida de datos crítica.

Falta de asistencia técnica

Con la intensa dependencia de las operaciones comerciales en la tecnologías de la información, resulta crítico que estén implementados los sistemas de asistencia relevantes. Los usuarios de software sin licencia a menudo no disponen de acceso a la asistencia técnica crítica proporcionada por los vendedores y, como consecuencia, el software funciona de manera más eficaz.

Daño a la reputación

Aunque resulta difícil de cuantificar, el daño innegable que supone a la reputación de una empresa el hecho de que se descubra que opera con software ilegal constituye un riesgo real: piense en el impacto si sus clientes no estuviesen obteniendo el nivel de servicio que esperan. De hecho, una encuesta realizada en el Reino Unido mostró que el 42% de las personas opinaban que si sus clientes supieran que usaban software ilegal serían menos propensos a realizar transacciones con ellas.[5]

[4] Fuente: Estudio de "Los riesgos de obtener y utilizar software pirateado" de IDC, 2006
[5] Fuente: Estudio de "Ética corporativa" de YouGov, 2006

Riesgos financieros y legales

Penas legales

El desarrollo de software implica años de inversión. Combina ideas y talentos de programadores, escritores y artistas gráficos. Al igual que la mayoría de las obras creativas, el software de ordenador está protegido por leyes de derechos de autor y estas leyes las deben respetar los usuarios para que la industria del software siga innovando.

Cuando compra software no se convierte en el propietario de los derechos de autor. Más bien, al comprar una licencia se convierte en el concesionario de los derechos de autor, con derecho a utilizar el software bajo ciertas condiciones impuestas por el propietario de los derechos de autor, por lo general el editor del software. La licencia es un documento legal que define las condiciones de uso de un producto de software dado. Si una empresa infringe las condiciones de un contrato de licencia –como copiar, distribuir o instalar software en una manera que esté prohibida por la licencia, ya sea intencionadamente o no– está infringiendo los derechos de autor y cometiendo un delito. Las penas civiles y penales varían a lo largo de Europa pero pueden acarrear multas elevadas.

Costes de ser descubierto

Si se sospecha que utiliza software sin licencia, la BSA entrará en acción. Si se le halla culpable de infringir la legislación de derechos de autor de software por tener software sin licencia instalado en ordenadores de la empresa, ésta se enfrentará a un pago de daños sustanciales, así como costas legales. La empresa también tendrá que comprar las versiones legales del software que requiera para poder seguir operando.

Multas

En función del sector en que opere, el software sin licencia puede dejarle encarando multas de una serie de organismos como autoridades financieras, organismos de aplicación de la ley o de protección de datos, etc. Muchos de estos organismos tienen criterios que determinan procesos aceptables y dichos procesos se pueden ver impactados por tener software sin licencia, dejando la empresa expuesta a multas financieras adicionales.

Costes de rectificar un problema

Si se descubren empresas con software ilegal, a menudo tendrán que eliminar todas las versiones sin licencia, lo que significa que tendrán que sustituir el software sin licencia requerido por versiones legales. Simplemente, no merece la pena correr este tipo de riesgo por recortar gastos cuando se trata de licencias de software, por no mencionar la perturbación que podría causar a la empresa el hecho de tener que enfrentarse a un juicio potencial.

¿Cómo llega software sin licencia a los ordenadores de su empresa?

El software sin licencia de las empresas puede proceder de una serie de fuentes: descargas no autorizadas por parte de los empleados, descargas ocultas en cuadros emergentes lanzados por visitar ciertos sitios web y una mala gestión de las licencias de software son solamente algunos ejemplos. Las causas de tales equivocaciones a menudo son fruto de una falta de concienciación entre los ejecutivos y empleados de la empresa, unas políticas de informática inadecuadas y deficientes procesos de gestión de software. Desgraciadamente, en algunos casos la utilización de software sin licencia es deliberada, estando la directiva totalmente al corriente de la situación pero aún sin darse cuenta de los riesgos asociados.

En la sección que lleva por título "Cómo reducir los riesgos" se trata de los enfoques para combatir los retos que se relatan a continuación.

Mala gestión de software y de licencias de software

Comprender la importancia del software, los tipos de software disponibles y las tres diferentes formas de licencia de software puede tener un impacto significativo en la forma en que opera y se expande la empresa y, consecuentemente, se debería tomar en consideración a la hora de tomar decisiones comerciales. Si se incrementa la concienciación sobre los activos de software de la organización y se asegura que dichos activos se administran y protegen totalmente, los mismos se pueden utilizar de una manera más eficaz para mejorar la productividad y la eficacia.

Hay disponible una variedad de licencias de software para diferentes requisitos: desde el sencillo formato de "haga clic para aceptar" hasta los acuerdos negociados más complejos. La flexibilidad prosigue aumentado año tras año. Muchas licencias estándares permiten la instalación en uno a cinco ordenadores, mientras que los contratos de licencia de volumen por lo general permiten realizar una serie determinada de instalaciones desde un CD maestro. Cualesquiera instalaciones superiores a los niveles fijados se deben acordar con el editor del software o con el distribuidor. Con demasiada frecuencia, la ausencia de registros precisos de las instalaciones o de políticas empresariales rigurosas significa que las empresas pueden acabar infringiendo la ley.

La infralicencia sucede cuando el software se utiliza en más ordenadores de los que permite la licencia y es una consecuencia habitual de la gestión de software y licencias de software ineficaz. Si la licencia permite la instalación del software en 20 ordenadores, cualquier instalación del software realizada en más ordenadores infringe las condiciones de la licencia. En efecto, se trata de una copia ilegal y si se le descubre con un software sin licencia se enfrenta a unos riesgos significativos, como se esboza anteriormente.

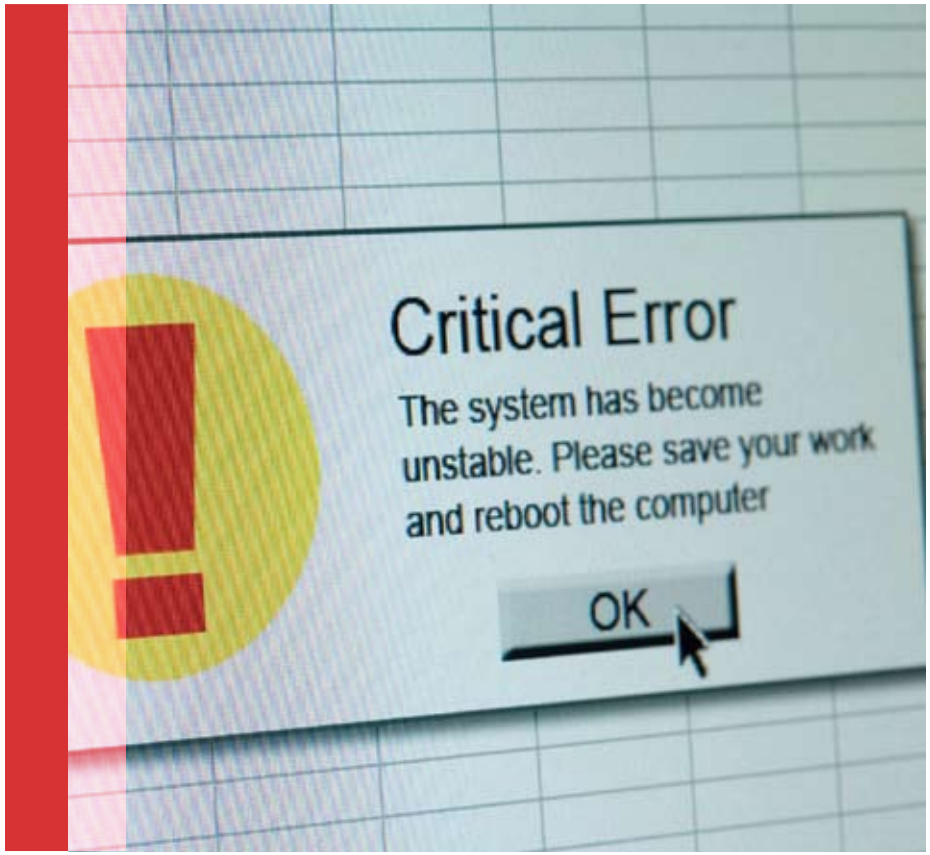
Descargas por Internet

Internet es una herramienta comercial inestimable en la que muchas organizaciones confían intensamente. No obstante, también introduce la posibilidad de descargar a los ordenadores de la empresa software no deseado ni aprobado, a no ser que estén implantados los controles apropiados.

A medida que se ha hecho más rápido el acceso a Internet, resulta mucho más sencillo comprar y/o descargar música, películas y otros multimedia. Cada vez resulta más fácil transferir productos entre ordenadores sin necesidad de medio físicos y con poco riesgo de detección. La piratería, que en el pasado requería una comprensión de códigos informáticos complejos, ahora se puede realizar con sólo hacer clic con el ratón.

Sin tecnología de bloqueo presente para prevenir dichas descargas no autorizadas, la empresa está vulnerable a la descarga de software por parte de los empleados sin su conocimiento o consentimiento.

Hay una serie de riesgos inherentes a esta actividad. Si un empleado ha instalado software sin licencia, el propietario o el director gerente de la empresa siguen siendo responsables de la infracción de derechos de autor y la empresa todavía tendría que enfrentarse a riesgos legales y financieros. Si no se conoce la fuente del software, entonces el software descargado podría contener virus, spyware o troyanos a los que se ha dado acceso directo a sus redes informáticas.



También existe cada vez más riesgo con los "cuadros emergentes" que aparecen cuando un empleado visita ciertos sitios web: frecuentemente los que ofrecen descargas de software o imágenes a precios de ganga. A veces estos actúan como una fachada de actividades ilegales e instalarán software, virus o spyware en el ordenador engañando al empleado para que haga clic en el cuadro emergente.

Sitios de subasta por Internet

Uno de los mayores éxitos de Internet han sido sin duda los sitios de subasta. En ellos la gente puede vender online libros, juguetes, artículos de coleccionistas e incluso casas. La flexibilidad, la velocidad y el éxito de dichos sitios es un testimonio no sólo de su popularidad sino también de los beneficios que ofrecen tanto a compradores como a vendedores. No obstante, entre la mayoría de las ofertas honestas y genuinas hay trampas para el comprador no precavido. Los precios muy baratos de software aparentemente genuinos pueden resultar tentadores para las empresas pequeñas y en crecimiento que buscan recortar costes. No obstante, la capacidad de ocultar la identidad o crear una falsa ha llevado a muchos a utilizar este medio para actividades ilegales y los sitios de subastas se han convertido en un vehículo idóneo para aquellos que buscan vender software sin licencia o pirateado.

Un estudio realizado en 2006 por analistas de IDC reveló que, en realidad, menos del 49% del software de Microsoft ofrecido en eBay era original.[6]

Una vez que se ha dado cuenta de que ha comprado software ilegal puede resultar muy difícil lograr compensación. Muy pocos de los consumidores "embaucados" que han presentado quejas han recibido reembolso de su compra. Y de aquellos a los que sí les devolvieron dinero –por lo general después de dedicar mucho tiempo y esfuerzo para llevar a cabo las reclamaciones – las devoluciones monetarias que recibieron no llegan a lo que pagaron por los artículos pirateados.

[6] Fuente: Estudio de "Los riesgos de obtener y utilizar software pirateado" de IDC, 2006

Trabajo móvil

Los trabajadores de todo el mundo cada vez realizan más a menudo tareas fuera de la oficina, con lo que los empresarios les equipan con una serie de dispositivos para que trabajen más eficazmente desde casa o en otras ubicaciones. Pero esta mayor libertad viene acompañada de nuevos retos: la proliferación de dispositivos utilizados para trabajar fuera de la oficina ha incrementado las oportunidades de que disponen los empleados de descargar software ilegal a las redes de las empresas. La empresa sigue siendo responsable del software instalado en los ordenadores portátiles ya que estos siguen siendo recursos corporativos. Lo mismo se aplica a los ordenadores que los empleados pueden utilizar en casa si éstos son propiedad del empresario.

En consecuencia, cualquier política que tenga una empresa en cuanto al uso de Internet tendrá que incluir el uso en el hogar de los activos de la empresa.

Proveedores fraudulentos

Existe una pequeña minoría de proveedores de software que adaptan las normas a beneficio propio y venden mercancía ilegal a sabiendas.

Muchas PYMEs subcontratan la gestión informática a proveedores externos, por lo que es crucial comprobar cuidadosamente las credenciales del proveedor de software.

Asegúrese de que su proveedor o distribuidor de software obtiene el mismo de canales de distribución autorizados.

Puede comprobar fácilmente los métodos de distribución poniéndose en contacto directo con los editores del software y preguntándoles quiénes están autorizados a distribuir sus productos.

Modo de reducir los riesgos

Hay una serie de medidas que puede tomar su empresa para reducir al mínimo los riesgos que plantea el software sin licencia.

Auditorías regulares y políticas de uso eficaces

Esto no es un "asunto de tecnología" sino de carácter comercial, lo que a menudo se puede resolver mediante la mejor práctica comercial. Dados los riesgos, resulta fundamental obtener una toma de posición a nivel comercial para implementar ciertos procesos.

Como mínimo, todas las empresas deberían auditar regularmente el software instalado en sus ordenadores y deberían tener implementadas políticas de empleados en lo concerniente al uso aceptado de la tecnología de la empresa (incluyendo la tecnología utilizada en el hogar o las tecnologías portátiles utilizadas por el empleado pero que son propiedad de la empresa). Debería quedar claro que las políticas se harán cumplir y que, en la medida de lo posible, los responsables de recursos humanos deberían estar involucrados para asegurar el éxito.

Gestión de activos de software

Sorprendentemente, una tercera parte de las PYMEs no ha oído hablar de la Gestión de Activos de Software.[7]

La Gestión de Activos de Software (SAM por sus siglas inglesas) es una metodología que ayuda a las empresas a definir e implementar procesos para optimizar su inversión en software. Mediante el SAM, que es lo suficientemente flexible para que lo puedan utilizar las empresas de cualquier tamaño y en cualquier fase de desarrollo, se pueden identificar los puntos en los que la empresa puede ser vulnerable a los riesgos tratados anteriormente y asegurar que estén implantados los procesos para mitigar o prevenir que se convierta en una víctima de los citados riesgos.

El SAM implica reunir a los empleados, los procesos y, cuando así se requiera, la tecnología para asegurar que los activos de software se gestionan, protegen y utilizan de la manera más eficaz y eficiente posible. Además, se hace un seguimiento, una evaluación y una gestión sistemáticos de las licencias y utilizaciones. Los beneficios comerciales del SAM pueden ser sustanciales: además de aportar tranquilidad, puede reducir los gastos en tecnologías de la información y permite que las organizaciones planeen y presupuesten de manera precisa los requerimientos de software, incluyendo los programas nuevos y las mejoras de licencia.

Para desarrollar el SAM de una manera eficaz en la empresa, se pueden tomar una serie de medidas. No se tienen que poner en práctica todos estos elementos desde un principio –cada uno aportará algunas mejoras– pero el punto de partida deberá ser reconocer que el software es un activo crítico y la gestión del mismo un asunto comercial clave.

[7] Fuente: Estudio de "Riesgo comercial" de GfK NOP, 2007

Ocho pasos para implementar la gestión de activos de software:

1

Obtener apoyo en toda la empresa

La implementación del SAM representa un cambio cultural significativo: resulta crucial asegurar que tanto los directivos principales como los usuarios finales apoyen el proyecto y comprendan la necesidad del SAM.

2

Nombrar a un responsable de activos de software

A no ser que se tenga una persona que supervise el software de toda la empresa, resulta muy difícil hacer un seguimiento de los activos de software. Dicho responsable no tiene por qué ser del departamento de tecnologías de la información pero, dependiendo del tamaño de la organización, la persona más indicada es la que tenga a su cargo la administración de las tecnologías de la información y, consecuentemente, participe en las compras de software. Si sólo hay una persona responsable de las tecnologías de la información –lo que a menudo es el caso en las firmas más pequeñas– hágase esta función uno de los cometidos claros y definidos de la descripción del puesto de trabajo.

3

Auditar el software y el uso de licencias actuales

Se necesitará hacer un inventario de los activos de software actuales para saber exactamente qué software opera en la empresa y las licencias requeridas para este software.

Sólo sabiendo qué software está instalado y el número de ordenadores que tiene la empresa y si hay algunas copias de programas que hayan podido instalar lo empleados, se estará en disposición de identificar los riesgos y problemas potenciales y tomar medidas para contrarrestarlos.

4

Crear una base de datos de gestión de activos de software

Tener una buena base de datos para almacenar toda la información relacionada con el software es un factor crucial para que la estrategia del SAM tenga éxito. Podría usar una hoja de cálculo o invertir en algo diseñado para la tarea. De una manera o de otra, esto resultará inestimable.

5 Centralizar la compra y distribución del software

Si no existe una visión única de los gastos en software o las responsabilidades de compra, será prácticamente imposible conseguir los beneficios completos del SAM.

6 Establecer políticas y procedimientos

Controlar cómo entra en la empresa el software es una de las mejores medidas preventivas que se pueden tomar. Una política para los empleados clara y aplicada que abarque lo que se permite y lo que no, ayudará a mantener la situación bajo control.

Asegurar que los empleados entienden completamente y apoyan las estrategias de gestión de activos de software significará que se está más cerca de controlar el entorno en el que se introduce software en la organización.

7 Revisar periódicamente

Téngase en cuenta que el SAM es un proceso continuo que precisará un control mediante auditorías periódicas con el fin de funcionar de una manera regular y eficaz.

8 Utilizar un consultor imparcial para que asesore en el proceso

Para ayudar a las empresas que deseen evitar los riesgos del software sin licencia, la BSA ha creado un recurso online en su sitio web (www.bsa.org) que proporciona consejo y herramientas para la gestión del software. Para más información, visite el sitio de Herramientas y Recursos.

¿Qué sucede si piensa que podría encontrarse en riesgo?

Las empresas deberían tratar el software como cualquier otro activo valioso. Si se toman medidas y se implementan las sugerencias aquí expuestas, se pueden gestionar los riesgos comerciales asociados con el software ilegal y cosechar los frutos de un entorno de tecnologías de la información más eficaz.

No obstante, si le preocupa que su empresa esté en riesgo debido al software ilegal, hay una serie de organismos con los que puede ponerse en contacto para obtener ayuda. Los primeros puntos de contacto deberían ser los distribuidores y vendedores para que le contesten cualquier pregunta que pudiese tener en relación con las licencias de software.

Otras herramientas disponibles en el sitio web de la BSA comprenden:

1

Guía de gestión y licencias de software:
Hay folletos disponibles para descargar en siete idiomas, diseñados para ayudar a las empresas a implementar procedimientos de gestión de software y clarificar las cuestiones de cumplimiento de las licencias.

2

Lista de proveedores de gestión de recursos:
Una lista de los principales proveedores y consultores de software que pueden ayudar a las empresas con los temas de licencias y la implementación de programas de gestión de software.

Lleve a cabo una revision de estado gratuita y on line

La herramienta Revisión de estado la desarrolló BSA para ayudar a las empresas a identificar, entender y gestionar los activos de tecnologías de la información de una manera más eficaz. En unos pocos minutos puede:

1. **Realizar un análisis de la posición de su software actual en cuanto a gestión**
2. **Resaltar áreas de vulnerabilidad potencial**
3. **Recomendar mejoras**
4. **Generar un informe de revisión de estado para sus archivos**

http://global.bsa.org/healthchecktool

Apéndice: Hallazgos clave del estudio de Gfk NOP

En 2007, la BSA encargó un estudio paneuropeo para investigar las actitudes de las PYMEs en cuanto a la piratería de software y descubrir si se entendían bien los riesgos asociados a la utilización de software ilegal.

1. El 94% de las PYMEs europeas afirman que las tecnologías de la información son "muy" o "bastante" importantes para la capacidad de sus empresas de operar con éxito.

2. A lo largo de Europa (sin incluir a Rusia), una quinta parte de los encuestados creen que el uso de software sin licencia "no conlleva riesgo".

3. El 87% no se dan cuenta de que el uso de software ilegal podría hacerles más vulnerable a los virus.

4. El 97% no considera un problema tener que utilizar versiones antiguas de software debido a no poder actualizarlas por tratarse de versiones ilegales.

5. El riesgo más común citado por los encuestados es "actos procesales penales" (23%), seguido de "multas financieras" (21%). Sólo un 3% afirmó que "tener que operar con versiones antiguas/no actualizables" suponía un riesgo, a pesar de la amenaza comercial de los competidores con las soluciones más recientes.

6. No obstante, el doble de las PYMEs de Europa central y oriental y Rusia hacen referencia a "la pérdida/corrupción de datos" como un riesgo derivado de la utilización de software sin licencia, comparado con las empresas de Europa occidental. En Rusia, "el fallo de software" se contempla como un riesgo por parte de un 27% pero sólo el 8% de las empresas de Europa occidental compartían esta opinión.

7. Las PYMEs mayores (100 – 250 empleados) son más proclives a tener implantada alguna forma de proceso para gestionar el uso de software (37%), comparado con las PYMEs más pequeñas (19%).

8. En general, el método favorito de controlar y gestionar el uso del software es mediante "auditorías periódicas de los ordenadores de los empleados" (33%), situándose en segundo lugar (25%) la "política empresarial".

La investigación

El estudio lo realizó Gfk NOP en representación de la BSA mediante encuestas telefónicas de 1.800 pequeñas y medianas empresas de diferentes países europeos: Reino Unido, Francia, Alemania, Países Bajos, Italia, España, Rusia, Polonia y Hungría.

Se realizaron 200 encuestas en cada uno de los países. Para los fines de este estudio, las PYMEs se definieron como empresas de entre 10 y 250 empleados.

Sede central internacional de BSA
1150 18th Street, NW
Suite 700
Washington, DC 20036
EE. UU.
Teléfono: +1 202 872 5500
Fax: +1 202 872 5501

BSA Europa, Oriente Medio y África
2 Queen Anne's Gate Buildings
Dartmouth Street
Londres SW1H 9BP
Reino Unido
Teléfono: + 44 (0) 20 7340 6080
Fax: + 44 (0) 20 7340 6090

BSA Pacífico asiático
300 Beach Road
#25-08 The Concourse
Singapur 199555
Teléfono: + 65 6292 2072
Fax: + 65 6292 636

http://www.bsa.org

Business Software Alliance (BSA) es la voz de la industria mundial del software comercial y del hardware asociado ante los gobiernos y en el mercado internacional. Sus miembros constituyen una de las industrias de crecimiento más rápido del mundo. Los programas de BSA fomentan la innovación tecnológica a través de las iniciativas de educación y política que promueven la protección de los derechos de autor, la ciberseguridad, la industria y el comercio electrónico.