TONE at the TOP®

PRESENTADO POR: The Institute of Internal Auditors | Audit Executive Center

Edición 82 | Junio 2017

Proveemos información concisa sobre temas relacionados con gobierno a la alta dirección, juntas directivas y comités de auditoría.

La Visión que Auditoría Interna Trae a la Cultura de la Ciberseguridad

La vertiginosa propagación del ransomware (software malicioso) WannaCrypt — rápidamente denominado #WannaCry en las redes sociales después de haber paralizado un estimado de 200.000 computadoras en toda Europa, Asia y Américas — tiene a las funciones de gobernabilidad y gestión de riesgos pensando más seriamente acerca de cómo fortalecer los controles de seguridad cibernética. Después de muchos años de devastadoras fallas cibernéticas, ¿por qué que las organizaciones siguen siendo sorprendidas cuando un nuevo ataque es lanzado?

Estas brechas bien pueden ser incitadas sin saberlo por las culturas de ciberseguridad de las organizaciones, escribió el Presidente y Director ejecutivo del IIA Global, Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA, en un blog post poco después de que #WannaCry barrió el globo. "Proporcionar garantías sobre la seguridad cibernética implica algo más que mirar si los protocolos y las políticas diseñadas para bloquear o desalentar los ataques cibernéticos están en su lugar y operan con eficacia ", escribió. "Debemos considerar cómo la cultura de la organización influye en cómo se llevan a cabo esas protecciones."

Un ejemplo de esto es que algunas organizaciones pueden estar dispuestas a aceptar comportamientos de alto riesgo en prácticas de correo electrónico a cambio de una mayor productividad. Otra es cómo los esfuerzos para proteger los datos mediante el cifrado puede verse socavado si las normas que prohíben o limitan versiones en papel de los datos no están en su lugar o son ignorados. Chambers también ofreció precaución sobre "la mística de TI", donde la seguridad cibernética puede ser vista únicamente dentro del ámbito del departamento de TI y no están abiertos a preguntas de otras partes interesadas.

Construir relaciones de cooperación con TI, directores de riesgos, oficiales de seguridad de la información, recursos humanos y otros que gestionan los riesgos cibernéticos ayudarán a los auditores internos a fortalecer la cultura de la ciberseguridad de la organización. De lo contrario, la auditoría interna no podrá obtener una comprensión clara de lo que impulsa los riesgos cibernéticos y lo que influye en la cultura de la ciberseguridad de la organización y compartir esos conocimientos con la dirección y el consejo.

Sobre El IIA

El Instituto de Auditores Internos Inc. (IIA) es una asociación global de profesionales con más de 190.000 miembros en 170 países. El IIA actúa como el principal defensor de la profesión de auditoría interna, emisor de normas internacionales y primordial investigador y educador.

El IIA

1035 Greenwood Blvd. Suite 401
Lake Mary, FL 32746 USA.

Suscripciones a Disposición

Visite **www.globaliia.org/Tone-at-the-Top** para solicitar su suscripción gratuita.

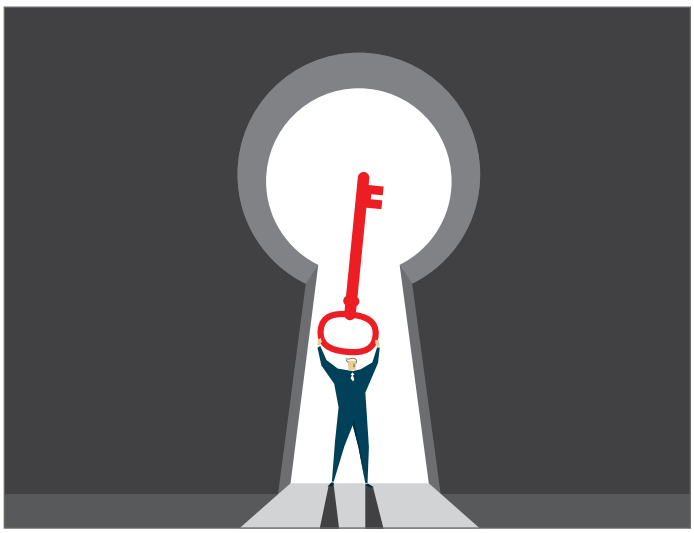
Comentarios de los Lectores

Envíe sus preguntas/comentarios a **tone@theiia.org**

Consejo Asesor de Contenido

Con décadas de experiencia en la alta dirección y consejo de administración, los siguientes apreciados profesionales proporcionan orientación sobre el contenido de esta publicación:

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano



Incluso los parches de seguridad — la solución obvia que podría haber impedido el alboroto del #WannaCry — tienen un componente cultural que va más allá de la designación limitada de tecnología. La colocación de un parche para cerrar una brecha de seguridad cibernética puede ser muy compleja porque no está claro cuál será el impacto en diversos sistemas operativos sin pruebas adecuadas, dijo Doug Anderson, director general de Soluciones CAE del IIA. "No podemos sólo culpar a TI en este caso, o culpar a los que supervisan TI. Es más complicado que eso, porque realmente están tratando de equilibrar el costo y beneficio al mirar un riesgo a una organización."

Existen barreras bien conocidas para la capacidad de la auditoría interna para abordar la cultura organizacional. La publicación el Pulso de Auditoría Interna de 2016 del IIA de Norte América informó que el 24 por ciento de los encuestados no cree que auditoría interna tenga la libertad de evaluar toda la organización y al personal, mientras que el 35 por ciento no cree que tengan el apoyo total de la dirección ejecutiva para hacerlo, y el 23 por ciento creen que no cuentan con el pleno apoyo de la junta y Comité para hacerlo.

Ganar un Asiento en la Mesa

Mientras los altos directivos continúen viendo a la ciberseguridad como dominio exclusivo de TI, la tendencia a buscar y señalar a un culpable cuando surja un problema persistirá. Eso Impide una colaboración eficaz y hace más difícil emerger una cultura más cooperativa de ciberseguridad.

"La auditoría interna es una de las pocas voces que está deliberadamente posicionada para ir a través de toda

la organización, y es capaz de ver cómo las distintas áreas funcionan entre ellas y asegurarse de que la información correcta está llegando a las personas adecuadas", dice Anderson. Cuanto mejor lo haga auditoría interna, más se le pedirá que aporte información y que participe en la planificación estratégica de negocios, lo que debería incluir decisiones sobre riesgos cibernéticos.

Ganar una oportunidad para influir en la cultura general de gestión de riesgos de la organización también depende en gran medida de cómo los auditores internos entienden su papel. Aquellos que creen que su propósito es identificar y reportar problemas, no llegarán muy lejos, dice Jim Pelletier, Vicepresidente de Relaciones Profesionales y de partes interesadas del IIA. Reconocer que están en condiciones de ayudar a la organización a alcanzar sus objetivos es una señal de que un director ejecutivo de auditoría o un presidente de un comité de auditoría tiene una comprensión del nivel de madurez de la organización. Esto les ayuda a aprovechar mejor los recursos de la auditoría interna para impactar positivamente en la organización.

"Eso impregnará la cultura, porque el director ejecutivo de auditoría ganará confianza a través del tiempo al demostrar que él o ella no está ahí para darle una bofetada, molestarle un poco y alejarse", dice Pelletier. El comité de auditoría, a su vez, es menos probable que utilice la información obtenida de la auditoría interna simplemente para castigar a la administración por no haber hecho algo, añade. Todavía habrán situaciones en las que se produzcan fraudes o abusos, que deben ser manejados por separado, pero "el trabajo cotidiano debe tener un impacto positivo en la organización."

Las Juntas y Comités de Auditoría necesitan proteger el Rol de Auditoría Interna en la Seguridad Cibernética

De acuerdo con Deloitte & Touche es necesario un compromiso frecuente y proactivo por parte del consejo de administración — especialmente el comité de auditoría — para supervisar un exitoso programa de ciberseguridad. "El presidente del comité de auditoría puede ser un enlace particularmente eficaz con otros grupos en el cumplimiento y la comunicación de las expectativas en materia de seguridad y mitigación de riesgos", dice el Informe de 2015. Deloitte también recomienda reclutar Directores con experiencia en ciberseguridad para que formen parte del comité de auditoría para que se tomen decisiones informadas sobre la suficiencia de los esfuerzos que están supervisando.

El consejo de administración y el comité de auditoría ayudan a la auditoría interna a preservar su independencia, dice Pelletier, manteniéndose involucrados en su supervisión de la función. "En algunas situaciones, los consejos podrían decir, ¿Dónde estaba auditoría interna?" Y mi respuesta es: "La auditoría interna está en donde la pusieron", dice. Corresponde al consejo de administración y al comité de auditoría garantizar que auditoría interna tenga una posición elevada que garantice el acceso necesario y donde "no haya temor ni preocupación por los temas que puedan tocar. Están topando los temas que la junta considera que son los más importantes."

Poco después del ataque #WannaCry, el Centro Ejecutivo de Auditoría del IIA publicó consejos que aclaraban lo que el consejo de administración debería esperar de auditoría interna para una protección óptima del riesgo cibernético:

- Es adecuada una cuidadosa evaluación de las actividades operativas críticas de la organización que identifica la infraestructura electrónica de apoyo para asegurar el alcance de su evaluación del riesgo cibernético. En lugar de partir de una lista de sistemas o protecciones ya establecidas, empiece por las actividades críticas de negocio y redirijalas al apoyo de infraestructura.
- Una reevaluación de la robustez de la evaluación del riesgo para los riesgos cibernéticos, asegurando que esté orientada a considerar todas las complejidades y matices inherentes de los riesgos cibernéticos en lugar de riesgos menos difíciles.
- Una revisión de los planes de continuidad de negocio para asegurar que cubren todos los diversos escenarios que pueden resultar de ataques cibernéticos y que se refieren a cómo el negocio seguirá funcionando — no sólo si las joyas de la corona están protegidas.
- Iniciación de rutinas de hacking ético para encontrar vulnerabilidades que un ciberataque podría explotar. Los cambios más rápidos en la tecnología requieren que esto se realice en forma permanente en lugar de periódicamente sólo cuando surja un problema.
- Una revisión de las operaciones básicas de TI alrededor de la administración de parches, que probablemente ya está en el plan de auditoría, pero necesita ser acelerada dada la actual situación.
- Una revisión de los programas y de los esfuerzos para mantener a los empleados bien entrenados e informados de su papel crítico en la prevención con éxito de ataques cibernéticos.

Cambiar el Enfoque de la Seguridad hacia la Resiliencia

El Informe Pulso de la profesión de 2016 del IIA destacó la necesidad de cambiar el enfoque de la ciberseguridad a la ciber resiliencia, dado el creciente consenso entre los expertos de que es una cuestión, no si una empresa experimentará un ciberataque sino de cuándo lo sufrirá. Entre más del 90 por ciento de encuestados que informaron que sus organizaciones tienen un plan de negocio de continuidad, sólo el 25% dijo que el plan tiene procedimientos claros y específicos para responder a un ciberataque, 17 por ciento de los encuestados informaron que sus planes no proporcionan ningún procedimiento. Si un Plan de continuidad del negocio carece de procedimientos detallados para responder a un ciberataque, el informe recomienda, que la auditoría interna debería garantizar que los procedimientos son incluídos en otros documentos, como en un plan de respuesta a incidentes, que puede o no estar vinculado al plan de continuidad del negocio.

El informe de Deloitte & Touche, Ciberseguridad: El papel cambiante del Comité de Auditoría y Auditoría Interna, cita a la resiliencia como una de las tres características esenciales de un plan viable de seguridad cibernética. El Centro de calidad de Auditoría también parece estar de acuerdo en que las organizaciones necesitan prestar más atención a la planificación de cómo van a responder y cómo recuperarse de un ataque en lugar de centrarse únicamente en medidas preventivas.

El documento del Centro de Calidad de auditoría, El Papel del CPA (Contador Público Certificado) en el Direccionamiento de Riesgo de Ciberseguridad: Cómo la profesión de Auditoría promueve la Resiliencia a la Ciberseguridad, que se publicará próximamente, discutirá cómo puede evolucionar el papel del auditor en la ciberseguridad.

Encuesta Rápida

¿Hasta qué punto la cultura de su organización influye positivamente en su capacidad de respuesta cibernética?

En nada | **Mínimamente**
Moderadamente | **Ampliamente**
No lo sé

Visite **www.theiia.org/tone** para responder la pregunta y ver cómo otros están respondiendo.

El presente documento fue traducido por el IAI ECUADOR el 26/06/2017

2017-0135