PERSPECTIVAS Y PERCEPCIONES GLOBALES

Ciberseguridad en 2022

PARTE 1: Cómo las nuevas propuestas de la SEC podrían cambiar el juego

PARTE 2: Socios críticos — Auditoría interna y el CISO

PARTE 3: Respuesta y recuperación ante incidentes cibernéticos

Traducción al Español Auspiciada por:
FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

The Institute of Internal Auditors

CONTENIDO

PARTE 1: Cómo las nuevas propuestas de la SEC podrían cambiar el juego 3

Introducción 5

Preparando el escenario 6

La ciberseguridad domina el panorama de riesgos 6

El gran cambio 9

Un primer paso histórico hacia la divulgación de incidentes cibernéticos 9

El papel de la Auditoría Interna sigue siendo la misma 13

Identificar, evaluar y comunicar 13

Conclusión 15

PARTE 2: Socios críticos - Auditoría Interna y el CISO 16

Introducción 18

El caso de la colectiva ciberseguridad 19

Cinco claves para el éxito 20

Comprender y alinearse con el perfil de riesgo cibernético de la organización 20

Comprensión de los roles 21

Relevancia 21

Comunicar al consejo de administración y a la dirección ejecutiva 22

Proteger y respetar la independencia 22

Añadir valor 24

Conclusión 25

PARTE 3: Respuesta a los incidentes cibernéticos y recuperación 26

Introducción 28

Controles clave 29

Dar a la auditoría interna un papel en la respuesta cibernética 29

Conclusión 33

Parte 1:

Cómo las nuevas propuestas de la SEC podrían cambiar el juego

Sobre los expertos

Andy Watkin-Child

Watkin-Child es un veterano de 20 años de experiencia en ciberseguridad , gestión de riesgos y tecnología, y cofundador de The Augusta Group, un proveedor de soluciones para la gestión, supervisión y garantia de la ciberseguridad y el riesgo cibernético. Ha ocupado puestos de liderazgo internacional en la 1ra y 2nda Líneas de Defensa (LoD) para la ciberseguridad, la gestión de riesgos cibernéticos, el riesgo operativo y la tecnología, trabajando con equipos de liderazgo de empresas con balances de más de 1 billón de euros en los sectores de ingeniería y fabricación, los servicios financieros y la edicion y medios de comunicacion. Es un miembro experimentado de consejos de administración, equipos de liderazgo de riesgo globales y comités de ciberseguridad, riesgo operacional y GDPR.

Manoj Satnaliwala

Satnaliwala es director ejecutivo de auditoría y vicepresidente senior de auditoría interna de Caliber Home Loans y es responsable de todas las actividades de auditoría, trabajando directamente con el comité de auditoría. Antes de su puesto actual, dirigió la función de auditoría de Radian Group Inc., la tercera aseguradora hipotecaria más grande de los Estados Unidos, y fue director de auditoría interna de PwC, donde administró la validación de los controles para la auditoría interna, como parte del proyecto CCAR para una gran sociedad de control.

Introducción

Las nuevas propuestas de regulación podrían tener enormes implicaciones

El ciclo de noticias en 2022 y, ha sido poco positivo, en los últimos años, y las amenazas cibernéticas han ocupado un lugar importante en una mezcla que incluye la crisis de Ucrania, las amenazas persistentes de COVID-19 y las crecientes tensiones entre EE. UU. y China. Juntas, estas variables y más se han combinado para que la ciberseguridad ocupe un lugar importante, y de hecho principal, en los mapas de riesgo de los auditores internos.

Sin embargo, en 2022 también se han producido novedades relacionadas con la ciberseguridad que prometen afectar un amplio espectro de organizaciones, cuya comprensión requerirá un mayor esfuerzo y cuyas implicaciones tardaran en comprenderse plenamente. Entre ellas destacan dos propuestas regulatorias de la Comisión de Bolsa y Valores de EE. UU. (SEC). La segunda propuesta es especialmente digna de mención porque exigiría a las empresas que cotizan en bolsa y operan en EE. UU. que divulguen sus políticas, procedimientos y estrategias de gobierno en materia de ciberseguridad, así como los conocimientos y la experiencia de la junta -si los hay-, en el ámbito de la ciberseguridad. Si se implementan (como es probable que ocurra de alguna manera), las organizaciones que cotizan en bolsa, independientemente de su industria o tamaño, estarán sujetas a estas nuevas normas. Sin hipérbole, estos desarrollos representan un nuevo capítulo para la ciberseguridad y nuevo, aunque familiar, para la comunidad de auditoría interna, que desempeñará un papel fundamental en la navegación de sus organizaciones a través de este desafío.

Aunque no es un desafío que deba tomarse a la ligera, afortunadamente la auditoría interna conoce las herramientas y habilidades que necesita para ofrecer garantías sobre esta área de riesgo en evolución. La parte 1 de la serie de tres partes Global Knowledge Brief del IIA sobre ciberseguridad presenta una visión general de las nuevas propuestas de la SEC, incluyendo las implicaciones que tienen para la regulación de la información sobre ciberseguridad en los EE. UU. y en el extranjero. También explora cómo los auditores internos pueden desempeñar un papel importante para ayudar a sus organizaciones a gestionar un panorama de cumplimiento alterado que las nuevas regulaciones podrían crear pronto.

Preparando el escenario

La ciberseguridad domina el panorama de riesgos

El mayor riesgo de nuestro tiempo

La ciberseguridad sigue siendo una prioridad en todos los niveles de todas las organizaciones en todas las industrias en 2022, y esa preocupación se refleja claramente en los datos del Pulso *Norteamericano de Auditoría Interna de 2022* del IIA (*Pulse*)[1] . Cuando se les pidió que calificaran el nivel de riesgo de sus organizaciones entre 13 riesgos principales, los líderes de auditoría interna que respondieron a la encuesta de Pulse clasificaron los riesgos relacionados con la tecnología entre los tres principales: ciberseguridad, TI y relaciones con terceros (que a menudo incluyen servicios de TI). Incluso entre estos tres principales, la ciberseguridad ocupó fácilmente el primer puesto, con el 85 % de los encuestados calificándolo como un riesgo alto o muy alto, 24 puntos porcentuales más que las calificaciones para la TI, el segundo riesgo más alto.

Esta preocupación está justificada. En 2021, los ataques cibernéticos de casi todo tipo aumentaron de forma alarmante. Según el *Informe sobre Ciber amenazas de SonicWall de 2022*[2] , el número de amenazas cifradas en 2021 se disparó un 167 % (10,4 millones de ataques), el ransomware aumentó un 105 % (623,3 millones de ataques), el cryptojacking (ataques a equipos para minar criptomonedas) aumentó un 19 % (97,1 millones de ataques), los intentos de intrusión aumentaron un 11 % (5,3 billones de ataques) y el malware dirigido a Internet de las cosas (IoT) aumentó un 6 % (60,1 millones de ataques).

Además, todos estos ataques tienen un coste importante por los daños que infligen. Se espera que el coste total anual de los ciberataques alcance los 10,5 billones de dólares en 2025, lo que supone un crecimiento promedio del 15 % anual, según la última versión del Almanaque de Ciberseguridad 2022 de Cisco/Cybersecurity Ventures.[3] .

Y esto ni siquiera tiene en cuenta los cambios drásticos en el panorama geopolítico que afectan a la ciberseguridad. Incluso antes de la invasión rusa de Ucrania, había muchas pruebas de que los supuestos ataques cibernéticos, patrocinados por el estado, con altos niveles de sofisticación, estaban aumentando en impacto y frecuencia. La brecha de 2020 en los sistemas de SolarWind, con sede en Texas, que fue llevada a cabo por un grupo de piratas informáticos supuestamente dirigidos por el Servicio de Inteligencia Exterior de Rusia, se vio comprometida y sin detectar durante meses la infraestructura digital de hasta 18.000 clientes[4] —entre ellos Microsoft, Cisco, Intel, Deloitte, partes del Pentágono, el Departamento de Seguridad Nacional de EE. UU., el Departamento de Energía y la Administración Nacional de Seguridad Nuclear.

En 2021, se produjo otro presunto importante ataque patrocinado por el estado contra una empresa estadounidense, en Colonial Pipeline Co.[5] El ataque interrumpió temporalmente el flujo de casi la mitad de los suministros de gasolina y

[1]. El IIA, *2022 North American Pulse of Internal Audit,* marzo de 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of- auditoría interna/
[2]. SonicWall, *Informe de ciberamenazas de SonicWall de 2022,* 2022, https://www.sonicwall.com/2022-cyber-threat-report/ .
[3]. Steve Morgan, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics", Cybersecurity Ventures, Cisco, 19 de enero de 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/ .
[4]. Isabella Jibilian y Katie Canales, “Estados Unidos está preparando sanciones contra Rusia por el ataque cibernético de SolarWinds. Aquí hay una explicación simple de cómo sucedió el hackeo masivo y por qué es tan importante”, Business Insider, actualizado el 15 de abril de 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber- seguridad-2020-12 .
[5]. Andrew Marquardt, “Mientras Biden advierte sobre un ciberataque ruso, ¿cuáles son los precedentes? Esto es lo que sucedió cuando un importante oleoducto fue pirateado el año pasado”, Fortune, 22 de marzo de 2022, https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/ .

combustible para aviones a la costa este. Finalmente, Colonial pagó un rescate de casi 5 millones de dólares al grupo de hackers DarkSide para restaurar la red y recuperar los datos.

Punto de ruptura geopolítica

Desde estos ataques, las preocupaciones con Rusia no han hecho más que aumentar, alcanzando su punto álgido con la invasión de Ucrania. De hecho, la agresión de Rusia contra Ucrania incluye la guerra cibernética: un ataque a gran escala contra la red eléctrica ucraniana.[6] — además de la guerra tradicional, y aumenta la preocupación de que Rusia pueda tomar represalias contra las innumerables sanciones económicas que le han impuesto la OTAN y los EE.UU. Apenas una semana antes de la entrada formal de Rusia en Ucrania, la Agencia de ciberseguridad y seguridad de las infraestructuras (CISA) emitió una declaración poco habitual, "Shields Up (Escudos arriba)[7] ", en la que advierte a las empresas estadounidenses de todos los tamaños que adopten una postura reforzada en relación con la ciberseguridad y la protección de los activos críticos. "Los recientes avisos publicados por la CISA y otras fuentes no clasificadas revelan que los actores de amenazas patrocinados por el estado ruso están apuntando a las siguientes industrias y organizaciones en los Estados Unidos y otras naciones occidentales: investigación de COVID-19, gobiernos, organizaciones electorales, atención médica y farmacéutica, defensa, energía, videojuegos, nuclear, instalaciones comerciales, agua, aviación y fabricación crítica", escribió CISA en una declaración de marzo de 2022[8] evaluando las amenazas cibernéticas rusas.

En mayo de 2021, el presidente Biden firmó una orden ejecutiva[9] diseñada para mejorar el estado de la seguridad nacional en los EE. UU. La orden abordaba específicamente la necesidad de que las agencias gubernamentales revisaran y desarrollaran nuevas directrices y normas de ciberseguridad, y de que las organizaciones se centraran en mejorar la seguridad de la cadena de suministro de software y el intercambio de información sobre amenazas. Más recientemente, el presidente también emitió una declaración en la que reiteraba la amenaza de la ciberseguridad rusa y destacaba la evolución de las directrices de la CISA.[10] sobre el tema.

Rusia no es el único actor estatal que presuntamente respalda ciberataques desestabilizadores. Según un informe de 2021[11] de The Evanina Group, China se ha vuelto cada vez más agresiva en el frente cibernético, especialmente en lo que respecta a la adquisición de datos personales y la privacidad de los datos.

"La capacidad de China para obtener de manera integral nuestra propiedad intelectual y secretos comerciales a través de métodos ilegales, legales y sofisticados no se parece a nada que hayamos presenciado", dijo William Evanina, ex director del Centro Nacional de Contrainteligencia y Seguridad.

Evanina se refirió a numerosos incidentes cibernéticos vinculados al Partido Comunista Chino, incluida la violación cibernética de Equifax de 2017; una campaña de 2011-2018 de cuatro ciudadanos chinos para hackear decenas de empresas, universidades y entidades gubernamentales; y una campaña cibernética patrocinada por el estado de 2011 a 2013 que ataca a las compañías de oleoductos y gasoductos de EE. UU. (el Departamento de Justicia publicó un informe sobre este incidente en julio de 2021). También se refirió a un informe de julio de 2021 de la Agencia de Seguridad Nacional

[6]. IANS, Ucrania detuvo un ciberataque respaldado por Rusia en la red eléctrica", 14 de abril de 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid .
[7]. Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), "Shields Up", consultado el 22 de abril de 2022, https://www.cisa.gov/shields-up .
[8]. Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), "Russia Cyber Threat Overview and Advisories", Departamento de Seguridad Nacional, consultado el 22 de abril de 2022, https://www.cisa.gov/uscert/russia .
[9]. Administración de Servicios Generales de EE. UU. (GSA), "Orden ejecutiva 14028: Mejora de la ciberseguridad de la nación", 12 de mayo de 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order- 14028-mejorando-las-naciones-ciberseguridad .
[10]. Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), "Shields Up".
[11]. William Evanina, "Declaración de William R. Evanina, CEO, The Evanina Group, ante el Comité Selecto de Inteligencia del Senado, en una audiencia sobre la amenaza integral a Estados Unidos planteada por el Partido Comunista de China (PCCh), The Evanina Group, agosto 4, 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf .

(NSA), la Oficina Federal de Investigaciones (FBI) y CISA que publicó más de 50 tácticas y herramientas cibernéticas utilizadas por los hackers patrocinados por el estado chino contra los EE. UU.

Es en este complejo y peligroso entorno cibernético donde la SEC ha tomado medidas históricas para abordar la salud y la preparación cibernética en todo el panorama organizativo, en particular en lo que respecta a la presentación de informes a la SEC y (en algunos casos) al público. Estas medidas son las primeras de su clase y podrían tener importantes no solo para las empresas estadounidenses que cotizan en bolsa, sino también para las empresas de todo el mundo.

El gran cambio

Un primer paso histórico hacia la divulgación de incidentes cibernéticos

Las propuestas

En un lapso de dos meses, la SEC dio a conocer dos propuestas muy esperadas que abordan la ciberseguridad en el sector empresarial. La primera propuesta[12] , revelada en febrero de 2022, se enfoca en los asesores de inversión registrados, las empresas de inversión registradas y las empresas o fondos de desarrollo empresarial. Según las normas propuestas, los asesores y los fondos estarían obligados a:

- Adoptar e implementar políticas y procedimientos escritos de ciberseguridad para abordar los riesgos de ciberseguridad que podrían perjudicar a los clientes asesores y a los inversores de fondos.
- Informar de los incidentes de ciberseguridad significativos que afecten al asesor o a sus clientes de fondos o fondos privados a la SEC en un nuevo formulario confidencial.
- Divulgar públicamente los riesgos de ciberseguridad y los incidentes significativos de ciberseguridad ocurridos en los dos últimos años fiscales en sus folletos y declaraciones de registro.

Además, la propuesta establecería nuevos requisitos de mantenimiento de registros para los asesores y los fondos diseñados para mejorar la disponibilidad de la información relacionada con la ciberseguridad, así como para ayudar a facilitar las capacidades de inspección y aplicación de la SEC.

"El riesgo cibernético se relaciona con cada parte de la misión de tres partes de la SEC y, en particular, con nuestros objetivos de proteger a los inversores y mantener el orden en los mercados", dijo el presidente de la SEC, Gary Gensler, en un comunicado de prensa .[13] . "Las normas y modificaciones propuestas están diseñadas para mejorar la preparación en ciberseguridad y podrían mejorar la confianza de los inversores en la resistencia de los asesores y los fondos frente a las amenazas y los ataques de ciberseguridad".

Si bien estas reglas reflejan, aunque implícitamente, las expectativas de la SEC sobre cómo las entidades reguladas deben gestionar los riesgos de ciberseguridad y notificar los incidentes de ciberseguridad, la segunda propuesta hace explícitas tales expectativas. Dirigida a todas las empresas que cotizan en bolsa, la segunda propuesta[14] , publicada en marzo de 2022, pretende "mejorar y estandarizar la información relativa a la gestión de los riesgos de ciberseguridad, la estrategia, la gobernanza y la notificación de incidentes de ciberseguridad por parte de las empresas públicas que están sujetas a los requisitos de información de la Ley de Bolsa de Valores de 1934". Para ello, las nuevas normas exigirían a las empresas públicas proporcionar información sobre:

---

[12]. Comisión de Bolsa y Valores de EE. UU. (SEC), "Gestión de riesgos de ciberseguridad para asesores de inversión, empresas de inversión registradas y empresas de desarrollo empresarial", 9 de febrero de 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf .

[13]. Comisión de Bolsa y Valores de EE. UU. (SEC), "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds", comunicado de prensa, 9 de febrero de 2022, https://www.sec.gov/news/press-release/ 2022-20 .

[14]. Comisión de Bolsa y Valores de EE. UU. (SEC), "Gestión de riesgos cibernéticos, estrategia, gobernanza y divulgación de incidentes", 9 de marzo de 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf .

- Las políticas y procedimientos de la compañía para identificar y gestionar los riesgos de ciberseguridad. Con las reglas se incluye una lista extensa pero no exhaustiva de estrategias, políticas y procedimientos de gestión de riesgos que pueden estar sujetos a divulgación, que incluye:
    - Si el registrante tiene un programa de evaluación de riesgos de ciberseguridad.
    - Si la registrante contrata asesores, consultores, auditores u otros terceros en relación con cualquier programa de evaluación de riesgos de ciberseguridad.
    - Si el registrante tiene políticas y procedimientos para supervisar e identificar los riesgos de ciberseguridad asociados con el uso de cualquier proveedor de servicios externo.
    - Si el registrante lleva a cabo actividades para prevenir, detectar y minimizar los efectos de los incidentes de ciberseguridad.
    - Si el registrante tiene planes de continuidad del negocio, contingencia y recuperación en caso de un incidente de ciberseguridad.
    - Si los incidentes de ciberseguridad anteriores han informado cambios en la gobernanza, las políticas y los procedimientos o las tecnologías del registrante.
    - Si los riesgos e incidentes relacionados con la ciberseguridad han afectado o es razonablemente probable que afecten los resultados de las operaciones o la situación financiera del registrante.
    - Si los riesgos de ciberseguridad se consideran parte de la estrategia empresarial, la planificación financiera y la asignación de capital del registrante.

- El papel de la gerencia en la implementación de políticas y procedimientos de ciberseguridad, incluyendo:
    - Si determinados puestos directivos o comités son responsables de medir y gestionar los riesgos de ciberseguridad.
    - Si el solicitante de registro ha designado un director de seguridad de la información o alguien en un puesto comparable.
    - Si los procesos por los que dichas personas o comités son informados y supervisan la prevención, mitigación, detección y remediación de incidentes de ciberseguridad.
    - Si dichas personas o comités informan a la junta directiva o a un comité de la junta directiva sobre los riesgos de ciberseguridad, así como la frecuencia con la que informan.
    - Ya sea toda la junta, miembros específicos de la junta o un comité de la junta es responsable de la supervisión de los riesgos de ciberseguridad.
    - Si la junta está informada sobre los riesgos de ciberseguridad y la frecuencia de sus discusiones sobre dicho riesgo.
    - Si la junta o el comité de la junta considera los riesgos de ciberseguridad como parte de su estrategia empresarial, gestión de riesgos y supervisión financiera, y como lo hace.

- La experiencia en ciberseguridad de la junta directiva, si la hay, y su supervisión de los riesgos de ciberseguridad. Esto incluye información sobre:
    - Si la junta tiene experiencia laboral en ciberseguridad.
    - Si la junta ha obtenido una certificación o un título en ciberseguridad.
    - Si la junta tiene conocimientos, habilidades u otros antecedentes en ciberseguridad.

Además, la propuesta incluye una modificación al Formulario 8-K, que obligaría que las empresas públicas revelar los incidentes de ciberseguridad en un plazo de cuatro días hábiles, al igual que ya están obligados a hacerlo para cualquier otro evento material no programado. Dichas revelaciones incluirían:

- Cuándo se descubrió el incidente y si continúa.
- Una breve descripción de la naturaleza y el alcance del incidente.
- Si algún dato fue robado, alterado, accedido o utilizado para cualquier otro propósito no autorizado.
- El efecto del incidente en las operaciones de la empresa.
- Si la empresa ha solucionado o está solucionando el incidente.

Según la SEC, esta información proporcionaría a los inversores una información "consistente, comparable y útil para la toma de decisiones". “Hoy en día, la ciberseguridad es un riesgo emergente con el que los emisores públicos deben lidiar cada vez más”, dijo Gensler .[15] “La interconexión de nuestras redes, el uso de análisis de datos predictiva y el insaciable deseo de datos no hacen más que acelerarse, poniendo en riesgo nuestras cuentas financieras, inversiones e información privada. Los inversores quieren saber más sobre cómo los emisores están gestionando esos riesgos crecientes”.

La importancia histórica

En muchos sentidos, la estructura de estas normas descritas refleja otras normas de divulgación de la SEC, como las relacionadas con las condiciones financieras y los resultados operativos (Sarbanes-Oxley), la información privilegiada y los puntos fuertes, débiles, oportunidades y amenazas de la organización. Sin embargo, dar el paso adicional de elevar los riesgos de ciberseguridad hasta el punto de requerir tales divulgaciones no tiene precedentes.

“Estados Unidos es probablemente el primer país, y yo diría que el único, del mundo en regular la ciberseguridad”, dice Andy Watkin-Child, socio fundador de The Augusta Group y Parava Security Solutions, y fundador de Cybersecurity Maturity Model Certification Europe. (CMMC Europa). “Las empresas de EE. UU. pueden estar familiarizadas con el Reglamento General de Protección de Datos (GDPR) de la UE y pueden agrupar rápidamente estas propuestas, pero la protección de datos y la ciberseguridad son dos paradigmas diferentes. Hay una gran diferencia, y aparte de, posiblemente, el Reglamento de Gestión Financiera del Departamento de Defensa (DoD), que podría resultar en que incluso los contratistas extranjeros sean investigados por el Departamento de Justicia por vulnerabilidades de ciberseguridad - no hay nada como esto en el ámbito de la ciberseguridad”.

Watkin-Child también explica cómo la importancia de las nuevas normas podría tener fuertes efectos de propagación en el extranjero. “La crisis de Ucrania ha demostrado que la ciberseguridad es un arma y, de hecho, la OTAN la considera un grado de operación desde el 2016”, afirma. “La ciberseguridad es una herramienta ofensiva junto con las armas nucleares. El problema con eso es que, al ser un dominio de operación, representa una grave amenaza para las infraestructuras nacionales¨. La propuesta de la SEC está afectando primero a los grandes jugadores -las empresas comerciales- pero mi creencia es que esto, con suerte, se filtrara a las organizaciones más allá de la competencia de la SEC porque el panorama empresarial, así como el panorama federal, esta tan entrelazado a nivel global".

En la guerra, dice Watkin-Child, no se puede considerar la ciberseguridad dentro de un solo ejército; si un aliado es vulnerable, eso tiene un efecto directo en toda la operación conjunta. La protección de la ciberseguridad para empresas públicas -y privadas- no es diferente. “Si los sistemas de armas estadounidenses no pueden ser hackeados mientras que los sistemas británicos sí, no tiene sentido tener protección”, afirma. “Hay una razón por la cual el presidente [de EE. UU.] ha hablado con la OTAN sobre, entre otras cosas, los estándares comunes de ciberseguridad. Es lo correcto, porque si una entidad como Rusia utiliza el sector empresarial para atacar a los generadores de energía, por ejemplo, tu agua, tu electricidad, tu gas, tu sanidad... todo desaparecerá”.

[15]. Gary Gensler, "Declaración sobre la propuesta de divulgación obligatoria de ciberseguridad", Comisión de Bolsa y Valores de EE. UU. (SEC), 9 de marzo de 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309 .

Estas posibles consecuencias son obviamente de carácter macro, pero es importante no descartar también las consecuencias a nivel de organización. Y a pesar de lo que uno pueda sentir al ver las extensas listas de elementos que podrían justificar la inclusión en las declaraciones de ciberseguridad, no todas las consecuencias son negativas.

“Por supuesto, hay que tener en cuenta el aspecto legal de la información”, dice Watkin-Child, “pero, como se establece en las propuestas, no solo se informa a la SEC. Se informa a todos los participantes en el mercado que puedan tener un impacto en su negocio. La comunidad de inversores, las agencias de calificación crediticia, las compañías de seguros... todos ellos van a ver, junto con la SEC, lo bueno que es usted en la ciberseguridad, o no, según el caso. Esta transparencia conlleva un riesgo, pero también representa una oportunidad”.

La función de la Auditoría Interna sigue siendo la misma

Identificar, evaluar y comunicar

Las herramientas están en su lugar

La Ley Sarbanes-Oxley de 2002 (SOX) proporcionó responsabilidades adicionales y abrió nuevas oportunidades para que las funciones de auditoría interna añadieran valor a sus organizaciones. De hecho, a medida que las organizaciones navegaban por la nueva legislación, para muchos la auditoría interna se convirtió en sinónimo de cumplimiento de la SOX. Debido a la naturaleza de las nuevas propuestas de la SEC, hay motivos para creer que lo mismo podría suceder en el ámbito de la ciberseguridad.

A primera vista, esto puede parecer al menos una imposibilidad a corto plazo debido a la naturaleza compleja del campo de la ciberseguridad. Según los encuestados de Pulse[16], la ciberseguridad solo representa en promedio el 9 % de la asignación del plan de auditoría en las organizaciones que cotizan en bolsa, lo que supone un aumento del 7 % en los tres años anteriores, pero muy por debajo del 35 % asignada a la información financiera. Esto puede deberse a varias razones, como las limitaciones presupuestarias, la falta de recursos suficientes y la falta de conocimiento o experiencia.

Sin embargo, el verdadero valor que puede aportar la auditoría interna no es necesariamente a través del conocimiento de la ciberseguridad, sino el conocimiento de la identificación de riesgo, la comunicación del riesgo y la evaluación de los controles para hacer frente al riesgo. De hecho, estas son las mismas cosas que las propuestas de la SEC desean enfatizar para un riesgo específico.

“Es importante darse cuenta de que estas propuestas no son realmente de la ciberseguridad, sino sobre la gestión de riesgos de ciberseguridad”, dice Watkin-Child. “Cuando la gente piensa en ciberseguridad, todos piensan en implementar controles y arreglar cosas. Lo que busca la SEC es algo completamente diferente; busca que las organizaciones evalúen sus riesgos de ciberseguridad. Quieren que las juntas de las organizaciones tengan las estructuras de gobierno necesarias para evaluar y garantizar la supervisión de su programa de gestión de riesgos de ciberseguridad, sea cual sea la forma que adopte”.

“Lo que la SEC quiere ver es que las juntas asuman la responsabilidad de supervisar y asegurar el resto”, dice Manoj Satnaliwala, director ejecutivo de auditoría de Caliber Home Loans, Inc. “La brecha no está realmente en los estándares de ciberseguridad: existen marcos para guiar a las organizaciones, como el marco de ciberseguridad del NIST. La brecha real está en la rendición de cuentas, que puede convertirse rápidamente en un vaivén de responsabilidad”.

El papel de la auditoría interna puede ayudar a equilibrar este vaivén. “Las juntas y la gerencia necesitan ayuda. La auditoría interna a través del aseguramiento garantiza la rendición de cuentas y, mediante una mayor visibilidad en toda la organización, promueve la apropiación compartida del riesgo”, dice Satnaliwala. “El riesgo es diferente, pero el rol de la auditoría interna sigue siendo realmente consistente. Las funciones de auditoría no tienen que empezar de cero, y no es razonable esperar que cada taller de auditoría interna esté en el meollo de un programa de ciberseguridad, pero en lo que respecta a este reto, es poco más que mirar las propuestas de la SEC y preguntarse: '¿Cuáles son las expectativas de la SEC?' Mientras haya al menos algunos recursos de ciberseguridad ya implementados, no creo que se necesite ningún

[16]. El IIA, “2022 Pulso Norteamericano de Auditoría Interna,”

cambio en la función media de auditoría interna, aparte de ajustar los enfoques para garantizar una cobertura de riesgo adecuada".

Sin embargo, tener acceso a estos recursos de ciberseguridad suele ser más fácil de decir que de hacer. El desarrollo de cualquier grado de experiencia en ciberseguridad a través de la capacitación y certificaciones no sucederá de la noche a la mañana, y especialmente para las pequeñas funciones de auditoría interna con presupuestos limitados para contratar talentos costosos y de alta demanda, las opciones para desempeñar cualquier tipo de papel más allá del cumplimiento de los procesos son limitadas. En estos casos, la auditoría interna debe tener una comprensión global de dónde se puede acceder mejor a los conocimientos. Esto puede ser:

- **Dentro de la propia base de talento de la organización.** Aquellos con experiencia en una capacidad de auditoría de TI más tradicional suelen tener la base de conocimientos para completar la capacitación técnica en ciberseguridad con relativa rapidez. Además, algunos fundamentos de ciberseguridad pueden incorporarse en áreas como la gestión de cambios, los controles de acceso, las operaciones de TI y la recuperación ante desastres, lo que podría reducir la necesidad de la contratación externa a largo plazo.
- **Mediante la colaboración con las funciones de auditoría externa de segunda línea y de confianza.** Aunque la independencia y la objetividad de la auditoría interna deben mantenerse de conformidad con las *Normas Internacionales para la Práctica Profesional de la Auditoría Interna* (IPPF), establecer una relación de trabajo más colaborativa con las funciones relevantes, como la de TI, puede proporcionar a los auditores un acceso indirecto a competencias técnicas que, de otro modo, pueden ser difíciles o costosas de obtener.

Conclusión

Tiempo de preparación

La ciberseguridad, como tema, siempre está evolucionando, ya que los malos actores siguen innovando en sus enfoques y las empresas continúan innovando para frustrarlos. Sin embargo, mientras la historia de la ciberseguridad sigue escribiéndose, el año 2022 será recordado por los hitos alcanzados en un esfuerzo por contrarrestar las nefastas tendencias observadas en el panorama empresarial. Aunque las propuestas de la SEC deben superar un período de 60 días para recibir comentarios antes de que se publiquen las normas oficiales, no debería haber muchas sorpresas para las empresas que cotizan en bolsa y sus funciones de auditoría interna.

La auditoría interna puede y debe utilizar el tiempo que tiene, si no lo ha hecho, para hacer un balance del alcance total de los activos de su organización que deben tomarse en cuenta en una estrategia de ciberseguridad. Sin ese conocimiento, a los auditores internos tendrán dificultades para evaluar si los actuales controles, las políticas y estrategias de gobernanza relacionadas con la ciberseguridad son suficientes. Dichas evaluaciones no solo son importantes para la seguridad de la organización, sino también para toda la comunidad del mercado. El mundo está cada día más interconectado, y esto significa que las responsabilidades relativas a riesgos como la ciberseguridad son en gran medida compartidas. Después de todo, como la historia ha demostrado una y otra vez, la violación de una organización podría tener un impacto muy real en la seguridad de otra.

Una cadena es tan fuerte como su eslabón más débil.

PARTE 2

Socios críticos — Auditoría interna y el CISO

Sobre los expertos

Jerry Perullo

Jerry Perullo es el fundador de Adversarial Risk Management, una firma de gobierno y una empresa de estrategia de programas de ciberseguridad que permite a las empresas en crecimiento establecer rápidamente programas de ciberseguridad maduros. Antes de fundar Adversarial, Perullo se retiró como director de seguridad de la información de IntercontinentalExchange (NYSE:ICE) después de 20 años construyendo y liderando el programa de ciberseguridad en una familia global de infraestructura económica crítica, incluyendo la Bolsa de Valores de Nueva York. NACD Directorship Certified®, Perullo también forma parte de la Junta Directiva del Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC) durante 6 años, ultimamente como Presidente. Perullo también da conferencias en el Instituto de Tecnología de Georgia, donde es profesor de práctica en la Escuela de Ciberseguridad y Privacidad, y comparte sus experiencias con líderes de riesgo tecnológico a través de su podcast lifeafterCISO.com.

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal es Gerente de Auditoría Interna con sede en Dubái. Hassan fue destacado por el Instituto de Auditores Internos (IIA) como uno de los 15 líderes emergentes mundiales menores de 30 años. Hassan tiene un BBA, un MBA y un certificado en Estudios del Medio Oriente. Hassan también es CIA, CRMA y CFE. Hassan también posee certificaciones profesionales en Automatización de Procesos Roboticos (RPA), Análisis de Datos, Internet de las Cosas (IoT), Gestión de la Calidad, Salud y Seguridad, Gestión Ambiental y Gestión de Riesgos.

Alan Maran

Alan es el Jefe de Auditoría Interna (CAE) en Chewy, Inc. Lleva en la empresa desde enero de 2019. En este papel, es responsable de supervisar las actividades estratégicas y de ejecución generales para la función de auditoría interna, incluida la realización de evaluaciones de riesgos empresariales ágiles, propocionando apoyo de asesoramiento continuo y oportuno para diversas actividades defendidas por la administración; y la garantía sobre la idoneidad de los controles en los riesgos clave identificados para la organización, la alineación con las operaciones, los sistemas corporativos y la gobernanza de TI, el riesgo y cumplimiento (GRC) de TI en toda la empresa, el enfoque continuo en el desarrollo de los miembros del Equipo de Auditoría Interna, con un mayor enfoque en el análisis de datos, la ciberseguridad, privacidad de datos. Alan es un ejecutivo de auditoría experimentado que sigue apasionado por el aprendizaje, con más de 22 años de experiencia en empresas de comercio electrónico, Fintech, tecnología e industrias de fabricación. Antes de unirse a Chewy, ocupó puestos de liderazgos progresivos comenzando su carrera en Ernst & Young, LLC, y luego progreso en otros puestos de Auditoría Interna en organizaciones multinacionales de Fortune 500. Tiene un MBA; y un Master en Finanzas por la Universidad del Estado de Washington; es un Examinador de Fraude Certificado (CFE), un Experto Certificado en Blockchain y está afiliado a los Capítulos locales del Instituto de Auditores Internos.

Srini Srinivasan, PMP, CBIP

Srini Srinivasan es el Director de Seguridad de la Informacion y Datos de Chewy, Inc. Lleva en la empresa desde octubre de 2019, cuando Srini se incorporó como Jefe de Seguridad, Datos y Sistemas Corporativos. En este cargo, es responsable de supervisar la seguridad de la información, la gestión de plataformas de análisis y datos, los sistemas corporativos y la gobernanza, el riesgo y wl cumplimiento de TI(GRC) en toda la empresa. Srini es un experimentado ejecutivo de tecnología con más de 25 años de experiencia que abarca comercio electrónico, los servicios bancarios y financieros, el comercio minorista y el marketing. Antes de unirse a Chewy, ocupó puestos de liderazgo en Citizens Financial Group. Tiene un master en Informatica por la Universidad de Bharathidasan y un MBA por la Universidad de Bentley.

Introducción

Las asociaciones de ciberseguridad son fundamentales para el éxito

La ciberseguridad sigue siendo uno de los principales riesgos para todas las organizaciones. Las encuestas reflejan constantemente los esfuerzos implacables y descarados de los ciberdelincuentes para piratear datos confidenciales o por atraer a los no capacitados y a los desprevenidos para que divulguen información sensible o permitan el acceso a los malos agentes.

Por ejemplo, el Informe de Verizon sobre investigaciones de filtraciones de datos de 2022 refleja un sorprendente aumento del 13% en las filtraciones relacionadas con el ransomware en 2021, más que en los últimos cinco años combinados. Sin embargo, el informe concluye que los métodos más exitosos de ataques de ransomware siguen siendo constantes: el abuso de software de acceso remoto y uso compartido (40%) y del correo electrónico (35%), según el informe de Verizon.[17]

La nueva guía del IIA, Auditoría de operaciones de ciberseguridad: prevención y detección (GTAG) , está diseñada para ayudar a las organizaciones a examinar y priorizar la garantía sobre las operaciones de ciberseguridad. Su objetivo es ayudar a los auditores internos a definir las operaciones de ciberseguridad, identificar sus componentes, considerar las orientaciones de control pertinentes en los marcos de control de TI y comprender los enfoques para auditar las operaciones de ciberseguridad.

Una de las claves para mejorar el aseguramiento de la ciberseguridad que no se contempla en la guía es tener una relación saludable entre los jefes de auditoría interna y los directores de seguridad de la información (CISO). Esta relación potencialmente simbiótica puede ayudar a alinear la auditoría interna y la seguridad de la información en los marcos, riesgos y controles, al tiempo que apoya la gestión del creciente perfil de riesgo de ciberseguridad.

Este informe de Conocimiento Global examina los beneficios de una relación sólida entre los jefes de auditoría interna y sus contrapartes de seguridad de la información, analiza las vías para establecer y alimentar dichas relaciones al tiempo que garantiza la independencia de la auditoría interna, y evalúa cómo estas asociaciones pueden añadir valor a la organización.

17. "3 Conclusiones del informe de investigaciones de violación de datos de Verizon de 2022", J. Mack, Rapid7, 31 de mayo de 2022, https://www.rapid7.com/blog/post/2022/05/31/3-takeaways-from- el-2022-verizon-data-breach-investigations-report/ .

El caso de la Ciberseguridad Colectiva

El riesgo cibernético exige un enfoque integral

La ciberseguridad sigue siendo un área de riesgo que crece y evoluciona, y cada año los planes de los ciberdelincuentes se vuelven más sofisticados y abundantes. No faltan estadísticas que muestren que las organizaciones siguen siendo vulnerables a los ataques cibernéticos. Al mismo tiempo, crece la presión para que las organizaciones de todo el espectro de la industria adopten estrategias empresariales basadas en datos que dependen en gran medida de la recopilación, la gestión, análisis y utilización de datos, mientras aprovechan las nuevas tecnologías para mejorar el rendimiento y los resultados.

Al igual que ocurre con otras áreas de riesgo importantes, el riesgo cibernético debe entenderse y gestionarse en toda la organización. Sin embargo, pocas las organizaciones que adoptan un enfoque global para gestionar la ciberseguridad, según el informe " El estado de la resiliencia cibernética " , elaborado por Microsoft y la firma de gestión de riesgos y corretaje de seguros Marsh. Basado en una encuesta[18] de más de 600 responsables de la toma de decisiones sobre riesgos cibernéticos, el informe concluye que solo 4 de cada 10 organizaciones involucran a la planificación legal, corporativa, financiero, de las operaciones o la gestión de la cadena de suministro en la elaboración de planes de riesgos cibernéticos.[19]

“Una de las cosas que frena la confianza es que la mayoría de las empresas no han adoptado un enfoque integral del riesgo cibernético; un enfoque que, en esencia, se basa en la comunicación de base amplia y fomenta la colaboración y la alineación, entre las partes interesadas durante los momentos clave de la toma de decisiones en su viaje de resiliencia cibernética”.[20] según el informe.

Entre las principales tendencias de riesgo identificadas en el informe:

“Los objetivos cibernéticos específicos de la empresa -incluyendo medidas de ciberseguridad, los seguros, los datos y la analítica, y los planes de respuesta a incidentes- deben estar alineados con la construcción de la resiliencia cibernética frente a la simple prevención de incidentes, ya que toda la organización puede esperar un ciberataque”.[21]

Para respaldar un enfoque eficaz en toda la empresa, los jefes de auditoría interna pueden contribuir significativamente estableciendo y fomentando relaciones con los CISO. Tales relaciones deben basarse en la comprensión, los objetivos y el respeto mutuos.

El veterano CISO y fundador de Adversarial Risk Management, Jerry Perullo, que trabajó en la empresa matriz de la Bolsa de Nueva York, Intercontinental Exchange (NYSE: ICE), matriz, dijo que una mala comunicación o un entendimiento poco claro de las funciones de seguridad de la información y de auditoría interna pueden perjudicar la alineación en la ciberseguridad. Por el contrario, una buena relación entre los responsables de la auditoría interna y la seguridad de la información abre la puerta a una comprensión más profunda de los objetivos, la estrategia, las operaciones y las políticas que pueden hacer que la auditoría interna -y, por extensión, sus conclusiones y recomendaciones, sean más relevantes para los líderes de riesgos cibernéticos., la gerencia ejecutiva y la junta, dijo. Además, una sólida relación entre la auditoría interna y los equipos de seguridad de la información amplía el conocimiento de la misión crítica de cada área y cómo ambas apoyan a la ciberseguridad general.

18. “Encuesta de riesgo cibernético de Marsh y Microsoft 2022”

19. “ El estado de la resiliencia cibernética”, Marsh Microsoft, 2022, https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html?utm_source=forbes&utm_medium=referral -link&utm_campaign=gl-cyber-risk-2022-the-state-of-cyber-resilience .

20. ibídem.

21. ibídem.

“Al final del día, la auditoría interna quiere educarse sobre la seguridad de la información”, dijo Perullo. “Hay muchas maneras de hacer esto, pero no hay nada como aprender del propio equipo (de seguridad de la información)”.

En su trabajo de consultoría con empresas emergentes, Perullo suele empezar por establecer programas de gobernanza para la ciberseguridad. Eso generalmente implica crear un comité de gobernanza de ciberseguridad multifuncional que incluya la gestión ejecutiva, las finanzas, el departamento legal y seguridad de la información. También suelen incluir a altos ejecutivos de auditoría interna como observadores, dijo.

Cinco claves para el éxito

Beneficios de una sólida relación entre auditoría interna y CISO

La auditoría interna y los CISO identifican numerosos beneficios de una asociación bien elaborada. Los detalles y la sofisticación de tales asociaciones pueden variar según el tamaño de la organización, el nivel de regulación en cada industria o el perfil de riesgo de ciberseguridad de una organización. Sin embargo, surgen cinco áreas en las que la colaboración y la cooperación pueden generar claros beneficios sin importar el tamaño de la organización o la industria en la que opera.

Comprender y alinearse con el perfil de riesgo cibernético de la organización

Un perfil de riesgo es un análisis cuantitativo de los tipos de amenazas que enfrenta una organización. Desde una perspectiva de ciberseguridad, dicho análisis identifica activos y riesgos cibernéticos, examina políticas y prácticas diseñadas para administrar esos riesgos y se esfuerza por comprender cualquier vulnerabilidad que pueda estar presente. La comprensión de la auditoría interna del perfil de riesgo cibernético proporciona una base para construir un plan de auditoría que no solo respalde el enfoque general de la organización hacia la seguridad cibernética, sino que también puede mejorar la relevancia y el valor de la auditoría interna en esta área crítica.

Alan Maran, director de auditoría interna de Chewy, Inc., ha desarrollado una sólida relación con el CISO de la organización, Srini Srinivasan, durante los tres años transcurridos desde que el minorista en línea de alimentos para mascotas y otros productos relacionados con ellas se hizo público. Srinivasan dijo que la seguridad de la información se asoció con la auditoría interna, el departamento legal y otras partes interesadas para evaluar y medir de manera integral el perfil de riesgo cibernético de la empresa según el marco de seguridad cibernética del NIST .

“Esa es nuestra línea de base”, dijo Srinivasan. “Luego establecimos una hoja de ruta de tres años para la seguridad cibernética y la gobernanza, la adaptamos y la mejoramos en función de la evaluación del marco de ciberseguridad que hicimos. Ahora hacemos una evaluación anualmente para ver si estamos haciendo mejoras en esas áreas de oportunidad y evaluar cómo se miden nuestras puntuaciones de riesgo en general”.

Este enfoque de colaboración que involucra a la auditoría interna desde el principio permitió una estrategia mutua que incorpora servicios de asesoría y garantía de auditoría interna con el objetivo de mejorar constantemente la postura general de seguridad cibernética de Chewy.

“No se trata de una perspectiva de 'siempre necesito auditar la TI y la seguridad'. También debemos apoyarlo”, dijo Maran. “Desde el lado de la auditoría interna, vemos que somos un socio con una fuerte mentalidad de apoyar a Srini y su equipo en el desarrollo de una estrategia completa”.

Una ventaja añadida de la colaboración es que la seguridad de la información y la garantía independiente se están incorporando en los nuevos proyectos desde el principio. En otras palabras, la seguridad de la información, la auditoría interna y los controles de gobernanza han dejado de ser algo secundario, dijo Srinivasan.

“Lo qute e hacemos es que, es poner en marcha las iniciativas del proyecto, nuestros equipos se involucran y se asocian con los equipos de ingeniería, los equipos de productos y los equipos comerciales. . . ¿Cuáles son las consideraciones de seguridad? ¿Seguimos las mejores prácticas?” dijo Srinivasan.

Este enfoque ayuda a identificar, minimizar y, si es posible, eliminar los riesgos cibernéticos mediante la creación de procesos y controles apropiados a medida que se desarrolla el proyecto, dijo Srinivasan. “Entonces, cuando el proyecto se pone en marcha, se vuelve muy fácil para ambos (equipos) porque tenemos un entendimiento sólido. Cuando cumplimos con las evaluaciones de control de auditoría o las revisiones de acceso o los controles de gobierno, tenemos muchos más conocimientos”.

Comprensión de los roles

La relación construida por Maran y Srinivasan se vio favorecida en gran medida por el hecho de que Chewy era una empresa relativamente nueva que cotizaba en bolsa, lo que brindó la oportunidad de dar forma a la relación desde cero. Esto también generó una expectativa de comunicación abierta y frecuente entre Maran, Srinivasan y sus equipos.

“Era una forma ideal de establecer esta transparencia y confianza entre las partes interesadas clave, por lo que no queríamos dejar pasar esta oportunidad”, dijo Srinivasan.

Esto no quiere decir que nunca haya desacuerdos. Pero cuando surgen conflictos, la relación facilita el debate y la búsqueda de una solución que sirva a ambas partes, dijo Srinivasan.

“Para mí no hay ningún beneficio en mantener algo alejado de la auditoría interna”, dijo. “Cuanto más sepan sobre lo que estamos haciendo. . . mayor nivel de apreciación tendrán. Del mismo modo, desde la perspectiva de la auditoría interna, puedo decir que creo que no hay ‘te lo dije” aquí”.

En última instancia, el enfoque colaborativo permite operar de manera ágil donde la auditoría interna forma parte de un proceso en el que las deficiencias pueden detectarse y abordarse antes, dijo Srinivasan.

Maran añade que la interacción franca afirma y refuerza la comprensión mutua de los papeles.

“Srini no da por sentado que lo sabemos todo, pero al mismo tiempo, es respetuoso con nuestras preocupaciones y nuestro punto de vista”, dijo.

Relevancia

Proporcionar conocimientos y conclusiones de aseguramiento sobre cuestiones críticas en el momento adecuado es uno de los mayores desafíos de la auditoría interna en cualquier área de riesgo, pero especialmente en de la ciberseguridad. Este riesgo, que evoluciona rápidamente, exige que la garantía sea pertinente y oportuna.

Perullo advirtió que los compromisos de auditoría interna y las recomendaciones relacionadas que no se alinean con la misión de seguridad cibernética de la organización pueden hacer más daño que bien. Pueden crear confusión dentro de la seguridad de la información acerca de lo que la auditoría interna quiere ver, especialmente si la auditoría interna no está segura.

“Es posible que la auditoría interna inicialmente no tenga una buena idea de lo que quiere ver”, dijo. “Es mejor colaborar antes de la auditoría y observar el proceso de gobernanza cibernética para garantizar que las auditorías estén alineadas con la misión”.

Hassan Khayal, consultor de auditoría interna con experiencia en ciberseguridad, dijo que esta es un área donde la auditoría interna es particularmente vulnerable a las críticas. Con demasiada frecuencia, los auditores internos se resisten a conocer a los miembros de los equipos de TI o de seguridad de la información y aprender más sobre el tema con el pretexto de proteger la independencia de la auditoría interna.

“Fui descaradamente con mis primeras asignaciones y le diría a la persona de TI: 'Escucha, estoy aquí más para aprender de ti que otra cosa'. Tomaría a la persona que entendía el proceso o los conocimientos técnicos y tendría una conversación amistosa durante el almuerzo para conocer exactamente los detalles de lo que estaban haciendo”.

Este proceso de formación también ayuda al auditor interno a comprender la madurez de la ciberseguridad de la organización, lo que es fundamental para brindar recomendaciones relevantes, dijo Khayal.

“Si se trata de una pequeña o mediana empresa, o incluso de una organización más grande que no cotiza en bolsa, entonces no hay mucho que pueda o deba hacer”, dijo. “En cierto punto, las recomendaciones pueden ser demasiado agresivas, por lo que las recomendaciones que hacen no son realistas”.

El establecimiento de una sólida relación entre los equipos de auditoría interna y de seguridad de la información reduce la probabilidad que se produzcan compromisos y recomendaciones de auditoría irrelevantes o equivocados. Ese beneficio ha sido afirmado en Chewy.

“El equipo de Alan y el propio Alan están muy familiarizados con nuestra estrategia de seguridad general, desde una perspectiva tecnológica, qué estamos haciendo al respecto y cuáles son algunos de nuestros principales riesgos”, dijo Srinivasan. “Nosotros, no tenemos la enorme brecha entre las calificaciones de riesgo y nuestras capacidades internas. Esto continuará ayudándonos a hacer un mejor trabajo en términos de mejorar el conocimiento general de nuestro equipo o de los miembros de nuestro equipo en Chewy, así como de nuestro equipo de liderazgo”.

Comunicar al consejo de administración y a la dirección ejecutiva

La cultura organizativa de Chewy ofrece una mayor visión del riesgo respaldada por conversaciones abiertas. Maran y Srinivasan han asumido los roles de educar a los participantes (la gerencia ejecutiva y la junta directiva) sobre su colaboración y los beneficios que ha aportado.

“En muchas organizaciones, las personas están adoptando una actitud individualista. Es como, 'Oh, es seguridad de TI, así que hablaremos con el CISO, y el CISO se encargará de eso'. Pero dentro de una perspectiva de riesgos integrada o de gestión de riesgos empresariales, cualquier riesgo que veamos para la empresa puede volver a toda la empresa”, dijo Maran. “Un ataque cibernético puede afectar a tus operaciones, a tus resultados y a tus finanzas. Srini también ha hecho un buen trabajo al educar a los líderes sobre lo que estamos haciendo y sobre los riesgos que estamos mitigando. Así que, desde esa perspectiva, ha sido una colaboración”.

Esto también se traduce en respuestas oportunas y ágiles a los cambiantes panoramas cibernéticos regulatorios y de riesgos. Por ejemplo, Maran y Srinivasan confían cada vez más en que la organización puede responder a las reglas de informes de seguridad cibernética propuestas por la Comisión de Bolsa y Valores de EE. UU. presentadas en el primer trimestre de 2022.

Esa colaboración va más allá de la seguridad de la información y auditoría interna. “No se limita a la seguridad de la organización”, dijo Srinivasan. “Tenemos otros participantes clave en los que tenemos asociaciones similares, incluido el equipo de contabilidad y el equipo legal. Creo que establecer estas relaciones transparentes nos prepara muy bien para cuando entran en escena estas normativas en evolución y los requisitos adicionales”.

Aunque la dirección de Chewy se beneficia de mensajes coherentes y unificados, Khayal advierte sobre los peligros significativos que supone no mantener a la dirección actualizada sobre el estado y las necesidades de ciberseguridad de la organización. La TI y la ciberseguridad pueden verse rápidamente como simples centros de costos cuando los líderes no están informados ni educados al respecto, dijo. Cuando la auditoría interna evita comprender la seguridad de la información, es menos probable que brinde una garantía valiosa y relevante en esta área, dijo Khayal. Esto afecta las opiniones sobre ciberseguridad desde la dirección ejecutiva y la perspectiva de la junta.

Proteger y respetar la independencia

Khayal, que está trabajando para convertirse en un auditor certificado de sistemas de información (CISA), dijo que su compromiso de conseguir la certificación ya ha impulsado su credibilidad entre los profesionales de TI y seguridad de la

información. También le ha permitido interactuar con esos compañeros de trabajo de cierto nivel, lo que hace que sea más probable que ofrezcan información que podría considerarse demasiado avanzada o compleja para un auditor que ingresa solo cuando realiza un trabajo de auditoría. Es más, no ve esa interacción como una amenaza a su capacidad para realizar un trabajo de auditoría independiente y objetivo.

“Al final del día, estás en el lugar de trabajo”, dijo. “Cuando les decimos a los auditores que sean independientes, personalmente no creo que les estemos diciendo, 'No puedes tener amigos en el trabajo; debes ir siempre a almorzar solo'”.

Khayal dijo que adopta este enfoque en todas las áreas de la organización. Habla de Linux con el personal informático o de las redes sociales con el personal de marketing.

“Es una buena oportunidad para desarrollarte profesionalmente mientras mantienes las relaciones”, dijo. “Es como cuando les decimos a nuestros clientes de auditoría o a los auditados: 'Estamos observando el proceso y las transacciones; no vamos tras la gente.' Entonces, cuando llevas a la gente a almorzar, no estás tomando el proceso o la transacción”.

En Chewy, la estrecha relación de trabajo entre Maran y Srinivasan respalda el entendimiento mutuo de la necesidad de una verificación independiente, dijo Maran.

“La naturaleza de nuestra profesión es confiar pero verificar. Desde el punto de vista de la objetividad, tengo el deber de hacerlo”, dijo. “Entonces, sí, confiamos hasta cierto punto, especialmente en las cosas incrementales que hemos probado. En la mayoría de los casos validamos que las cosas no han cambiado. Pero sigo probando también la integridad de la información proporcionada por la gestión. No miramos un informe solo por su valor nominal; volvemos a la fuente para asegurarnos de que estamos obteniendo los mismos resultados que ellos para garantizar que sea completo y preciso”.

En última instancia, comprender el papel de cada uno en la organización lo hace más fácil, dijo Maran.

Aquí hay un acuerdo. Esto es lo que necesito hacer. Esta es el aseguramiento que necesito brindar al liderazgo senior: la junta, las partes interesadas y el comité de auditoría”, dijo. “Nos estamos alineando en las auditorías que vamos a hacer para el año. Nos alineamos en el alcance. Sí, a veces tenemos conversaciones sobre nuestro punto de vista y cómo lo ven los demás, pero rara vez no estamos de acuerdo en las áreas de riesgo sobre las que debemos brindar seguridad”.

Srinivasan agrega que el enfoque en un enfoque de ciberseguridad basado en datos supone que habrá un acuerdo sobre los hechos entre la seguridad de la información y la auditoría interna.

“Si hay algún desacuerdo, debemos trabajar y llegar al mismo conjunto de hechos”, dijo. “Entonces puedes tener cierto nivel de subjetividad, que individualmente, puede decir, 'Vale, siento que esto es de criticidad media o de criticidad alta o de criticidad baja'. Creo que eso conduce a una discusión y a resultados saludables, en lugar de chocar cabezas sin tener un marco de referencia común”.

Añadir valor

Mejorar la resistencia de la ciberseguridad

Srinivasan dijo que su enfoque desde el principio fue mantenerse fiel a la misión de Chewy. Eso significó lograr tres cosas: practicar los principios operativos internos de la empresa, garantizar la alineación entre la seguridad de la información y la auditoría interna, y generar confianza a través de la transparencia.

“Creo que hemos recorrido un largo camino, y esto realmente está dando muchos frutos en cuanto a lo que supone que los miembros del equipo y la dirección se mantengan al día”, dijo.

Como se señaló anteriormente, el alto grado de comunicación, colaboración y cooperación respalda un enfoque ágil que incorpora continuamente la auditoría interna en el proceso de ciberseguridad. Srinivasan señala que las fuerzas principales, como el creciente enfoque en la sostenibilidad, las consideraciones de la cadena de suministro, las condiciones del mercado, los desarrollos geopolíticos y más, requieren enfoques fuertes para la ciberseguridad y la garantía relacionada.

“Creo que eso nos obliga a estar alerta, ágiles, receptivos y relevantes”, dijo. “Si optamos por un enfoque clásico en cascada con tiempos de espera más largos, perderemos el tren. Me alegro por el nivel de compromiso que tenemos”.

Ampliar los conocimientos

Otro beneficio intrínseco de la asociación es cómo ambos equipos han evolucionado y crecido en su comprensión y apreciación de los enfoques de cada uno para lograr el mismo objetivo: mantener la ciberseguridad de la organización.

“Siempre estamos comprobando el conocimiento técnico de cada uno en términos de, '¿Vimos esto? ¿Estás pensando en eso? Este es mi punto de vista sobre este análisis de riesgo: ¿se alinea también con su perspectiva?'”, dijo Maran. “Entonces, desde el principio ya estamos pensando dónde buscaremos, y Srini está participando en las reuniones iniciales. Está en la conversación antes de que empecemos a auditar. Realmente no hay sorpresas”.

Pero el verdadero valor agregado proviene de la colaboración una vez que se ejecutan los compromisos de auditoría y la auditoría interna trata directamente con el personal de seguridad y TI.

“Desde la perspectiva del desarrollo profesional, especialmente con la mentalidad de TI y seguridad cibernética, en realidad es muy gratificante porque ves mucho más que solo marcar casillas y decir: '¿Hiciste esto?'”, dijo Maran. “Hay mucho más. Hay interpretación; hay experiencia técnica que debe hacerse bien, así que creo que ahí es donde mi equipo aprende mucho”.

Conclusión

Una relación saludable entre la auditoría interna y la seguridad de la información ofrece múltiples beneficios para la organización, principalmente para alinear y comprender el perfil de riesgo cibernético de la organización, desde vulnerabilidades y oportunidades hasta pruebas de madurez y penetración.

Además, una relación sólida puede mejorar la resiliencia y la agilidad en caso de que la organización necesite responder a incidentes cibernéticos, cambios en los factores que influyen en la ciberseguridad o el panorama regulatorio en evolución. Ayuda a proporcionar mensajes coherentes y unificados al C-suite y a la junta sobre los riesgos, las necesidades, las prioridades y la salud de la ciberseguridad. La independencia de la auditoría interna se puede proteger con éxito, incluso mejorar, cuando ambas partes desarrollan una comprensión y una apreciación más profundas de las funciones, enfoques y deberes. En última instancia, una relación sólida entre los jefes de auditoría y los CISO puede fortalecer la seguridad de TI al respaldar un enfoque de ciberseguridad en toda la empresa.

“La mentalidad está cambiando de una simple auditoría: 'Necesito entrar, evaluar y presentar observaciones significativas', a decir realmente: 'Esta es mi empresa; esto es lo que realmente me importa; y así es como voy a ayudar a este equipo a tener éxito'”, dijo Maran.

PARTE 3

Respuesta y Recuperación de Incidentes Cibernéticos

Sobre los expertos

Brian Tremblay

Brian Tremblay lidera la Práctica de Cumplimiento en Onapsis, donde es responsable de ayudar a los clientes a comprender y navegar los desafíos y oportunidades creados por la creciente superposición de cumplimiento, ciberseguridad y continuidad comercial relacionada con los controles generales de TI y asuntos regulatorios y de cumplimiento como Sarbanes- Oxley (SOX) y el Reglamento General de Protección de Datos (RGPD). Antes de Onapsis, fue el DEA de la empresa de semiconductores de alta tecnología Acacia Communications. Además de fundar y dirigir todas las actividades de la función de auditoría interna, ayudó a preparar la organización para salir a bolsa (incluida la implementación de SOX) y facilitó la implementación de la gestión de riesgos empresariales (ERM). Previamente, Tremblay fue Director de Auditoría Interna en Iron Mountain, supervisando todas las auditorías y proyectos dentro de América del Norte, además de servir de enlace con los gerentes de calidad global. Anteriormente, como gerente sénior en Houghton Mifflin Harcourt, creó un departamento de auditoría interna y ejecutó una implementación de SOX. Anteriormente en su carrera, trabajó en Raytheon y Deloitte.

DaMon Ross Sr.

En 2020, DaMon Ross Sr. inició Cyber Defense International, donde él y su equipo aprovechan las operaciones de ciberseguridad de élite y las capacidades de inteligencia de amenazas cibernéticas para ofrecer soluciones y servicios de ciberseguridad accesibles a organizaciones que carecen de los medios para desarrollar las capacidades por sí mismas. Antes de iniciar Cyber Defense International, Ross se desempeñó como vicepresidente senior de operaciones de ciberseguridad en SunTrust Bank. En este cargo, se le asignó la tarea de crear el centro de operaciones de ciberseguridad 24/7/365 de SunTrust. Como tal, Ross creó equipos que se especializan en inteligencia cibernética, monitoreo de amenazas cibernéticas, respuesta a incidentes cibernéticos y delitos cibernéticos. En particular, también se asoció con éxito con socios legales, de recursos humanos, seguridad corporativa y ética empresarial y riesgo para establecer el primer programa de monitoreo de amenazas internas del banco. Ross también facilitó el establecimiento de numerosas asociaciones para compartir información, incluidas aquellas con la Fuerza de Tarea de Delitos Electrónicos del Servicio Secreto de los Estados Unidos y el Departamento de Seguridad Nacional.

Introducción

Volver a lo básico

La seguridad cibernética ha sido durante mucho tiempo un punto focal destacado de las organizaciones y sus funciones de auditoría interna, y con la introducción de las nuevas propuestas de la Comisión de Bolsa y Valores (SEC) sobre gestión de riesgos de seguridad cibernética, estrategia, gobernanza y divulgación de incidentes, 2022 no ha sido una excepción. El ímpetu para estas y otras propuestas regulatorias está justificado. Según un informe del Identity Theft Resource Center , se registraron 1862 violaciones de datos de alto perfil en 2021, una cifra que superó el total de 2020 en un 68 %, así como el récord histórico establecido en 2017. Ninguna industria se ha librado de la tendencia.[22]

En este entorno, las organizaciones desean, y de hecho requieren, controles y procesos de ciberseguridad claros y sólidos construidos sobre fundamentos básicos, incluido el aprendizaje continuo sobre el riesgo y sus regulaciones relacionadas, así como la comunicación y la alineación entre la junta directiva, la gerencia y la auditoría interna. La Parte 1 de la serie de tres partes del IIA, Ciberseguridad en 2022, se centra en los posibles impactos regulatorios, mientras que la Parte 2 examina los beneficios de una relación simbiótica entre los directores de seguridad de la información (CISO) y sus contrapartes de auditoría interna. Esta parte final enfatiza el desarrollo y la implementación de la estrategia de respuesta a incidentes cibernéticos de una organización y, más específicamente, donde la auditoría interna puede proporcionar valor organizacional al evaluar los controles críticos para recuperarse rápidamente de una violación de seguridad cibernética.

[22]. Centro de recursos de robo de identidad, "El informe anual de violación de datos del Centro de recursos de robo de identidad establece un nuevo récord para el número de compromisos", 24 de enero de 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021 -annual-data-breach-report-sets-new-record-for-number-of-compromises/ .

Controles clave

Dar a la auditoría interna un papel en la respuesta cibernética

La falacia de la respuesta a incidentes

Aunque los términos "respuesta a incidentes cibernéticos" y "respuesta y recuperación de ciberseguridad" son exactos y útiles, también implican una visión un tanto incompleta de lo que tales planes requieren para ser efectivos.

La auditoría interna en su función más esencial proporciona a las organizaciones una garantía independiente sobre la gestión de riesgos. Esto incluye no solo la garantía de una respuesta adecuada a los incidentes cibernéticos, sino también una evaluación adecuada de los controles para garantizar que el riesgo y sus efectos se mitiguen o, idealmente, se eviten. Para alcanzar un estándar tan elevado sobre cualquier riesgo dado, la atención no debe reservarse simplemente para responder a un riesgo. En cambio, es más efectivo ver la respuesta a incidentes cibernéticos de una manera holística y cíclica que prioriza los controles preventivos y las medidas de respuesta activa.

"La gestión de riesgos es como una rueda", dijo Brian Tremblay, líder de prácticas de cumplimiento en Onapsis, Inc. "Al comienzo de la rueda, tenemos los controles correctos y los procesos son lo que creemos que deberían ser. Y luego, cuando sucede algo, la conversación se convierte inmediatamente en: '¿Funcionaron los controles como se esperaba y sucedió lo que pensamos que iba a suceder?' Luego, a partir de ahí, aprendemos qué debe cambiar y el ciclo comienza de nuevo. Si la única vez que está respondiendo a un evento es después del hecho, es probable que esté siendo ineficiente con su tiempo y recursos. El presente y el futuro deben tener el mismo peso porque no solo estamos construyendo el negocio de hoy, estamos construyendo el negocio del futuro. Dado que las organizaciones a menudo luchan con esto, este es un lugar realmente importante donde la auditoría interna se debe enfocar".

Fundamentos inmutables

Los riesgos rara vez se vuelven menos complejos, y debido a que la ciberseguridad es intrínsecamente altamente técnica, la curva de aprendizaje para comprender tanto el riesgo en sí como los sistemas necesarios para mitigarlo solo se ha vuelto más pronunciada con cada avance tecnológico posterior. Sin embargo, esto no significa necesariamente que la estructura fundamental de un plan de respuesta a incidentes cibernéticos y los controles dentro de él cambien drásticamente.

Estos controles se describen en la Guía complementaria más reciente del IIA, *Auditoría de respuesta y recuperación ante incidentes cibernéticos* , y se pueden agrupar en cuatro objetivos comerciales de alto nivel:

- **Planificación de respuesta a incidentes.** Deben establecerse políticas y procedimientos para orientar la determinación de si se ha producido un incidente y qué hacer al respecto. La planificación debe involucrar a las partes interesadas clave, definir roles y responsabilidades, y probarse según corresponda para promover la concienciación y la ejecución.
- **Identificación de incidentes.** Los procesos para analizar los datos de los controles de detección conducen a la determinación de la existencia de un ciber incidente, que suele ser el desencadenante de la ejecución de uno o más planes de respuesta.
- **Comunicaciones.** Hay muchas partes interesadas potenciales en los incidentes cibernéticos, por lo que cada plan de respuesta debe incorporar una estrategia de comunicación para la notificación adecuada y oportuna de los impactos y los esfuerzos de resolución.

- **Respuesta Técnica y Recuperación.** La naturaleza del incidente determina en gran medida la remediación técnica necesaria y los controles de restauración, que a menudo implican la coordinación de esfuerzos internos y externos.[23]

Lograr estos objetivos comerciales y adherirse a un marco de respuesta a incidentes cibernéticos establecido, como el Marco para mejorar la infraestructura crítica del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) proporcionar: conocimiento que los equipos de auditoría interna pueden o no poseer. Sin embargo, al mismo tiempo, hay un amplio espacio para que otros con disciplinas menos técnicas pero igualmente valiosas proporcionen un valor significativo. La auditoría interna, con su exclusivo acceso y comprensión de las funciones de la organización en todos los departamentos, así como su perspectiva independiente fundamental para proporcionar un aseguramiento objetivo, es una de esas disciplinas.

“Desde la perspectiva de la auditoría interna, el enfoque de la respuesta a incidentes cibernéticos no es diferente de cualquier otro riesgo en el sentido de que el enfoque está en el proceso real y el resultado de ese proceso”, dijo DaMon Ross Sr., fundador de Cyber Defense International, LLC, y anterior vicepresidente senior, jefe de operaciones de seguridad cibernética en SunTrust. “Incluso con la naturaleza técnica de los materiales, cualquier auditor interno acostumbrado a operar en un espacio de proceso captará lo que importa con bastante rapidez”.

Dicho proceso tiene más que un parecido pasajero con lo que la auditoría interna puede ver en los programas de cumplimiento Sarbanes-Oxley (SOX), planes de respuesta a crisis o cualquier estrategia de gestión de riesgos establecida. "Diferentes organizaciones tienen diferentes terminologías, pero un plan de incidentes cibernéticos es esencialmente una política de gobierno que describe cuándo ocurre un incidente cibernético, cuáles son las funciones y responsabilidades de todas las partes aplicables y quién debe estar en la mesa para la toma de decisiones", dijo. Ross.

Tremblay expresó un sentimiento similar. Los controles relevantes para los riesgos cibernéticos también forman parte de los marcos utilizados para gestionar los riesgos de cumplimiento asociados con Sarbanes-Oxley, dijo.

Por ejemplo, uno de los primeros pasos que toman los piratas informáticos cuando ingresan a cualquier tecnología es acceder a los derechos y privilegios necesarios para lograr su objetivo. En el gran esquema de riesgo, esto cae bajo el riesgo de acceso no autorizado. No hay diferencia si eso se aplica a SOX o un riesgo cibernético, dijo Tremblay. “Los riesgos, cuando se reducen a sus formas más simples, y los controles para mitigar esos riesgos, son esencialmente idénticos”.

Controles de documentación

Como mencionó Tremblay, los controles que están contenidos dentro de dicha política también tienen una superposición significativa con lo que se puede ver con otros riesgos organizacionales. Un ejemplo es tener un proceso de documentación eficaz. Ross está de acuerdo. Las organizaciones deben comprender cómo se ven los flujos de trabajo que documentan adecuadamente los incidentes cibernéticos y cómo se unen todas las partes móviles que se ejecutan en paralelo, dijo.

“Esto no es solo para grandes incidentes. Toda organización debería tener una función que se ocupe de este día a día. Digamos que una computadora tiene malware. Son pequeños incidentes como ese los que pueden convertirse en incidentes más grandes, y en el caso de que ocurra lo peor, la documentación adecuada ayuda a comprender cómo se intensificó. Esa función es un control en sí misma”.

Detección y controles de infraestructura física

Otro control crítico, y que cae bajo la rúbrica de riesgos de acceso no autorizado, es la infraestructura física. Si bien es posible que dichos controles no le vengan a la mente de inmediato cuando se habla de seguridad cibernética, el acceso

[23]. El IIA, *Auditoría de Respuesta y Recuperación de Incidentes Cibernéticos*, Orientación Suplementaria, Guía de Práctica, https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf .

no autorizado a discos duros o servidores donde se almacena información confidencial fue responsable del 10 % de todas las infracciones maliciosas en 2020, lo que costó a las organizaciones un promedio de $4,36 millones por infracción, según una investigación . del Ponemon Institute publicado por IBM Security.

Dicha infraestructura puede incluir salas de servidores seguras con acceso restringido, así como medidas de seguridad más básicas, como puertas cerradas con llave en todas las instalaciones. Si bien la seguridad de la infraestructura es importante, contar con controles para detectar y documentar actividades potencialmente sospechosas puede ser más relevante.

“Cuando hablo de infraestructura física, no me refiero tanto a puertas cerradas como a asegurarme de que haya notificación y documentación de la acción que crea el riesgo real. Es como el plato principal de la comida en lugar del aperitivo”, dijo Tremblay.

Identificar y brindar seguridad para tales sistemas cae directamente dentro de los conjuntos de habilidades establecidos de la auditoría interna, dijo Ross, y agregó: “La auditoría interna tiene la capacidad de identificar los sistemas que son de mayor riesgo o críticos para el sustento de la organización. De hecho, es probable que la auditoría interna ya tenga estos sistemas identificados como parte de la garantía del cumplimiento de las leyes y regulaciones federales relacionadas con otros riesgos. Todo lo que se necesita es expandir ese pensamiento para incluir nuevos tipos de aprovisionamiento que puedan ofrecer un acceso elevado”.

Alineación de las expectativas de recuperación

La documentación efectiva en todas las etapas de un plan de respuesta a incidentes cibernéticos es fundamental. Sin embargo, igualmente crítica es la comunicación de los datos que proporciona dicha documentación y la alineación de las expectativas de detección y recuperación de la organización.

Según Tremblay, esta es una de las brechas más grandes que ha visto en los planes de respuesta cibernética de las organizaciones, y donde la auditoría interna puede brindar el mayor valor. “El papel de la auditoría interna en la recuperación ante desastres cibernéticos es doble”, dijo. “Primero, asegúrese de que el incidente exista, y puede probar que existe a través de la documentación o cualquier tecnología o proceso que utilice. Lo segundo, y lo que no veo que se haga lo suficiente, es sentarse con todas los participantes clave [para determinar] cuál será el cronograma de recuperación realista basado en el apetito por el riesgo de la organización”.

El cronograma, dijo Tremblay, lo establecerá el 'propietario' de la aplicación en cuestión en la organización, que podría ser el CISO, el jefe de la cadena de suministro o cualquier otro líder, dependiendo de dónde ocurra el incidente. La clave para la auditoría interna es funcionar como enlace entre esa parte y todas las demás partes que dependen de esa aplicación para las funciones diarias.

“Por ejemplo, el CISO puede decir que un tiempo de recuperación de 48 horas es aceptable, pero si no acude al CFO u otros líderes o funciones que confían en que la tecnología esté en funcionamiento y obtenga su opinión, está configurando prepárate para un desastre potencial”, dijo Tremblay. “Por ejemplo, el CFO puede decir que 48 horas está bien, pero solo si no estamos cerrando los libros. Pero si estamos cerrando los libros, no es aceptable ningún tiempo de inactividad porque la organización tendría que presentar una extensión, lo que se vería muy mal en los mercados públicos”.

Dichas conversaciones no requieren necesariamente que una de las partes anule a la otra. Más bien, a través de dicha comunicación, la auditoría interna puede negociar el consenso de acuerdo con el apetito por el riesgo de la organización. “En los casos en los que existen discrepancias”, dijo Tremblay, “lo que [la auditoría] interna puede preguntar es: '¿Realmente vale la pena que eso suceda?' El CEO podría decir: 'Sí, lo es, porque va a costar un millón de dólares resolver ese problema'. Lo que realmente estamos haciendo es asegurarnos de que el plan se haya desarrollado realmente en torno a las partes interesadas en torno a la tecnología”.

Continúa: “Creo que esta es un área en la que nosotros, como profesión, no hemos sido especialmente buenos. Creo que tratamos de marcar la casilla para validar ciertas cosas sin realmente decir: 'Oye, como parte de la revisión de los controles

en torno a la respuesta a incidentes, identificamos una brecha en los requisitos entre las partes interesadas de tecnologías particulares'. Eso es muy válido. Eso es identificar un riesgo comercial no identificado previamente que es valioso para la organización".

Funcionalidad cruzada

Es un error común pensar que la propiedad principal de la respuesta de ciberseguridad recae en el CISO y el equipo de seguridad. Esto sólo es parcialmente cierto. Si bien la experiencia y los conocimientos necesarios para implementar los aspectos más técnicos de una estrategia cibernética probablemente se encontrarán en ese departamento, es peligroso suponer que el departamento tendrá el ancho de banda, o el deseo, de asumir la carga por su cuenta.

"La respuesta a incidentes cibernéticos es, al menos debería ser, un proceso multifuncional", dijo Ross. "La principal razón del retraso en los tiempos de respuesta de la organización que veo no es el departamento de seguridad de la información en sí mismo en términos de conocimiento, sino el establecimiento de roles y responsabilidades interfuncionales con departamentos donde la seguridad no es su responsabilidad principal. Tienen otras cosas que hacer.

Según Ross, corregir este concepto erróneo y fomentar la idea de responsabilidad compartida entre todas las partes interesadas debería ser un área clave del enfoque de auditoría interna. "El énfasis no necesariamente debe estar en el equipo de seguridad y lo que están haciendo, sino más bien en cómo su proceso está siendo respaldado por otras entidades de la empresa que tienen un interés en él. El equipo de seguridad sabe qué hacer, pero no puede obligar a los equipos de TI y los desarrolladores de back-end a ayudar de manera crítica. Hay mucha política organizacional involucrada, y cuando estaba en esa posición, encontré un socio valioso en auditoría interna. Los equipos de seguridad no pueden pelear esas batallas solos. Si puede conseguir una parte algo neutral para ayudar a identificar dónde la organización tiene lagunas en el proceso, ayuda a todos".

Una estrategia útil para resaltar estas brechas y aclarar roles, dijo Ross, es que la auditoría interna, generalmente en colaboración con un consultor externo, facilite simulaciones de escritorio. "Una vez que tenga su plan de respuesta a incidentes cibernéticos en un lugar donde se pueda probar, una simulación de escritorio reúne al CIO, CISO, líderes de TI, el CEO, auditoría interna, todas las partes interesadas aplicables, juntos en una sala de conferencias o llamada de Zoom para recorrer un escenario plausible. Incluso sin experiencia técnica, la auditoría interna puede facilitar la discusión preguntando quién hace qué y evaluando cómo esas responsabilidades se alinean con la realidad. Podrían decir: 'En este punto, su equipo debería estar ejecutando X e Y de acuerdo con nuestro plan, pero en realidad, podría estar haciendo Z'. Ahí es cuando vas a escuchar la verdadera suciedad. La mayoría de las organizaciones tienen que hacerlas al menos una vez al año, pero la auditoría interna realmente debería hacerse cargo de ellas".

Conclusión

Evolucionando con el entorno de riesgo

La auditoría interna, debido a su lugar único en la organización, merece un asiento en la mesa cuando se trata de los planes de respuesta a incidentes cibernéticos de una organización. Pero este éxito no excusa a la auditoría interna de esforzarse por una exploración y comprensión más profundas de la ciberseguridad. De hecho, en un futuro que está prescindiendo rápidamente de la infraestructura física a favor de la tecnología basada en la nube, inevitablemente será necesaria y esperada una mayor experiencia de la auditoría interna.

“Cuando comencé mi carrera en auditoría interna, uno de los mejores puntos de venta fue que era un rol muy generalista”, dijo Tremblay. “Tienes que ver y aprender mucho sobre las cosas en las que no tienes que ser un experto. Pero ha habido un cambio tan masivo en torno a la tecnología que estoy empezando a preguntarme si los días del auditor interno generalista están contados. En cambio, tal vez la auditoría interna algún día se convierta en un experto en la materia (SME) en torno a cosas que son inherentemente críticas para las organizaciones. Entonces, en lugar de tener equipos de auditoría compuestos por 8-10 auditores operativos, de cumplimiento y de estados financieros, las organizaciones tendrán un auditor de ciberseguridad, un auditor de ESG, etc.

Ross está de acuerdo. “En cierto punto con la tecnología emergente, ¿cómo realmente entiendes las brechas en el proceso de respuesta a un nivel profundo si no puedes profundizar tanto? En realidad, nunca lo harías.

Es mucho lo que se puede lograr con el conocimiento y los recursos disponibles, pero se avecina un futuro emocionante y radicalmente nuevo. La auditoría interna debe ser parte de ella.

Números anteriores

Para acceder a números anteriores de Perspectivas y Percepciones Globales, visite www.theiia.org/GPI .

Comentarios del lector

Envíe sus preguntas o comentarios a globalperspectives@theiia.org .

Sobre el IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional que atiende a más de 215 000 miembros globales y ha otorgado 180 000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Establecido en 1941, el IIA es reconocido como el líder de la profesión de auditoría interna en estándares, certificación, educación, investigación y orientación técnica en todo el mundo. Para obtener más información, visite theiia.org .

Descargo de responsabilidad

El IIA publica este documento con fines informativos y educativos. Este material no pretende proporcionar respuestas definitivas a circunstancias individuales específicas y, como tal, solo pretende ser utilizado como guía. El IIA recomienda buscar el asesoramiento de expertos independientes relacionado directamente con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Copyright

Agosto 2022

La traducción al español de este documento fue autorizada por The Institute of Internal Auditors, Inc. y fue realizada por la Fundación Latinoamericana de Auditores Internos – FLAI.

Traductora: Andrea Correa (servicios contratados), revisor: Roberto Loo, control de calidad.

Traducción al Español Auspiciada por:

FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101