5 preguntas de ciberseguridad
que los CFO deben hacer a los CISO

> Armados con las respuestas, los directores financieros pueden desempeñar un papel esencial en la reducción del riesgo cibernético.

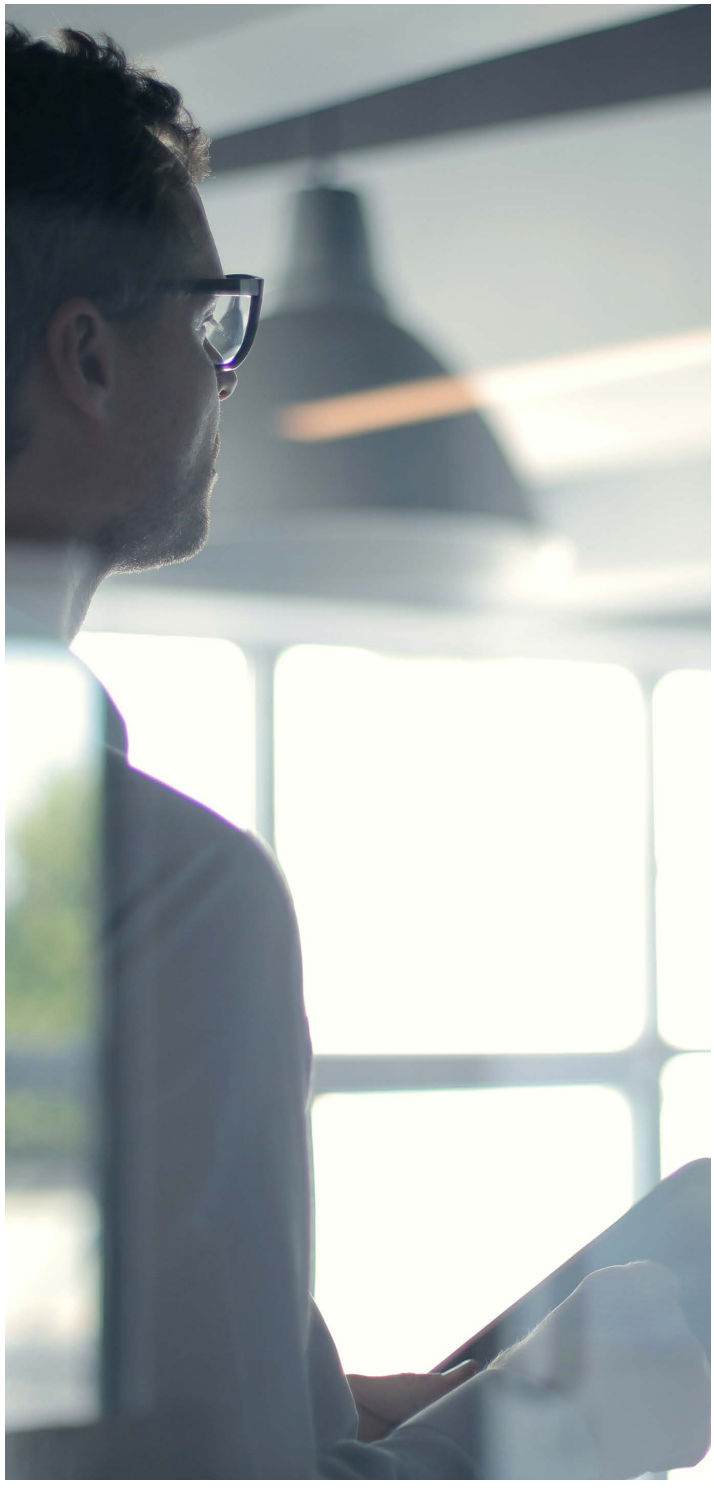
Incluso en una economía en contracción, es probable que las organizaciones mantengan su nivel de gasto en ciberseguridad. Pero eso no significa que en el clima económico actual de costos crecientes y una posible recesión no tomen una lupa sobre cómo están gastando el dinero presupuestado para defender los sistemas y los datos. De hecho, en muchas empresas, el gasto en ciberseguridad no está apuntando a los peligros más significativos, según los expertos, como lo demuestra la gran cantidad de ataques exitosos de ransomware y violaciones de datos.

Sin una comprensión integral del panorama de la seguridad y lo que la organización necesita hacer para protegerse, ¿cómo pueden los CFO tomar las decisiones correctas cuando se trata de inversiones en tecnología de ciberseguridad y otros recursos? No pueden.

Por lo tanto, los cfo deben asegurarse de tener una comprensión oportuna de los problemas de seguridad que enfrenta su organización. Eso requiere recurrir a las personas más conocedoras de la organización: directores de seguridad de la información (CISO) y otros líderes de seguridad en la primera línea de TI.

Aquí hay cinco preguntas que los CFO deberían hacer a sus CISO sobre la seguridad de sus empresas.

1. ¿Qué tan seguros estamos como organización?



Esta es una pregunta difícil de responder, pero debe hacerse, aunque no sea por otra razón que para dar al CFO una idea del nivel de ataques contra la empresa y lo que el equipo de seguridad está haciendo para proteger los sistemas y los datos.

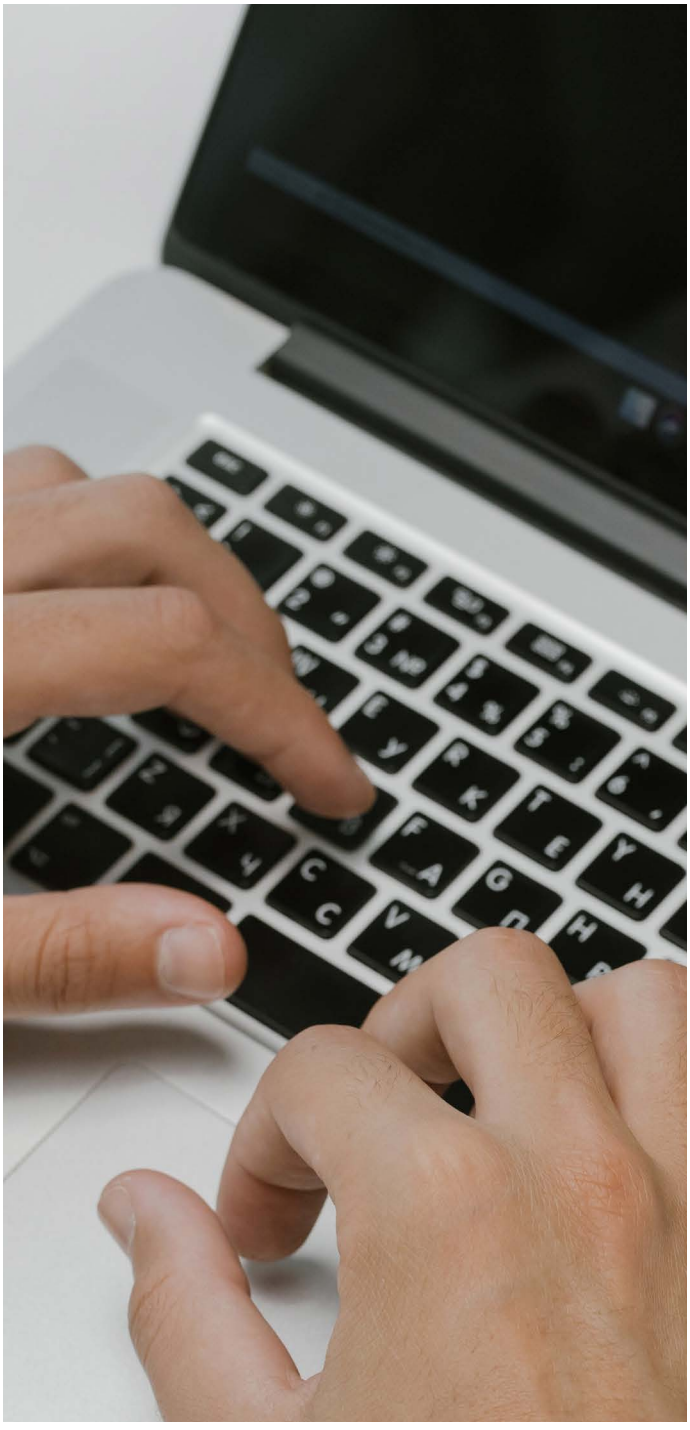
"Esta es una pregunta que se le hace con frecuencia a un CISO, y es una de las preguntas más difíciles de responder adecuadamente", dijo Michael Gordon, CFO de la compañía de software MongoDB. La respuesta ideal del CISO debería ser:

"Hemos identificado nuestras joyas de la corona y las hemos asegurado lo mejor que podemos, dados los recursos disponibles y el conocimiento que tenemos sobre el panorama de la ciberseguridad tal como es hoy", dijo Gordon.

Hay varias métricas tangibles que las organizaciones pueden usar para medir el nivel de riesgo de seguridad que enfrentan. Una es tener una idea de cuántos ataques o intentos de violación ha experimentado la organización.

Muchos ejecutivos que no son de TI y de nivel C no conocen todos los ataques que enfrenta su organización. Solo saben de los grandes y no de los que fueron bloqueados y resueltos rápidamente. Si tienen todos los datos, podrían “mejor” entender las solicitudes de gasto cibernético.

2. ¿Cuáles son las principales amenazas o riesgos de seguridad en nuestra industria?



Esto es algo así como una extensión de la pregunta anterior, pero es particularmente importante para los CFO en industrias que son objetivos principales de ataque.

Muchas amenazas y riesgos están dirigidos a tipos específicos de empresas, como empresas de servicios financieros y proveedores de atención médica. En algunos casos, los ataques reales están diseñados para tipos específicos de sistemas y datos.

Conocer las últimas tendencias relacionadas con los ataques específicos de la industria puede ayudar a los CFO a controlar qué inversiones debe realizar la organización para protegerse y mitigar los riesgos.

El hecho de que aún no le haya sucedido a su organización no significa que sea inmune dijo Patel. Es solo cuestión de tiempo. Comprender lo que está sucediendo en la industria puede ayudar al CFO a evaluar la preparación de su organización.

3. ¿Cómo nos aseguramos de que el equipo de ciberseguridad y el CISO estén involucrados en el desarrollo del negocio?

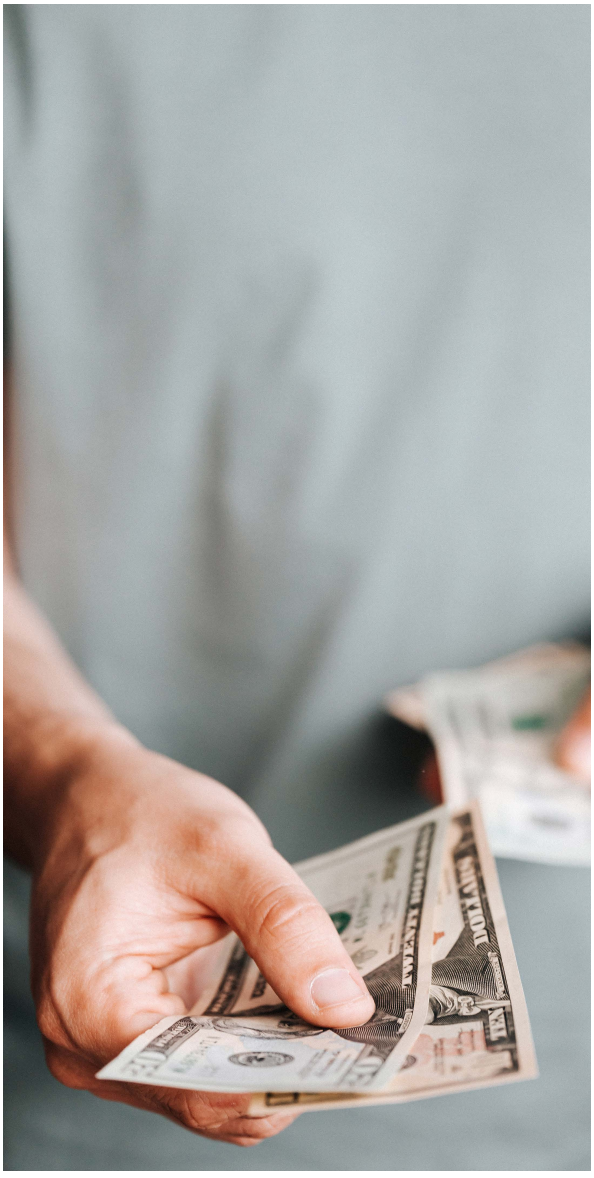
La seguridad ha sido vista durante mucho tiempo por muchos como un obstáculo para la innovación y la productividad, pero no tiene por qué ser así. Los CISO tienen un lugar en la mesa de la C-suite, y los CFO pueden trabajar con ellos para ayudar a que la seguridad sea una parte estratégica del negocio.

Las organizaciones inteligentes están abordando los problemas de ciberseguridad y protección de datos al infundir esfuerzos y conciencia de ciberseguridad desde todas las perspectivas y en todos los niveles.

Históricamente, la seguridad fue vista por muchos directores financieros como un centro de costos. Pero eso está cambiando.

Las organizaciones deben ver la seguridad como una oportunidad de desarrollo empresarial. Los cfo deben aprovechar los esfuerzos de CISO y seguridad para crecer, construir y expandir el negocio.

4. ¿Cuáles son los riesgos y costos potenciales de no implementar un control cibernético?

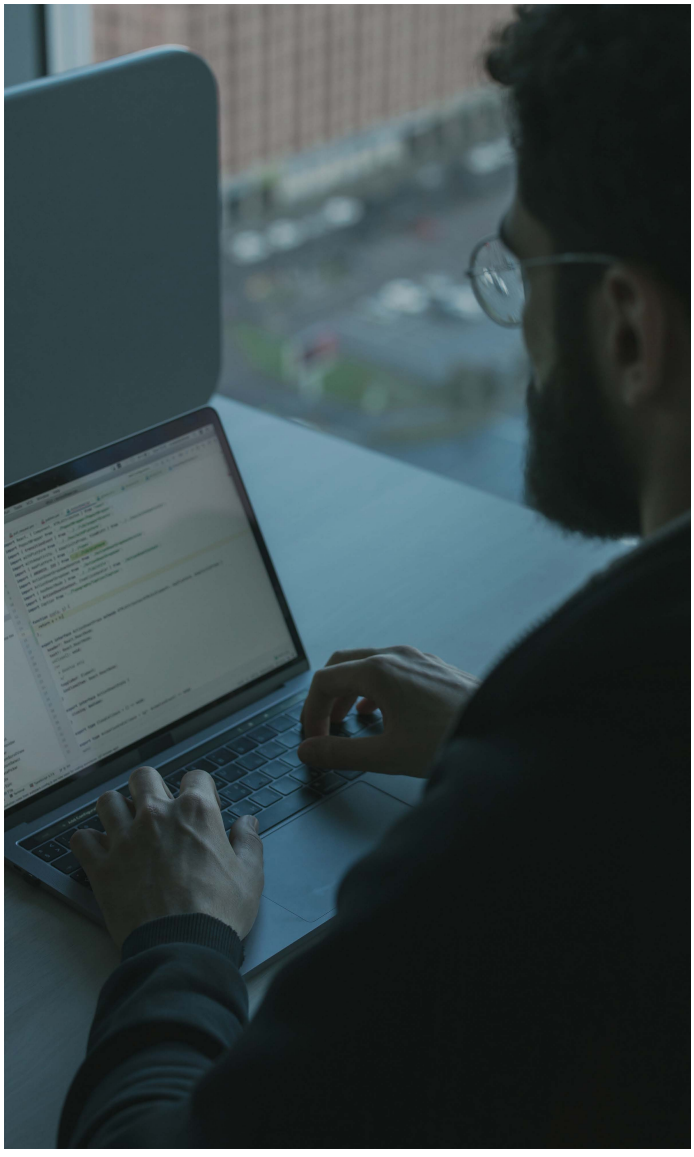


Medir el retorno de la inversión con el gasto en ciberseguridad puede ser complicado, porque el retorno potencial toma la forma de algo que no sucede, como un ataque.

Aún así, tiene sentido que los cfo pregunten a los líderes de seguridad sobre la probabilidad de que ocurra un tipo determinado de ataque, cuánto podría costarle a la organización y cuánto costaría prevenir este tipo de ataque.

Los costos también pueden tomar la forma de negocios perdidos después de un ataque.

5. ¿Los empleados entienden la seguridad de la información y están implementando protocolos de seguridad con éxito?



Un buen porcentaje del riesgo de ciberseguridad proviene de amenazas internas. Estas no son necesariamente acciones maliciosas, sino que a menudo son el resultado de negligencia o error humano.

En cualquier caso, las organizaciones deben asegurarse de que los empleados sean muy conscientes de los riesgos de seguridad y del uso adecuado de las herramientas y servicios tecnológicos.

Los trabajadores deben recibir capacitación sobre qué buscar para que puedan evitar ser víctimas de phishing y otros ataques, y los CFO deben preguntarse qué se debe hacer para mejorar la conciencia y la educación.

La capacitación y la concientización deben ocurrir en todos los niveles de la organización, incluidos los altos ejecutivos que pueden ser blanco de ataques específicos.

Fuente de información: cfo.com