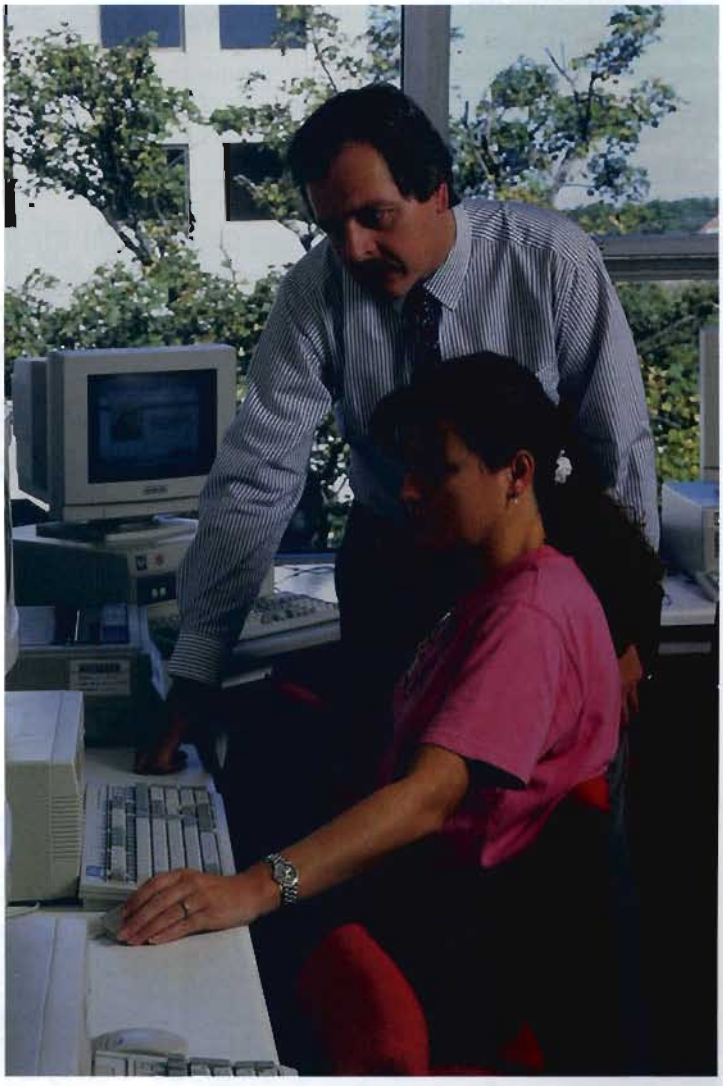
COMO ESTABLECER UNA POLITICA PARA EL MANEJO DEL CORREO ELECTRONICO

El correo electrónico que entra y sale de su organización puede estar afectando la productividad y sus utilidades. Pero si usted no entiende la responsabilidad que puede derivarse del mismo, este canal de comunicación podría entorpecer o, incluso, destruir su negocio.

En una entrevista reciente, Michael R. Overly, asesor especial para el departamento de tecnología de información de la firma estadounidense de abogados, Foley and Lardner de Los Angeles y autor del libro "E-Mail Policy: How to Develop Computer, E-mail and Internet Guidelines to Protect your Company and its Assets " (política de correo electrónico: cómo desarrollar políticas sobre el uso de computadoras, correo electrónico e Internet para proteger a su empresa y a sus activos), de la casa editorial AMACOM Books. habló de cómo una política clara sobre el uso del correo electrónico puede reducir o eliminar los peligros asociados con su flujo de comunicaciones.



¿Cuáles podrían ser las implicaciones cuando los empleados abusan del privilegio de usar el Internet, por ejemplo, mandando un exceso de mensajes personales?

El solo hecho de abrir "junk e-mail" (es decir, mensajes electrónicos "basura" como ofertas y promociones) puede costar caro. Por citar un caso, una multinacional descubrió que el correo electrónico basura recibido por sus empleados le estaba costando diariamente la suma de un dólar por empleado. Es mucha plata, si se tiene en cuenta que esta organización tenía ¡50.000 empleados! Cuando los empleados se dedican a usar el Internet durante largos períodos de tiempo, por motivos personales, las empresas y los departamentos también sufren pérdidas importantes en cuanto a la productividad y los recursos computacionales. De hecho, uno de los problemas más graves ocurre cuando un empleado descarga o intercambia archivos de gran tamaño a través del Internet. Esto puede crearle una gran carga a la red de una empresa, especialmente si se trata de archivos con imágenes o sonido.

¿Nos puede dar un ejemplo de cómo la descarga de un archivo puede socavar el sistema de una organización?

El Informe Starr es un buen ejemplo. En una empresa, un empleado descargó el documento, luego lo envió por toda la organización. Tenía mil copias de un informe de más de 500 páginas circulando por toda la red de la empresa, devorándose el espacio de almacenamiento. Algo así ejerce una enorme presión sobre un sistema.

¿Cómo puede protegerse una organización contra este tipo de abusos?

Puede instalar un software que alerte sobre la existencia de mensajes descargados del internet que tengan "attachments" o anexos de un tamaño exagerado. Cuando escriba su política sobre el uso del Internet, debe aclarar qué ítems no se pueden almacenar en el sistema. Adviértale a los empleados sobre el envío de "cartas cadena" por correo electrónico. Si necesitan descargar grandes archivos, pídales que lo hagan después del horario normal de trabajo, para evitar una sobrecarga del sistema.

¿Cuáles son algunas de las responsabilidades de índole legal que se derivan del uso del Internet, que deben ser tomadas en cuenta por las organizaciones?

"Un empleado envío mil copias del informe Starr. Algo así puede socavar el sistema de una empresa".

Si el correo electrónico de una organización se utiliza para distribuir mensajes ofensivos, de tipo sexual o racial, la empresa puede ser responsable. Esto aplica tanto si los mensajes son dispersados por el mismo gerente o por un empleado, como si son enviados a un tercero fuera de la empresa.

Supongamos que el supervisor o la organización desconoce la existencia de este material ofensivo. ¿Acaso no es cierto que una persona tiene que registrar la queja o llamar la atención sobre el acoso antes de que la organización sea responsable?

En Estados Unidos, algunas Cortes han fallado afirmativamente. En otros casos, han fallado lo contrario, en el sentido de que es necesario que exista una vigilancia. En los últimos dos años, dos decisiones de la Corte Suprema en este país determinaron que los empleadores pueden establecer una defensa contra cargos de responsabilidad por acoso sexual siempre y cuando hayan tomado precauciones razonables para evitar la ocurrencia del mismo y segundo, si una vez alertados sobre su existencia, tomaron acciones oportunamente. El hecho de tener una política clara sobre el uso de correo electrónico, respaldada por la revisión y la capacitación, sería suficiente para refutar un cargo semejante. World Com logró que una demanda en su contra fuera inadmitida luego de mostrar que contaba con una política de correo electrónico, que le hacía seguimiento a esta política y que había tomado acción inmediata contra el acoso.

¿Qué software existe para protegerse?

Se puede usar un software de monitoreo (supervisión). Este es increíblemente sofisticado y busca cierto tipo de mensajes dentro de todas las comunicaciones que entran, salen y fluyen por su organización.

Por ejemplo, en una búsqueda general, si una carta tiene dos palabrotas, no las señalará. Pero si tiene una docena de ellas en el primer párrafo, entonces marcará

dicha carta. Uno puede programarlo para que busque ciertos términos sexuales explícitos o un lenguaje racial provocativo. Si detecta esa palabra, aunque sea tan sólo una vez, señala la carta. O si, por ejemplo, tiene un producto nuevo, puede buscar la marca o el código del producto y ver si algún empleado está enviando información sobre el mismo. Marca la carta, una persona designada la revisa y si se estima que no es apropiada, entonces nunca llegará a su destino. No habrá responsabilidad.

Por cierto, las comunicaciones ofensivas no son las únicas que deberían preocupar a las empresas. Digamos que usted, Richard Lally, trabajara para la IBM y que su buzón electrónico fuera de Richard Lally en IBM.com. Cada vez que envíe un mensaje, parecería que estuviera hablando en nombre de la IBM. Si su empresa permite que los empleados usen su sistema para fines personales, debe exigir que cada mensaje lleve un negador, algo así como, "Las opiniones e ideas expresadas en este mensaje no necesariamente representan las del empleador".

Durante toda esta entrevista, hemos hablado sobre la política de correo electrónico. En general, ¿cuáles son los elementos básicos de dicha política?

Primero que todo, debe constar por escrito y comenzar con una afirmación clara dirigida al empleado, en el sentido de que los recursos de sistemas pertenecen a la empresa y que deben ser usados exclusivamente para fines laborales. La compañía puede, si quiere, permitir el uso personal esporádico, pero debe definir los términos para su uso.

Segundo, debe informar al empleado que cualquier mensaje creado o recibido en el sistema del empleador estará sujeto a revisión. El empleado no debe tener expectativa alguna de privacidad.

Tercero, debe estipular qué material no puede salir jamas del sistema.

Y cuarto, debe haber una declaración que le informe al empleado que cualquier violación de dicha política lo sujeta a una acción disciplinaria e, incluso, puede llevar al despido.

Algo así como un negador.

Exactamente. Pídale al empleado que lo firme e inclúyalo en su archivo de personal. Más tarde, circúlelo y actualícelo trimestralmente, si considera que es necesario.

Entrevista realizada por Richard Lally, autor y periodista, para "Information Management". Volumen 2 Número 2. Febrero de 1999. Reproducido con autorización. Para mayores informes, favor comunicarse con American Management Association en el teléfono (212) 903 8073.