La SEC está a punto de forzar a los CISO a las salas de juntas de Estados Unidos

Este año es el vigésimo aniversario de la legislación estadounidense conocida como Ley Sarbanes-Oxley (SOX). La SEC actuó rápidamente en SOX dada la amenaza existencial que enfrentan los mercados de capitales de EE. UU. por un posible colapso en la confianza de los informes financieros. Entre otras cosas, SOX trajo una transformación significativa a la sala de juntas corporativa.

Una de las cosas más impactantes que transformó fue la composición de la junta cuando requería la divulgación de la experiencia financiera de la sala de juntas. Esto tuvo el efecto de introducir aptitudes financieras y contables en muchos, si no en la mayoría de los directorios corporativos por primera vez. Notable en retrospectiva es que fue hace solo veinte años cuando era un concepto novedoso para las juntas corporativas de empresas públicas de EE. UU. tener un director en la sala de juntas que entendiera un estado financiero y cuestiones contables.

La próxima competencia del director corporativo que la SEC está transformando ahora es la experiencia cibernética de la sala de juntas.

La SEC propuso recientemente nuevas reglas que requerirían la divulgación en la sala de juntas de las empresas públicas de EE. UU. de los directores corporativos con experiencia en ciberseguridad. Este es actualmente un conjunto de habilidades relativamente raro dentro de las filas de la mayoría de las juntas corporativas, no solo en los EE. UU. sino en todo el mundo.

Si bien es raro, algunas empresas estadounidenses conocidas ya comprenden el valor de tener competencias profundas en seguridad cibernética en su directorio. Empresas como FedEx, Hasbro, PNC y UPS han transformado su enfoque para controlar el riesgo cibernético, comenzando con la experiencia cibernética de la sala de juntas.

¿Por qué estos tableros lo obtuvieron, mientras que muchos otros no? ¿Por qué estamos ahora en un punto en el que la SEC tiene que obligar a las juntas corporativas a agregar este conjunto de habilidades a sus filas de directores?

Recientemente entrevisté al ex ejecutivo de IBM y actual director corporativo de una empresa pública de EE. UU., Rodney Adkins, sobre su experiencia de primera mano con la vanguardia de la transformación de la supervisión del riesgo digital y cibernético en la sala de juntas. Inicialmente le pregunté sobre la necesidad de directores cibernéticos y digitales profundos y amplios en las juntas y comentó: Las habilidades de la sala de juntas deben reflejar los patrones del mercado.

Dado que el Foro Económico Mundial estima que el 60 % del crecimiento económico está siendo impulsado por las tecnologías digitales, gobernar la creación de este valor y cómo debe protegerse ya debería estar en juego en la mesa de juntas. Pero aún no lo es. Rod explicó el retraso en el gobierno corporativo sobre el riesgo cibernético de esta manera:

“El desencadenante de las tablas en las que estoy vino de un lugar inesperado. No fue la junta el catalizador de la reforma de la gobernanza. Fueron los equipos de gestión los que llegaron a la conclusión de que tenían que controlar el riesgo cibernético como un riesgo que nunca iba a desaparecer. Y luego todo se unió cuando las juntas se dieron cuenta de su parte en el sistema de seguridad cibernética y la necesidad de ejercer sus responsabilidades de manera más efectiva. Nos despertamos juntos como resultado de la creciente concienciación y educación sobre el riesgo cibernético que estábamos experimentando. Si bien existía el instinto natural de la sala de juntas de preocuparse por algunos de estos problemas, ahora es de gran ayuda tener directores en la sala de juntas que han sido operadores de ciberseguridad”.

El gobierno corporativo es un sistema en sí mismo que requiere las habilidades correctas del director, la estructura de la sala de juntas y el alcance de la supervisión del riesgo. Con el entorno de riesgo cibernético que cambia rápidamente al que se enfrenta cada empresa, el riesgo cibernético presenta amenazas claras y presentes de equidad, financieras y de litigio. El riesgo aumenta en las empresas que no tienen directores corporativos que entiendan estos temas. Y estos problemas están directamente en los intereses de los inversores, los clientes y todas las partes interesadas corporativas, lo que lo convierte en un problema de la SEC.

Estos problemas son lo suficientemente importantes como para que la SEC ahora proponga exigir la divulgación de la experiencia cibernética de la sala de juntas, como lo hicieron hace 20 años con la experiencia financiera. Le pregunté a Adkins sobre el desafío de mantenerse al tanto del cambiante panorama del riesgo cibernético y de las principales prácticas de ciberseguridad:

“Aunque formo parte de los directorios de algunas grandes empresas públicas conocidas, recientemente me uní al directorio de una empresa privada de ciberseguridad, NVISIONx, exactamente por este motivo. NVISIONx se centra en el riesgo cibernético sistémico a nivel de datos. Los datos son el elemento vital de todos los sistemas digitales, y los datos que se roban, se toman como rehenes o incluso se corrompen pueden introducir riesgos posteriores en los procesos operativos. Esto me ayuda a mantenerme a la vanguardia de estos temas y al tener a alguien como yo con experiencia en cibernética y TI operativa, a medida que surgen estos temas en la sala de juntas, puedo forzar más el diálogo sobre lo que es realmente crítico, cuáles son los problemas reales, las exposiciones, nuestro plan de juego y si tenemos el nivel adecuado de inversión y talento. Permite que la conversación sea mucho más rica”.

Las reglas propuestas por la SEC para la experiencia cibernética de la sala de juntas siguen el enfoque adoptado por la SEC hace 20 años con la experiencia financiera. En lugar de centrarse en los títulos de los puestos, la experiencia se trata de la profundidad de la experiencia, las competencias y la educación formal sobre estos temas. Las reglas propuestas por la SEC sugieren que la experiencia sea determinada por:

- Si el director tiene experiencia laboral previa en seguridad cibernética, incluida, por ejemplo, experiencia previa como oficial de seguridad de la información, analista de políticas de seguridad, auditor de seguridad, arquitecto o ingeniero de seguridad, operaciones de seguridad o gerente de respuesta a incidentes o planificador de continuidad comercial;
- Si el director ha obtenido una certificación o título en ciberseguridad; y
- Si el director tiene conocimientos, habilidades u otros antecedentes en seguridad cibernética, incluidas, por ejemplo, las áreas de política y gobierno de seguridad, gestión de riesgos, evaluación de seguridad, evaluación de control, arquitectura e ingeniería de seguridad, operaciones de seguridad, manejo de incidentes o planificación de continuidad comercial. .

La SEC quiere competencias operativas profundas en ciberseguridad en la sala de juntas, como lo hicieron con la experiencia financiera. Agregar esta competencia de director a las juntas directivas de las empresas públicas de EE. UU. fortalecerá la sala de juntas como un punto de control crítico en el sistema de seguridad cibernética de cada empresa. Como sucedió con SOX, es probable que los reguladores de todo el mundo también reflejen este requisito, creando una aceleración global de la transformación de las juntas cibernéticas.

“La complejidad de esta área es en parte culpable de por qué la reforma de la junta avanza tan lentamente”, según Rod Adkins. “Esta es un área muy exigente y la mayoría de las empresas ahora reconocen que las amenazas cibernéticas pueden causar daños graves. Pero cambiar la trayectoria tiene mucho que ver con los recursos, a medida que aumenta. Se necesitan personas que entiendan este espacio y que tengan un conocimiento mucho más profundo de estos temas que los profesionales que trabajan”.

Según la experiencia de Rod, la transformación del comité también suele acompañar a la incorporación de estas habilidades en la sala de juntas. La transformación de la sala de juntas sobre el riesgo cibernético no se limita a tener habilidades cibernéticas en la sala de juntas. La gobernanza en sí es un sistema que se basa en la estructura organizativa correcta para las actividades del director y el enfoque correcto en el riesgo. Más de 200 juntas en los EE. UU. R3000 ahora tienen algún tipo de comité de tecnología o ciberseguridad en su junta. Este principio organizativo aporta una mayor eficiencia de tareas, enfoque y responsabilidad a los mandatos del comité. Si bien muchas juntas aún siguen la práctica rezagada de encargar a su comité de auditoría la supervisión del riesgo cibernético. Esta es una práctica que el contador jefe interino de la SEC ha cuestionado.

Si bien a menudo puede haber un sesgo infundado de que los ejecutivos cibernéticos son especialistas técnicos, comprender el riesgo cibernético requiere una comprensión sólida de dónde proviene el valor comercial y cómo protegerlo. Dado el papel importante que tiene el sistema de negocios digital de cada empresa en los ingresos y la rentabilidad, llevar la experiencia cibernética a la sala de juntas es ahora lo que está en juego en la mesa de gobierno corporativo. Esto no solo fortalecerá la sala de juntas como un control cibernético clave sobre el riesgo a la baja, sino que también ayudará a las empresas a crear e impulsar valor a partir de la transformación digital.

El gobierno cibernético es un tema de competitividad y seguridad nacional y la SEC ahora propone cambios de sentido común y fáciles de implementar que obligarán a las juntas a hacer lo que podrían haber hecho ellos mismos todo el tiempo: gobernar de manera efectiva uno de los riesgos más importantes que enfrenta la organización.

La experiencia cibernética en las salas de juntas de Estados Unidos está muy atrasada.

Autor: **Bob Zukis**

Fuente: Forbes