TONE at the TOP®

Proporcionar a la Alta Dirección, Juntas Directivas y Comités de Auditoría información concisa relacionada con la Gobernanza.

Edición 106 | Agosto 2021

Enfrentando al Monstruo de la Ciberseguridad

El riesgo cibernético afecta a organizaciones de todos los tamaños y en todas las industrias, y parece que llegó para quedarse. Una encuesta de juntas directivas y ejecutivos globales clasificó las amenazas cibernéticas como uno de los diez principales riesgos en 2021, y los encuestados esperan que también sean un riesgo importante en 2030. De hecho, se espera que el ciberdelito mundial aumente un 15% por año, y se prevé que su impacto anual alcanzará los 10,5 billones de dólares en 2025, de acuerdo con estudios de Cybersecurity Ventures. La empresa de investigación cibernética lo llama la "mayor transferencia de riqueza económica de la historia".

Los eventos de ciberseguridad pueden tomar la forma de ransomware, ataques a recursos de trabajo remotos, ataques a la cadena de suministro, phishing o cualquier cantidad de otras prácticas delictivas. Pueden obstaculizar a una empresa, eliminar significativamente el valor empresarial y someterla a responsabilidad o publicidad que dañe su reputación. Los costos de una violación de datos son altos y están creciendo, con un promedio de $ 4.24 millones en 2021, casi un 10% más en un año, según los datos de IBM.

Es más, la pandemia de COVID-19 solo ha creado nuevas vulnerabilidades que aún no se han entendido ni abordado por completo.

Gestionando los Peligros

Con tanto en juego, hay una serie de pasos que las juntas pueden tomar para mejorar su vigilancia de los riesgos cibernéticos. Durante todo el proceso, la auditoría interna puede actuar como un socio fundamental. Trabajando en colaboración con los expertos en ciberseguridad de la organización, el equipo de auditoría interna puede proporcionar una verificación objetiva de que los planes de la organización se ejecutan según lo previsto y son adecuados para la tarea. "Pueden decirle a la junta si existe una gran exposición o una falsa sensación de seguridad", dijo Sandy Pundmann, CIA, socio senior jubilado de Asesoramiento financiero y de riesgos de Deloitte.

Existen varias estrategias que la junta puede abordar para ayudar a cubrir el riesgo cibernético. Pundmann y otros recomiendan que las juntas directivas mantengan un conocimiento profundo del perfil de riesgo cibernético de sus organizaciones, adopten su función de supervisión y practiquen un escepticismo saludable para asegurarse de tener una comprensión clara de las fortalezas, debilidades y vulnerabilidades.

Establecer roles de supervisión y agendar actualizaciones periódicas. Mientras que menos del 10% de las juntas directivas de hoy tienen un comité dedicado a la ciberseguridad dirigido por un miembro calificado de la junta, se espera que ese número aumente al 40% para 2025, según una encuesta de Gartner, Inc. El aumento esperado puede estar impulsado por la expansión del negocio digital durante la pandemia y la adopción del trabajo remoto y sus riesgos potenciales adicionales.

Hoy en día, la responsabilidad de la supervisión de la seguridad cibernética puede ser difícil de identificar porque a menudo está dispersa entre la administración

Sobre El IIA

El Instituto de Auditores Internos, Inc. es una asociación profesional global con más de 200.000 miembros en más de 170 países y territorios. El IIA sirve a la auditoría interna como el principal defensor de la profesión, creador de normas internacionales y principal investigador y educador.

El IIA

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746 USA

Suscripciones a Disposición

Visite www.theiia.org/Tone para registrarse a suscripciones complementarias.

Comentarios de los Lectores

Envíe sus preguntas y/o comentarios a: tone@theiia.org

y varios comités, dijo Pundmann. A un comité debería serle asignada la responsabilidad y debería discutir el tema en cada reunión, agregó. La ciberseguridad también debería estar en la agenda de la junta completa al menos dos veces al año.

Reconocer el nivel de amenaza. La ciberseguridad es más que un problema del equipo TI (Tecnología de la Información). "Ya sea antes o durante un incidente, no sólo se debería dejar [la seguridad cibernética] en manos del director de información y el equipo técnico", dijo John Noble, ex director del Centro Nacional de Seguridad Cibernética del Reino Unido, en un podcast de McKinsey. "Los líderes deben decidir cómo manejar las tensiones entre la usabilidad, la seguridad y el costo, y ahí es donde necesitamos que la junta esté haciendo las consultas pertinentes y validando los procesos."

Sumergirse más profundo. Las juntas deben estar conscientes si sus organizaciones están analizando y mejorando regularmente sus evaluaciones de riesgo cibernético. El equipo de auditoría interna es llamado a menudo a que realice una evaluación inicial o un proyecto, tal vez una auditoría de ataque y penetración, pero eso es solamente un primer paso, advirtió Pundmann. Las empresas necesitan una estrategia multifacética para prevenir, detectar y responder a los eventos cibernéticos. Los esfuerzos deberían incluir una evaluación de los pasos en curso que está tomando la compañía para comprender los ataques, la eficacia de las medidas que se están adoptando, cómo se monitorean los incidentes y las respuestas, y la mecánica y el éxito de la repuesta de la compañía. La evaluación de la estrategia completa puede comenzar a nivel de comité, pero debe ser discutida por la junta en pleno.

Como señaló una publicación de Deloitte, la primera línea contra el riesgo cibernético está formada por las unidades de negocio y TI, que abordan el riesgo en sus decisiones y operaciones diarias. La segunda línea de la organización es el liderazgo de gestión de riesgos de la información y la tecnología, que asume la gobernanza y la supervisión. La función de auditoría interna es cada vez más la tercera línea, llevando a cabo una revisión independiente de las medidas de seguridad y el desempeño.

Comprender qué distingue a este riesgo. Las organizaciones y sus juntas directivas están familiarizadas con los riesgos, pero la ciberseguridad es diferente por un par de razones. Primero, es altamente especializado y las amenazas cambian constantemente, poniéndolas más allá de la experiencia de muchos miembros de la junta. En segundo lugar, el uso de Internet es generalizado en la mayoría de las organizaciones, por lo que los riesgos y su impacto son multifacéticos y complejos. "El acceso empresarial a Internet es fundamental para generar valor, y todas esas transacciones que dependen del acceso a Internet son intrínsecamente inseguras", dijo un participante en un panel de discusión de la Red de Directores de Riesgo Cibernético. "Esto no es así para ningún otro aspecto del riesgo con el que las juntas lidian."

PREGUNTAS PARA MIEMBROS DE LA JUNTA

- ¿Con qué frecuencia la junta recibe actualizaciones sobre las amenazas a la seguridad cibernética de la organización y los pasos que se están tomando para abordar y gestionar los riesgos cibernéticos?
- ¿La organización está abordando la ciberseguridad como un problema de riesgo empresarial y no exclusivamente como una preocupación de TI?
- ¿La junta asume un papel proactivo en el seguimiento de los riesgos cibernéticos o asume que todo está bien a menos que se indique lo contrario?
- ¿Tiene la junta un comité de ciberseguridad dedicado? De no ser así, ¿otro comité, como el comité de auditoría, tiene la responsabilidad de supervisar la ciberseguridad?

Un ejemplo de la vida real. En un ejercicio teórico de simulación, *que puede ser llevado a cabo por auditoría interna,* otra administración o una parte externa, la junta y la administración pueden supervisar un ataque simulado para determinar cómo responde la organización, cómo se notifica a los inversionistas y cómo los clientes o socios comerciales son afectados. (Pundmann incluso trabajó con una junta que solicitó que solamente el Director de Información y el Gerente General estuvieran al tanto de la situación simulada, para hacer el ejercicio lo más realista posible). Una vez que la organización ha evaluado su respuesta, la junta puede recibir una actualización sobre los cambios que se han realizado o están en curso.

Auditoría interna también puede ser un actor fundamental en otro ejercicio valioso: una visualización del modelo de madurez, que ofrece una visión empresarial de alto nivel de los riesgos cibernéticos y compara dónde la organización está y dónde debería estar, todo esto explicado en términos sencillos. Debido a que no es posible monitorear y abordar todos los riesgos, estos ejercicios también pueden ayudar a aclarar qué objetivos son los más críticos para que la organización pueda mejorar la prevención y detección en esas áreas, dijo Pundmann.

No deje que los riesgos le tomen por sorpresa. A medida que se expande la adopción de la tecnología, también lo hacen los riesgos asociados con tecnologías emergentes desconocidas. Incluso un nuevo sistema ERP puede plantear desafíos de seguridad que no deben pasarse por alto, señaló Pundmann. Muchas empresas esperan, erróneamente, hasta que surgen problemas con un nuevo sistema antes de planificar cómo abordarlos. "Asegúrese de tener un plan de seguridad desde el principio para su estrategia cibernética y de control" indicó.

Las organizaciones involucradas en fusiones y adquisiciones también pueden enfrentar nuevas vulnerabilidades. "Si está adquiriendo una empresa, pregunte qué riesgos está asumiendo al conectar sus negocios", aconsejó.

Las empresas que trabajan con cadenas de suministro u otros terceros también pueden estar expuestas a riesgos de esas fuentes. Además, en el ámbito del cumplimiento, las organizaciones deben conocer las reglamentaciones pertinentes, como las reglas de la Comisión de Bolsa y Valores sobre divulgaciones de seguridad cibernética.

Aprovechamiento de los Recursos de Auditoría Interna

Las amenazas cibernéticas pueden ser abrumadoras, pero la auditoría interna puede proporcionar una perspectiva única e independiente sobre los riesgos de la organización y las mejores formas de abordarlos. Las juntas directivas que son proactivas en su monitoreo de los problemas de ciberseguridad y aprovechan al máximo el valor que la auditoría interna puede ofrecer deben estar en una mejor posición para abordar de manera efectiva los riesgos de ciberseguridad.

¿QUÉ ESTÁ PASANDO POR ALTO SU JUNTA?

60% de las organizaciones no tiene un jefe de ciberseguridad que se siente en la junta o en el nivel de dirección ejecutiva.

59% de las organizaciones dice que la relación entre la ciberseguridad y las líneas de negocio es, en el mejor de los casos, neutra, no confiable o inexistente.

20% de las juntas directivas confía mucho en que los riesgos de ciberseguridad y las medidas de mitigación que se les presentan pueden proteger a la organización de grandes ciberataques.

36% El 36% de las organizaciones dice que la ciberseguridad está involucrada desde la etapa de planificación de una nueva iniciativa empresarial.

Fuente: *"The Risky Six: Preguntas clave para exponer las brechas en la comprensión de la junta directiva sobre la ciberresiliencia organizacional"*, IIA Global y EY, 30 de marzo de 2021.

[1] *Executive Perspectives on Top Risks for 2021 and 2030*, Protiviti and NC State University's ERM Initiative, 2021.
[2] *"Cybercrime to Cost the World $10.5 Trillion Annually by 2025,"* Steve Morgan, *Cybercrime Magazine*, November 13, 2020.
[3] *Cost of a Data Breach Report*, IBM, 2021.
[4] *"Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025,"* Gartner press release, January 28, 2021.
[5] *"Boards and Cybersecurity,"* McKinsey and Company podcast, February 2, 2021.
[6] *"Cybersecurity and the Role of Internal Audit: An Urgent Call to Action,"* Sandy Pundmann, Deloitte, 2017.
[7] *"Cybersecurity: An Evolving Governance Challenge,"* Harvard Law School Forum on Corporate Governance, March 15, 2020.
[8] *"Commission Statement and Guidance on Public Company Cybersecurity Disclosures,"* Release Nos. 33-10459; 34-82746, Securities and Exchange Commission, February 26, 2018.

Encuesta Rápida

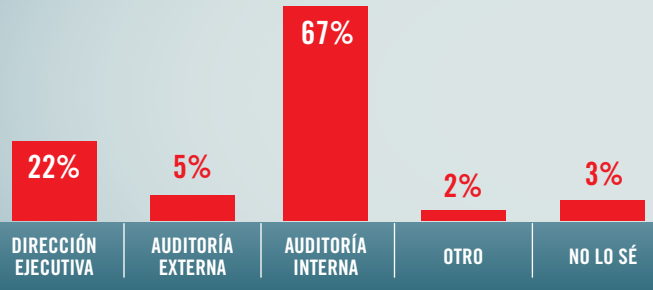
¿Su junta tiene un miembro con experiencia en ciberseguridad?

- ❑ Si
- ❑ No
- ❑ No lo sé

Visite www.theiia.org/Tone para responder la pregunta y conocer cómo responden los demás.

RESULTADOS DE LA ENCUESTA RÁPIDA

¿En quién confía la junta principalmente para asegurarse de la efectividad de la gestión de riesgos y el control interno?



Fuente: Encuesta Tone at the Top Junio 2021.

El presente documento fue traducido por el IAI ECUADOR el 4/10/2021.