MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS

OEA

Más derechos para más gente

INTERNET SECURITY ALLIANCE

MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS

OEA

Más derechos para más gente

INTERNET SECURITY ALLIANCE

¿POR QUÉ UN MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS?

Los ciberataques son las amenazas de más rápido crecimiento, y quizás los más peligrosos, que enfrentan las organizaciones actuales. Varios informes han demostrado que la revolución digital está afectando a América Latina más que quizás a cualquier región del mundo. Si bien esta revolución ofrece esperanzas de mejoras económicas y sociales impactantes para América Latina, también conlleva un riesgo sustancial. Según un estudio del Instituto SWIFT, "las redes de Internet de banda ancha y móviles 3G y 4G se han extendido por toda América Latina, lo que les permite a los empresarios aprovechar la tecnología para atraer nuevos clientes al sistema financiero global. Sin embargo, también ha provocado un rápido crecimiento de la ciberdelincuencia, ya que los piratas informáticos aprovechan las débiles defensas cibernéticas, las malas prácticas de higiene cibernética, las limitadas capacidades de aplicación de la ley y la mala gobernanza de la ciberseguridad."[1]

Las juntas directivas deben asumir un papel de liderazgo en la supervisión de la seguridad de los sistemas cibernéticos de su empresa. Sin embargo, un estudio reciente de la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo encontró que las juntas corporativas en América Latina en general tienen niveles de madurez bajos o medios relacionados con la ciberseguridad, y la mayoría de las juntas tienen solo un conocimiento "formativo" de la ciberseguridad[2]. En consecuencia, es posible que no sean conscientes de cómo pueden las amenazas cibernéticas afectar específicamente a sus organizaciones. Sin embargo, debido a la naturaleza siempre cambiante de la amenaza, las juntas están buscando un enfoque coherente para abordar el problema a nivel de la junta. Para responder a esto, el Internet Security Alliance (ISA) y la Asociación Nacional de Directores Corporativos (NACD, por sus siglas en inglés) crearon el primer Manual de Supervisión de Riesgo Cibernético para las Juntas Corporativas en 2014. El manual fue un éxito inmediato en la ayuda a las juntas para abordar el riesgo cibernético a escala global. De hecho, PricewaterhouseCoopers, en su Encuesta Global de Seguridad de la Información, hizo referencia al manual por su nombre e informó que:

"Las pautas de la Asociación Nacional de Directores Corporativos (NACD) aconsejan que las juntas vean los riesgos cibernéticos considerando toda la empresa y comprendan los posibles impactos legales. "Deben analizar, conjuntamente con la gerencia, los riesgos de ciberseguridad y la preparación y tener en cuenta las amenazas cibernéticas en el contexto de la tolerancia general al riesgo de la organización".

"Los encuestados dijeron que esta participación más profunda por parte de la junta ha ayudado a mejorar las prácticas de ciberseguridad de muchas maneras. No puede ser una coincidencia que, ante la mayor participación de las juntas en los debates presupuestarios de ciberseguridad, hubo un aumento del 24% en el gasto en seguridad."

"Otros resultados notables mencionados por los encuestados incluyen la identificación de riesgos clave, el fomento de una cultura organizacional de seguridad y una mejor alineación de la ciberseguridad con la gestión general de riesgos y los objetivos comerciales. "Más que nada, la participación de la junta ha abierto las líneas de comunicación entre ejecutivos y directores que tratan la ciberseguridad como si fuera un problema económico".

Si bien son generalizables tanto muchos elementos del gobierno corporativo, en general, como la supervisión del riesgo cibernético, en particular, también existen características únicas que se aplican a países y regiones específicos. La Organización de los Estados Americanos (OEA) y la ISA están trabajando para aprovechar el éxito comprobado del manual original de riesgo cibernético y adaptarlo a las necesidades únicas de la región de América Latina. Esta publicación es el resultado de un proceso de múltiples etapas en el que están comprometidos la OEA e ISA con cientos de partes interesadas de juntas corporativas, la academia, el gobierno y alta gerencia en toda la región en un esfuerzo por ayudar a las organizaciones a protegerse de las amenazas cibernéticas.

MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS

CONTENIDO

01 | **Agradecimientos** 5

02 | **Introducción** 7

03 | **Principio 1**
Los directores deben comprender y abordar la ciberseguridad como un problema de gestión de riesgos en toda la empresa, no solo como un problema de TI. 12

04 | **Principio 2**
Los directores deben entender las implicaciones legales de los riesgos cibernéticos según se relacionan con las circunstancias específicas de su empresa. 15

05 | **Principio 3**
Las juntas deben tener un acceso adecuado a la experiencia en ciberseguridad y se le debe proporcionar un tiempo regular y adecuado a las discusiones sobre la gestión de riesgos cibernéticos en las agendas de las reuniones de la junta. 18

06 | **Principio 4**
Los directores de la junta deben establecer la expectativa de que la gerencia establecerá un marco de gestión de riesgo cibernético para toda la empresa con personal y presupuesto adecuados. 21

07 | **Principio 5**
La discusión de la junta directiva sobre el riesgo cibernético debe incluir la identificación de qué riesgos evitar, cuáles aceptar y cuáles mitigar o transferir a través de un seguro, así como planes específicos asociados con cada abordaje. 24

08 | **Apéndice A**
Evaluación de la cultura de ciberseguridad de la junta 26

09 | **Apéndice B**
Preguntas fundamentales que los directores deberían preguntarse acerca de la ciberseguridad 28

10 | **Apéndice C**
Preguntas que le puede hacer la junta a la gerencia sobre la ciberseguridad relacionadas con el conocimiento de la situación 29

11 | **Apéndice D**
Preguntas que le puede hacer la junta a la gerencia sobre estrategia y operaciones 30

12 | **Apéndice E**
Preguntas que le puede hacer la junta a la gerencia sobre la ciberseguridad relacionadas con amenazas internas 31

13 | **Apéndice F**
Preguntas que le puede hacer la junta a la gerencia sobre la ciberseguridad relacionadas con la cadena de suministro 32

14 | **Apéndice G**
Preguntas que le puede hacer la junta a la gerencia sobre la planificación de un posible incidente, manejo de crisis y respuesta 33

15 | **Apéndice H**
Consideraciones de ciberseguridad durante las fases de fusiones y adquisiciones 35

16 | **Apéndice I**
Métricas de ciberseguridad a nivel de junta 39

17 | **Apéndice J**
Construcción de una relación con la gestión de la ciberseguridad y el equipo de seguridad 42

AGRADECIMIENTOS

Les agradecemos a los siguientes profesionales sus contribuciones al desarrollo de este Manual, en su participación en reuniones de proyectos, talleres, teleconferencias y creación de contenido.

La versión estadounidense del Manual de 2017 fue revisado según sus aportes colectivos, siguiendo un proceso de consenso, y no refleja necesariamente las opiniones de las empresas y organizaciones detalladas.

Organización de los Estados Americanos (OEA)

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Miguel Ángel Cañada

Internet Security Alliance Board of Directors

INTERNET SECURITY ALLIANCE - Larry Clinton
INTERNET SECURITY ALLIANCE - Josh Higgins
USAA - Gary McAlum
LEIDOS - JR Williamson
AIG - Tracie Grella
RAYTHEON - Jeff Brown
BNY MELLON - Adrian Peters
LOCKHEED MARTIN CORPORATION - Jim Connelly
UNISYS CORPORATION - Jonathan Goldberger
VODAFONE - Richard Spearman
ERNST AND YOUNG - Andrew Cotton CARNEGIE
MELLON UNIVERSITY - Tim McNulty SECURE
SYSTEMS INNOVATION CORPORATION - John Frazzini
NORTHROP GRUMMAN - Mike Papay
CENTENE - Lou DeSorbo
SYNCHRONY FINANCIAL - Matt Fleming
DIRECT COMPUTER RESOURCES - Joe Buonomo
NATIONAL ASSOCIATION OF MANUFACTURERS - Robyn Boerstling
BUNGE LIMITED - Robert Zandoli
FIS - Greg Montana
SAP - Tim McKnight
RSA - Shawn Edwards
MUFG UNION BANK, N.A. - Lisa Humbert GENERAL
ELECTRIC - Nasrin Rezai
STARBUCKS - Dave Estlick
CENTER FOR AUDIT QUALITY - Catherine Ide
THOMSON REUTERS - Richard Puckett

Contribuyentes

DELOITTE - Santiago Gutierrez
PINKERTON - Edith Flores
SECRETARIA DE RELACIONES EXTERIORES - Valeria Solis
CISCO - Gilberto Vicente
AIG - Ricardo Millan
BANBAJIO - Barbara Mair
HUAWEI TECHNOLOGIES - Francisco Cabrera
CENAGAS - Luis Lopez
HONEYWELL - Nahim Dias S.
CENTRO MEDICO ABC - Mary O'Keefe
GRUPO INDUSTRIAL SALTILLO - Lorena Cardenas HP - Aiza Romero Maza
ESTUDIOS Y ASESORIAS SCASOCIADOS LTDA - Cecilia Gutierrez
MINISTERIO DEL INTERIOR - Catherine Narvaez
SUBSECRETARIA DE TELECOMUNICACIONES (SUBTEL) - Jozsef Markovitz
DERECHOS DIGITALES - Pablo Viollier
CIBERSEGURIDAD HUMANA - Cristian Bravo Lillo
BANCO DE CREDITO E INVERSIONES, BCI - Lionel Olavarria Leyton
TRICOT - Susana Carey
MICROSOFT CHILE - Alex Pesso
DREAMLAB TECHNOLOGIES - Gabriel Bergel
CLEVERIT - Diego Stevens
ENTEL - Antonio Moreno Cano
MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA - Hernan Espinoza
SUBSECRETARIA DEL INTERIOR - Juan Pablo Gonzalez Gutierrez
SONDA - Juan Ernesto Landaeta
UNIVERSIDAD DE LOS ANDES - Pedro Anguita Ramirez
EY - Marcelo Zanotti
TECHNOLOGICAL UNIVERSITY OF CHILE - Karin Quiroga
ACTI - Jaime Pacheco
UNIVERSIDAD DE CHILE - Alejandro Hevia
REDBANC S.A. - Carolina Flisfisch
GLOBALSECURE - Manuel Moreno
FISCALIA PRIVADA - Gonzalo Errazuriz
SOLUCIONES ORION - Andres Cargill
RETAIL FINANCIERO AG - Claudio Ortiz T.
VINSON CONSULTING - TRANSBANK, REDBANK,

NEXUS - Alvaro Alliende
GACOF CONSULTING - Orlando Garces
CANCILLERIA - Diana Carolina Kecan Cervantes
CCIT - Juan Alcazar
ITM COLOMBIA - Armando Cuervo Vanegas
PRESIDENCIA - Martha Sanchez
HEINSOHN - Adriana Lucia Rios Sanchez
CORREO POLICIA - Alex Duran
ASO BANCARIA - Sandra Galvis
MINSAIT - Hernando Diaz Bello
ASO BANCARIA - Daniel Absalon Tocaria Diaz
CORREO POLICIA - Alvaro Rios
MINMINAS - Oscar Sanchez Sanchez
OPENLINK - Leonardo Rincon Romero
MINTRABAJO - Nidia Nayibe Gonzalez Pinzon
FONCEP - Hector Pedraza
MIN JUSTICIA - Adriana Aranguren
DAVIVIENDA - Fabian Ramirez
ESDEGUE - Jairo Becerra
MINTIC - Fabiana Garcia
ESDEGUE - Gladys Elena Medina Ochoa
TIGOUNE - Laura Botero
O4IT -Diana Carolina Echeverria Rojas
MGM INGENIERIA - Julian E. Morales Ortega
FIDUCOLDEX - Mabel Leonor Orjuela G.
SONDA - Carlos Bastidas
TIGOUNE - Alejandra Otalora
UROSARIO - Valerie Gauthier
CRCOM - Leidy Diana Rojas Garzon
COLCERT - Wilson Arturo Prieto H.
FOGAFIN - Edgar Yesid Garay Medin
COINTERNET - Gonzalo Romero
METRAIT - Juan Delgado
CRCOM - Felipe Sarmiento
DNP - Sandra Fernanda Poveda Avila
CCB - Jaime Gonzalez
TELEFONICA - Angela Maria Pava Orozco
GEC RISK ADVISORY - Andrea Bonime-Blanc
Graciela Braga
NYU and NJIT - Arnold Felberbaum
Passworld Technical College -Jeffrey Davis Jusino
Sonda - Marcos Gutierrez
Banco Central de Chile - Atilio Mashii
Banco del Austro - Fernando Aguilar Ochoa
Claro Colombia - Juan David Valderrama Silva
Instituto Federal de Telecomunicaciones - Cynthia Daniela Alvarez
Gerente TI - Giovanni Pachon
Ing.- Miguel Gaspar
Langtech - Luis Alfonso Nunez Gutierrez
Superintendencia de Bancos - Daniel Monzon
Lic. En Sistemas - Carin Molina
TTCSIRT - Angus Smith

INTRODUCCIÓN

El aumento del uso de Internet en América Latina está ocurriendo a una de las tasas más altas del mundo[3]. Consecuentemente, ha habido una digitalización del riesgo corporativo. En los últimos años, ha sido tan dramático el cambio del valor de los activos corporativos que ahora casi el 90% de los activos corporativos son digitales. Como resultado, los responsables de las políticas, los reguladores, los accionistas y el público están más conscientes que nunca de los riesgos corporativos de ciberseguridad. Las organizaciones corren riesgos de pérdida de propiedad intelectual y sus planes comerciales, destrucción o alteración de datos, disminución de la confianza pública e interna de las partes interesadas, interrupción de la infraestructura crítica y evolución de las sanciones reglamentarias. Cada uno de estos riesgos puede afectar negativamente las posiciones competitivas, el precio de las acciones y el valor para los accionistas.

Las compañías líderes perciben los riesgos cibernéticos de la misma manera como lo hacen con otros riesgos críticos: en términos de compensación de riesgo-recompensa. Esto es especialmente desafiante en el dominio cibernético por dos razones. Primero, la complejidad y persistencia de las amenazas cibernéticas ha crecido dramáticamente. Las corporaciones, incluso las empresas que son comparativamente pequeñas, ahora enfrentan eventos cada vez más sofisticados que logran sobrepasar las defensas tradicionales. Con el aumento de la complejidad de estos ataques, también aumenta el riesgo que representan para las organizaciones. Los efectos potenciales de una violación de los datos se están extendiendo mucho más allá de la pérdida, modificación o interrupción de la información. Los ataques cibernéticos pueden tener un impacto desastroso en la reputación y marca de una organización. Las empresas y los directores también pueden incurrir en riesgos legales y financieros derivados de los ciberataques[4].

A pesar de estos riesgos, la motivación para implementar tecnologías nuevas y emergentes para impulsar el desarrollo económico, reducir los costos, mejorar el servicio al cliente y estimular la innovación es más fuerte que nunca. A medida que crecen las amenazas de ciberseguridad, las Juntas Corporativas pueden ser proactivas en materia de ciberseguridad y dedicarse a realizar evaluaciones de riesgos y mantener un diálogo regular con la alta administración en toda la organización. Si no se abordan estas vulnerabilidades, los ciberdelincuentes pueden chantajear a las organizaciones con amenazas de divulgar información sobre sus vulnerabilidades, riesgos y secretos competitivos. Para las organizaciones, hay muchos otros beneficios de implementar medidas de ciberseguridad más robustas que la simple protección contra ataques. Estos incluyen:

- Ventaja competitiva sobre compañías que tienen una seguridad menos sólida;
- Mejora de la eficacia en función de los costos, mediante protocolos eficaces de gestión de riesgos;
- Preservación de la reputación de la empresa;
- Contribución para mantener la integridad de la infraestructura general y proteger la confianza de los consumidores y de las partes interesadas internas;
- Demostración directa de la responsabilidad corporativa hacia todas las partes interesadas potencialmente afectadas, más allá de los clientes: empleados, accionistas, proveedores y la comunidad.

El Foro Económico Mundial informa que el rápido ritmo de la innovación y la conectividad de la red continuará aumentando en los próximos años, lo que hace que sea aún más crítico que se tomen medidas a nivel de la junta directiva en materia de ciberseguridad[5].

Estas presiones competitivas hacen que la supervisión concienzuda y exhaustiva a nivel de junta sea esencial. Las juntas deberán reconocer que la gestión y mitigación del impacto del riesgo cibernético requiere un pensamiento estratégico que abarque más allá del departamento de TI. Un estudio de la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo recomienda que, como mínimo, las juntas comprendan los riesgos cibernéticos a los que se enfrentan sus empresas, los principales métodos de ataque que podrían emplearse en su contra, y cómo su empresa gestiona y evalúa los problemas cibernéticos[6].

Un panorama de amenazas cibernéticas que evoluciona rápidamente: ¿Cuál es la responsabilidad de la junta?

Hace tan solo unos años, los ataques cibernéticos se debían, en gran medida, a hackers y algunas personas altamente sofisticadas. Aún siendo problemáticos, muchas corporaciones podrían tildar estos eventos como simplemente un costo frustrante de hacer negocios.

Hoy en día, las corporaciones están asediadas por atacantes que forman parte de equipos ultra sofisticados que implementan malware cada vez más dirigido contra sistemas y personas, atacando de manera furtiva en múltiples etapas. Estos ataques, a veces denominados amenazas persistentes avanzadas (APT, por sus siglas en inglés), se lanzaron por primera vez contra entidades gubernamentales y contratistas de defensa. Más recientemente, han migrado a toda la economía, lo que significa que prácticamente cualquier organización está en riesgo.

Una de las características determinantes de estos ataques es que pueden penetrar en prácticamente todos los sistemas de defensa perimetral de una empresa, como los cortafuegos o los sistemas de detección de intrusos. Se calculan meticulosamente estos ataques para asaltar a un objetivo específico, y los intrusos buscan múltiples vías para explotar las vulnerabilidades en todas las capas de seguridad hasta lograr sus objetivos. La realidad es que si un atacante sofisticado tiene en la mira los sistemas de una compañía, casi con seguridad los violará. Esto no significa que la seguridad sea un imposible, solo significa que la ciberseguridad debe ser más que simplemente la seguridad perimetral basada en TI. Dado que los ataques se han vuelto más sofisticados, las defensas deben volverse más sofisticadas. **No es responsabilidad de la junta convertirse en expertos en TI, pero la junta debe saber qué preguntas hacerles a los departamentos de TI. Además, las juntas deben ejercer el liderazgo y el compromiso necesarios, supervisando de forma proactiva y responsabilizando a la gerencia y al grupo de la alta gerencia responsable, de lograr que la protección de la organización contra el ciberataque sea una prioridad**[7].

No solo deben ser protegidos los sistemas de TI. Los empleados, subcontratistas y trabajadores, ya sea que estén descontentos o simplemente mal entrenados, presentan una exposición al menos tan grande para las compañías como los ataques desde el exterior. Esto evidencia la necesidad de contar con un programa de seguridad sólido y adaptable, igualmente equilibrado para enfrentar las amenazas informáticas internas y externas. La gerencia debe asegurarle a la junta que los sistemas de TI están recibiendo una protección básica y que todo el ecosistema cibernético está protegido. Las organizaciones no podrán lidiar con amenazas avanzadas si no están en capacidad de detener ataques de gama baja. Y deben hacerlo de manera continua y persistente, porque la amenaza cibernética nunca desaparecerá[8].

Mayor conectividad, mayor riesgo

La creciente naturaleza interconectada de los sistemas de información tradicionales y los sistemas no tradicionales como dispositivos móviles, cámaras de seguridad, copiadoras, plataformas de videojuegos y automóviles, que se

ha denominado el Internet de las Cosas (IoT, por sus siglas en inglés), ha dado lugar a un gran aumento en el número de posibles puntos de entrada para los atacantes cibernéticos. Por lo tanto, es crítica la necesidad de que las organizaciones amplíen su manera de pensar sobre el riesgo cibernético,

Los atacantes cibernéticos intentan habitualmente robar todo tipo de datos, incluida la información personal de los clientes y empleados, datos financieros, planes de negocios, secretos comerciales e IP. Por ejemplo, en febrero de 2019, Blind Eagle, un grupo de piratería de amenazas persistentes avanzadas, se hizo pasar por policía cibernética de Colombia en un esfuerzo por robar secretos comerciales de sus organizaciones objetivo[9] Cada vez más, los atacantes cibernéticos están empleando tácticas que cifran los datos de una organización, en las que secuestran los datos hasta que se hace un pago por el descifrado, llamado "ransomware".

Un ejemplo: WannaCry

¿Qué fue WannaCry?
WannaCry fue un ciberataque mundial dirigido a equipos que ejecutaban Microsoft Windows mediante el cifrado de datos y la exigencia de pagos en la criptomoneda de Bitcoin. WannaCry fue una forma de ataque ransomware. El ataque tuvo lugar el 12 de mayo de 2017, comenzando en Asia y se extendió por más de 230,000 computadoras en más de 150 países. México fue el quinto país más afectado por el ciberataque[1].

¿Qué impacto tuvo WannaCry?
Una de las organizaciones más grandes afectadas por el ataque de WannaCry fue el Servicio Nacional de Salud (NHS, por sus siglas en inglés) del Reino Unido. El malware infectó unos 70,000 dispositivos, entre las que se incluían computadoras, escáneres de MRI y refrigeradores de almacenamiento de sangre, que tuvo como consecuencia una interrupción significativa de los servicios del NHS[1]. Nissan Motor Manufacturing detuvo la producción en una de sus instalaciones como resultado de las infecciones de WannaCry y también se vieron afectadas importantes organizaciones como FedEx[1]. Las pérdidas económicas del ataque en todo el mundo se han estimado en $ 4 mil millones[1].

Debido a la inmensa cantidad de conexiones a sistemas de datos externos, ya no resulta adecuado que las organizaciones protejan solo "su" red. Los vendedores, proveedores, socios, clientes o cualquier entidad relacionada con la empresa de manera electrónica pueden convertirse en un punto potencial de vulnerabilidad. Por ejemplo, los sistemas de una importante compañía petrolera fueron violados cuando un atacante sofisticado que no pudo penetrar en la red decidió insertar malware en el menú en línea de un restaurante local muy frecuentado por los empleados. Cuando los empleados utilizaron el menú en línea, concedieron involuntariamente el acceso al sistema corporativo a los delincuentes. Una vez adentro del sistema de la compañía, los intrusos pudieron atacar su negocio principal[10].

Amenazas cibernéticas en cifras

- Estimar el daño de los ataques cibernéticos es difícil, pero algunos lo estiman en $ 400-500 mil millones o más anualmente, en la que no se detecta una parte significativa de los costos[11]. Los costos de la ciberdelincuencia se quintuplicaron entre 2013 y 2015 y podrían alcanzar los $ 2 billones por año para 2019[12].

- La ciberseguridad se encuentra entre los principales riesgos para los mercados de América Latina, según una encuesta de profesionales que trabajan, o no, en el campo de riesgos[13].

- Brasil, Argentina y México ocupan el tercer, octavo y décimo lugar, respectivamente, en los rankings globales de países de origen para los ciberataques[14].

- Los ataques de ransomware en América Latina aumentaron un 131% en el último año[15]. México y Brasil ocupan el séptimo y octavo lugar en el mundo por ocurrencia de la mayoría de los ataques de ransomware[16].

- El 34% de todo el fraude por originación de nuevas cuentas proviene de América del Sur[17].

- El 80 por ciento de los ciberataques se deben al crimen organizado[18].

- La mediana de días transcurridos entre el momento en que una organización está comprometida y que se descubre la violación cibernética es 146[19]. El 53 por ciento de los ataques cibernéticos son identificados primero por terceros (por ejemplo, agentes de la ley o socios corporativos), y solo el 47 por ciento se descubre internamente[20].

• El 48 por ciento de los profesionales de seguridad de TI no inspeccionan la nube en busca de malware, a pesar del hecho de que el 49 por ciento de todas las aplicaciones empresariales ahora están almacenadas en la nube. De esas aplicaciones basadas en la nube, el departamento de TI conoce, sanciona o aprueba menos de la mitad[21].

• El 38 por ciento de las organizaciones de TI no tienen un proceso definido para revisar sus planes de respuesta a la violación cibernética, y casi un tercio no ha revisado ni actualizado sus planes desde su desarrollo inicial[22].

Empresa más pequeña, mayor riesgo

Aunque muchas empresas pequeñas y medianas han creído históricamente que son demasiado insignificantes para ser un blanco, esa percepción es errónea. De hecho, la mayoría de las pequeñas y medianas empresas han sido víctimas de ataques cibernéticos. Un estudio de la OEA-Symantec reveló que las pequeñas y medianas empresas (PYME) se están convirtiendo en un área de amenaza importante, en la que está creciendo rápidamente el número de incidentes entre las PYME[23]. El estudio identificó el ransomware Cryptolocker como una amenaza que, cada vez más, tiene en su mira a las PYME. También se están librando, en términos generales, ataques de malware que utiliza un cifrado de seguridad complejo contra las PYME[24]. Además de ser objetivos, las empresas más pequeñas suelen ser una ruta de ataque hacia organizaciones más grandes a través de sus relaciones con clientes, proveedores o empresas conjuntas, lo que hace que la administración de proveedores y socios sea una función crítica para todas las entidades interconectadas.

Existe un consenso general, en el campo de la ciberseguridad, de que los atacantes cibernéticos le llevan una gran delantera a las corporaciones que deben defenderse contra ellos.

Esto no significa que la defensa sea imposible, pero sí significa que los miembros de la junta directiva deberán asegurarse de que la gerencia está completamente comprometida en hacer que los sistemas de la organización sean tan resistentes como económicamente factibles. Esto incluye el desarrollo de planes de defensa y respuesta que sean capaces de afrontar métodos sofisticados de ataque. Si bien los programas complejos de ciberseguridad pueden ser difíciles de implementar dentro de organizaciones más pequeñas que están limitadas por la disponibilidad de recursos, todas las organizaciones deberían poder implementar los cinco principios centrales presentados en este manual.

¿Por qué nos atacarían?

Algunas organizaciones creen que es poco probable que sean víctimas de un ataque cibernético porque son de tamaño relativamente pequeño, no son una marca conocida y/o no tienen cantidades sustanciales de datos confidenciales del consumidor, como números de tarjetas de crédito o información médica.

De hecho, los adversarios tienen en la mira a organizaciones de todos los tamaños y de todas las industrias, buscando cualquier cosa que pueda ser de valor, incluidos los siguientes activos:

• Planes de negocios, incluidas las fusiones o estrategias de adquisición, ofertas, etc.;

• Algoritmos de negociación;

• Contratos o acuerdos propuestos con clientes, proveedores, distribuidores, socios de empresas conjuntas, etc.;

• Credenciales de inicio de sesión de los empleados y otra información útil;

• Información sobre las instalaciones, incluidos los diseños de plantas y equipos, mapas de construcción y planes futuros;

• Información de I + D, incluidos nuevos productos o servicios en desarrollo;

• Información sobre procesos de negocio clave;

• Código fuente;

• Listas de empleados, clientes, contratistas y proveedores;

• Datos del cliente, donante o fiduciario.

Fuente: *Internet Security Alliance*

Equilibrar la ciberseguridad con la rentabilidad

Luis Alberto Moreno, presidente del Banco Interamericano de Desarrollo, destacó el vínculo central entre la seguridad y el desarrollo económico exitoso en el informe de la OEA-BID: "Si queremos aprovechar al máximo la llamada Cuarta Revolución Industrial, debemos crear no solo una infraestructura digital moderna y robusta, sino también una que sea segura. Proteger a nuestros ciudadanos del delito cibernético no es una mera opción; es un elemento clave para nuestro desarrollo"[25].

Al igual que otros riesgos críticos que enfrentan las organizaciones, la ciberseguridad no puede considerarse de forma aislada. Los miembros de la gerencia y la junta deben lograr el equilibrio adecuado entre proteger la seguridad de una organización y mitigar las pérdidas, al tiempo que continúan asegurando la rentabilidad y el crecimiento en un entorno competitivo.

Muchas innovaciones técnicas y prácticas comerciales que mejoran la rentabilidad también pueden socavar la seguridad. Por ejemplo, muchas tecnologías como la tecnología móvil, la computación en la nube y los dispositivos "inteligentes" pueden generar ahorros significativos en los costos y eficiencias empresariales, pero también pueden crear problemas de seguridad importantes si se implementan incorrectamente. Si se implementan correctamente, podrían aumentar la seguridad.

De manera similar, las tendencias como traiga su propio dispositivo (BYOD, por sus siglas en inglés), el acceso a la información las 24 horas, los 7 días de la semana, el crecimiento de la analítica sofisticada de los "grandes datos" y el uso de largas cadenas de suministro internacionales pueden ser tan rentables que son elementos esenciales para que un negocio siga siendo competitivo. Sin embargo, estas prácticas también pueden debilitar dramáticamente la seguridad de la organización.

Las organizaciones se podrán defender mientras se mantengan competitivas y conserven la rentabilidad. Pero los métodos exitosos de ciberseguridad no pueden simplemente "añadirse" al final de los procesos de negocios. La ciberseguridad debe integrarse en los sistemas y procesos clave de una organización de principio a fin; y cuando se hace bien, puede apoyar en la construcción de una ventaja competitiva. Un estudio encontró que cuatro controles de seguridad básicos eran efectivos para prevenir el 85 por ciento de las intrusiones cibernéticas:

- Restricción de la instalación de aplicaciones por parte del usuario ("lista blanca").
- Asegurarse de que el sistema operativo esté "parchado" con actualizaciones actuales.
- Asegurar que las aplicaciones de software se actualicen regularmente.
- Restricción de los privilegios administrativos (es decir, la capacidad de instalar software o cambiar los ajustes de configuración de una computadora)[26].

El estudio demostró que estas prácticas de seguridad básicas no solo eran efectivas, sino que también mejoraron la eficiencia del negocio y crearon un retorno positivo inmediato de la inversión, incluso antes de considerar el impacto económico positivo de reducir las violaciones cibernéticas[27].

Para ser efectiva, sin embargo, la estrategia cibernética debe ser más que reactiva. Las organizaciones líderes también emplean una postura proactiva y con una de visión de futuro que incluye generar inteligencia sobre el entorno de riesgo cibernético y anticipar dónde podrían arremeter los posibles atacantes. Esto incluye someter sus propios sistemas y procesos a pruebas periódicas y rigurosas para detectar vulnerabilidades.

Los cinco principios para la supervisión efectiva del riesgo cibernético detallados en este manual se presentan en una forma relativamente generalizada para alentar la discusión y la reflexión de las juntas directivas. Naturalmente, los directores adaptarán estas recomendaciones en función de las características únicas de su organización, incluyendo el tamaño, la etapa del ciclo de vida, la estrategia, los planes de negocios, el sector industrial, la huella geográfica, la cultura, los vínculos con las empresas familiares y las inquietudes de las partes interesadas mayoritarias, etc.

PRINCIPIO 1

Las juntas deben comprender y abordar la ciberseguridad como un problema de gestión de riesgos en toda la empresa, no solo como un problema de TI.

Históricamente, las corporaciones han categorizado la seguridad de la información como un problema técnico u operacional que debe ser manejado por el departamento de tecnología de la información (TI). En una encuesta de empresas latinoamericanas, el 42% dijo que sus gestiones de ciberseguridad estaban a cargo del departamento de TI[28]. Esta situación se ve agravada en las estructuras corporativas que dejan que las funciones y unidades de negocios, dentro de la organización, se sientan desconectadas de tener la responsabilidad de la seguridad de sus propios datos. En cambio, esta responsabilidad fundamental se le deja a TI, un departamento que en la mayoría de las organizaciones trabaja con autoridad presupuestaria y recursos limitados. Además, el delegar la responsabilidad de TI inhibe el análisis crítico y la comunicación sobre temas de seguridad y dificulta la implementación de estrategias de seguridad efectivas.

En un ecosistema cada vez más interconectado, cada negocio es un negocio de tecnología donde la TI crea y agrega valor pero, si no cuenta con los recursos adecuados o no se implementa acertadamente, puede restar valor. La mayoría de las empresas invierten mucho en innovación de TI y hacen que las infraestructuras tecnológicas sean cada vez más importantes para la estrategia y las operaciones comerciales en general. Dependiendo de su sector y de los servicios que prestan, algunas empresas dependen más sustancialmente de TI que otras.

Los riesgos cibernéticos deben evaluarse de la misma manera en que una organización evalúa la seguridad física de sus activos humanos y físicos y los riesgos asociados con su posible compromiso. En otras palabras, la ciberseguridad es un problema de gestión de riesgos en toda la empresa que debe abordarse desde una perspectiva estratégica, económica, interdepartamental e interdivisional[29]. No es solo un problema de TI (o de tecnología), sino también de procesos de negocios, personas, datos o información, y valor. Por ejemplo, la ciberseguridad debe incorporarse en los procesos y programas de recursos humanos a través de un enfoque que abarque toda la organización. Además, dado que las juntas en América Latina suelen estar integradas total o parcialmente por miembros de familia, es importante que las familias propietarias de las empresas estén debidamente informadas y sean conscientes de los problemas de ciberseguridad. La OEA y el BID han identificado que un gobierno corporativo maduro, en materia de ciberseguridad, requeriría un compromiso regular por parte de la junta y hacer ajustes rápidos y apropiados de la estrategia de ciberseguridad basados en amenazas y riesgos, así como realizar una asignación efectiva de fondos y atención en toda la organización para abordar las amenazas conocidas y desconocidas. El Foro Económico Mundial también hace hincapié en la necesidad de que las juntas directivas garanticen que la gerencia integre la resiliencia cibernética y la evaluación de riesgos en la estrategia comercial general y la gestión de riesgos en toda la empresa, así como la asignación de recursos y presupuestos.

El riesgo cibernético y el ecosistema empresarial

Algunas de las violaciones de datos más sensibles hasta la fecha han tenido poco que ver con la piratería tradicional. Por ejemplo, un ataque de correo electrónico común dirigido a personas específicas (spear phishing, en inglés) es una de las principales causas de compromiso del sistema. Las estrategias de producto o producción que utilizan cadenas de suministro complejas, abarcando múltiples países y regiones, pueden aumentar el riesgo cibernético. Igualmente, las fusiones y adquisiciones que requieren la integración de sistemas complicados, a menudo en plazos acelerados y sin la debida diligencia, pueden aumentar el riesgo cibernético.

Otro obstáculo al que se enfrentan las empresas en la creación de un sistema seguro es cómo administrar el grado de conectividad que tiene la red corporativa con socios, proveedores, afiliados y clientes. Varias violaciones cibernéticas importantes y bien conocidas no comenzaron realmente dentro de los sistemas de TI del objetivo, sino que resultaron de vulnerabilidades en uno de sus proveedores o vendedores. A continuación, se proporcionan ejemplos de esto en la sección "Mayor conectividad, mayor riesgo", en la página 5 t. Específicamente en América Latina, una gran cantidad de datos confidenciales está culturalmente integrado, ya que muchas organizaciones han desarrollado relaciones familiares con sus proveedores de servicios y, a menudo comparten enormes cantidades de información del consumidor entre proveedores. Además, un número cada vez mayor de organizaciones tienen datos que residen en redes externas o en "nubes" públicas, que ni poseen ni operan y en las que tienen poca capacidad inherente de aseguramiento. Es un error suponer que un proveedor de la nube automáticamente protegerá adecuadamente los datos de una organización. Muchas organizaciones también están conectadas con elementos de la infraestructura crítica nacional, lo que aumenta la posibilidad de que la ciberseguridad en una empresa o institución se convierta en una cuestión de seguridad pública o incluso que afecte la seguridad nacional.

Las juntas directivas deben garantizar que la gerencia evaluará la ciberseguridad no solo en lo que se refiere a las propias redes de la organización, sino también en relación con el ecosistema más grande en el que opera. Las juntas progresivas involucrarán a la gerencia en una discusión sobre los distintos niveles de riesgo que existen en el ecosistema de la compañía y serán responsables de esto a medida que calculan la postura y la tolerancia de riesgo cibernético adecuadas para su propia corporación[30]. Deben prestarles especial atención a las "joyas de la corona" de la organización, los datos altamente confidenciales que la empresa necesita proteger más. La gerencia debe asegurar que la junta tenga una estrategia de protección que se construya a partir de esos objetivos de alto valor. La junta debe indicarle a la gerencia que considere no solo los ataques de mayor probabilidad, sino también los ataques de baja probabilidad y alto impacto que serían catastróficos[31]. El Apéndice "A" proporciona una guía más detallada sobre las preguntas que la junta directiva puede hacerle a la gerencia sobre estos temas.

Responsabilidad de la supervisión del riesgo cibernético a nivel de junta

Un tema para un buen debate es cómo organizar la junta para que gestione la supervisión del riesgo cibernético y el riesgo a nivel de empresa en general. El riesgo cibernético puede mitigarse y minimizarse significativamente si se lo aborda como un problema de gestión de riesgos en toda la empresa. Sin embargo, al igual que con los riesgos tradicionales, los riesgos cibernéticos nunca podrán eliminarse por completo, y las juntas deben comprender la naturaleza del entorno de amenazas de su empresa. La Blue Ribbon Commission de la NACD sobre Gobernanza del Riesgo recomendó que la supervisión del riesgo debería ser una función de toda la junta[32]. Investigaciones de la NACD registran que esto es cierto en la mayoría de las juntas de compañías públicas de EE. UU. que tienen los denominados "riesgos de panorama general" (es decir, riesgos con amplias implicaciones para la dirección estratégica, o debates sobre la interacción entre varios riesgos). Sin embargo, poco más de la mitad de las juntas le asignan la mayoría de las responsabilidades de supervisión de riesgos relacionados con

la ciberseguridad al comité de auditoría, que ya suele estar sobrecargado (Figura 2) y que también asume una responsabilidad importante en la supervisión de la información financiera y los riesgos de cumplimiento.

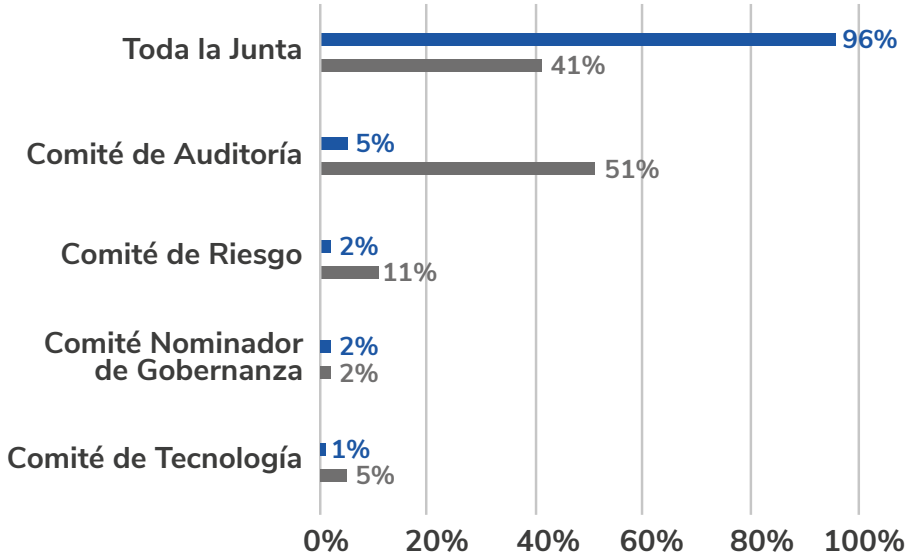
No existe un enfoque único que se ajuste a todas las juntas: algunos eligen llevar a cabo todas las deliberaciones relacionadas con riesgo cibernético a nivel de toda la junta; otros asignan responsabilidades específicas de supervisión relacionadas con la ciberseguridad a uno o más comités (auditoría, riesgo, tecnología, internacional, etc.); y otros utilizan una combinación de los métodos mencionados. El comité de nominación y gobernanza deberá garantizar que el abordaje elegido por la junta directiva está claramente definido en los estatutos del comité para evitar confusiones o duplicación de esfuerzos. Prácticamente todas las decisiones comerciales importantes, incluidas las fusiones/adquisiciones, el desarrollo de nuevos productos, especialmente aquellos que involucran problemas y oportunidades de transformación digital, y las alianzas estratégicas tienen importantes implicaciones de ciberseguridad. Por lo tanto, la ciberseguridad deberá integrarse en los análisis de negocios de la misma forma en que se integran las cuestiones legales y financieras en prácticamente todas las discusiones de negocios importantes. Se debe informar a toda la junta sobre asuntos de ciberseguridad en general al menos semestralmente y según lo requieran los incidentes o problemas comerciales específicos (por ejemplo, una fusión, una nueva asociación estratégica, lanzamiento de un nuevo producto y su cadena de suministro). Los comités con responsabilidad destinada a la supervisión del riesgo (y para la supervisión de los riesgos relacionados con la cibernética en particular) deben recibir información general sobre ciberseguridad por lo menos trimestralmente y cuando surjan incidentes o situaciones específicas.

Véase el Apéndice A para consultar preguntas sugeridas que ayudan a los directores a evaluar el nivel de comprensión de la junta sobre temas de ciberseguridad o ciber-alfabetización.

Con el fin de fomentar el intercambio de conocimientos y el diálogo, algunas juntas invitan a todos los directores a asistir a las discusiones a nivel de comité sobre temas de riesgo cibernético o a hacer uso de la membresía en varios comités. Por ejemplo, el comité de tecnología de la junta directiva de una compañía global incluye directores que son expertos en privacidad y seguridad desde la perspectiva del cliente. Los presidentes de los comités de auditoría y tecnología son miembros, respectivamente, del comité del otro, y los dos comités se reúnen una vez al año para una discusión que incluye una "inmersión profunda" sobre la ciberseguridad[33]. Algunas juntas incluso están estableciendo un comité de ciberseguridad para abordar mejor estos problemas.

Figura 2

¿A qué grupo le ha asignado la junta la mayoría de las tareas relacionadas con las siguientes áreas de supervisión de riesgos? (Lista parcial de selecciones múltiples de opciones de respuesta permitidas)



Fuente: *(2016-2017 NACD Public Company Governance Survey)*

PRINCIPIO 2

Los directores deben entender las implicaciones legales de los riesgos cibernéticos según se relacionan con las circunstancias específicas de su empresa.

El panorama legal y regulatorio con respecto a la ciberseguridad, incluidos los requerimientos de divulgación, la privacidad y la protección de datos, el intercambio de información, la protección de la infraestructura y más, es complejo y está en constante evolución. Las juntas deben estar al tanto de las cuestiones de responsabilidad actuales que enfrentan sus organizaciones y, potencialmente, los directores y dueños de empresas familiares y accionistas mayoritarios uno a uno. Por ejemplo, los ataques de alto perfil pueden generar demandas, incluidas demandas colectivas de accionistas y clientes, y podrían llevar a acciones de cumplimiento normativo. Los reclamantes también podrían alegar que la junta directiva de la organización descuidó su deber fiduciario al no tomar las medidas suficientes para confirmar la idoneidad de las protecciones de la empresa contra las violaciones de datos y sus consecuencias. Las exposiciones pueden variar considerablemente según el sector de la organización y las ubicaciones operativas. Independientemente de los méritos legales o el resultado final de cualquier impugnación, el daño a la reputación de una empresa por una violación cibernética puede ser grave y duradero. No solo es importante que la junta tome los siguientes pasos, sino que es igualmente importante que documente su diligencia debida.

Las juntas deben considerar cómo:

- Mantener registros de las discusiones sobre la ciberseguridad y los riesgos cibernéticos;
- Mantenerse informadas sobre los requisitos específicos de la industria, la región y el sector que se aplican a la organización, incluidas las leyes y los requisitos que podrían establecerse a nivel regional, estatal y local;
- Analizar los riesgos en evolución en relación con la resiliencia empresarial y los planes de respuesta;
- Determinar de antemano qué revelar después de un ataque cibernético.

La cultura de una empresa tiende a fluir desde arriba hacia abajo y, por lo tanto, las juntas deben adoptar un enfoque dinámico hacia la ciberseguridad, responsabilizando directamente a la gerencia, para mostrarles a los empleados que el riesgo cibernético siempre debe ser un asunto importante. Luego, se deben implementar estructuras de gobierno efectivas para apuntalar esa cultura y garantizar que la compañía esté enfocada adecuadamente en la gestión de estos riesgos. También es recomendable que los directores participen en simulaciones de violaciones cibernéticas para lograr exposición a los procedimientos de respuesta de la compañía en el caso de ocurrencia de un incidente grave, para mitigar su impacto potencial y para practicar un escenario potencial que requiera que la junta directiva tome una importante decisión.

Entre los temas que las juntas deben tener en cuenta están los siguientes:

Discusión de la junta y Actas

Las actas de la junta deben reflejar las ocasiones en que la ciberseguridad estuvo en la agenda de las reuniones de toda la junta y/o de los comités clave de la junta, así como también cuando los asuntos cibernéticos se entrelazaron en temas comerciales específicos ante la junta, como la capacitación de empleados o las alianzas estratégicas. Las discusiones en estas reuniones pueden incluir actualizaciones sobre riesgos específicos y estrategias de mitigación, así como informes sobre el programa general de ciberseguridad de la compañía y la integración de la tecnología con la estrategia, las políticas y las actividades comerciales de la organización.

Panorama legal

Como en gran parte del mundo, los gobiernos latinoamericanos están considerando realizar una ola de nuevas regulaciones con respecto a la ciberseguridad y la privacidad. Si bien es importante que las juntas exijan que su administración cumpla con la normativa cibernética y de privacidad, es fundamental que las juntas también comprendan que cumplir con las normas y regulaciones gubernamentales no es equivalente a estar seguro. Muchas regulaciones gubernamentales solo establecen medidas de seguridad mínimas que pueden ser insuficientes para proteger datos valiosos contra métodos de ciberataque cada vez más sofisticados.

Muchas organizaciones deberán gestionar reglas y requisitos que se superponen, e incluso se contradicen, derivados de la falta de coordinación entre las autoridades legislativas y reglamentarias, y las diferentes prioridades que mueven el desarrollo de nuevas regulaciones. Si bien los directores no necesitan tener un conocimiento profundo sobre esta área cada vez más compleja de la ley, deben ser informados por parte de un asesor interno o externo sobre los requisitos que se aplican a la empresa. Los informes de la gerencia deben permitirle a la junta evaluar si la organización está abordando adecuadamente tanto su seguridad como los posibles riesgos legales.

Los requisitos de divulgación y presentación de informes de una empresa dependen del tipo de negocio que realiza y del sector en el que opera. Sin embargo, todos los miembros de la junta deben tener en cuenta su deber primordial, como directores, de ejercer con cuidado, habilidad y diligencia razonables[34].

Un informe preparado por el Programa de Seguridad Cibernética de la OEA[35] recomendó definir y hacer cumplir marcos razonables regulatorios de privacidad y protección de datos, crear plataformas sostenibles nacionales de múltiples interesados y fortalecer la cooperación internacional. En los últimos años, el interés de los formuladores de políticas en ciberseguridad y la privacidad ha crecido, y si bien muchas leyes y regulaciones de ciberseguridad siguen en su etapa incipiente, hay varias tendencias emergentes en el panorama legal en América Latina[36]:

1. Desarrollo de regulaciones centradas en la privacidad y la protección de datos, alineadas con los requisitos de la Unión Europea;
2. Integración de la regulación de la ciberseguridad en las leyes de tecnología financiera;
3. Introducción de requisitos para notificar a las autoridades reguladoras de violaciones de datos.

Otro asunto legal que se debe tener en cuenta es la actividad criminal relacionada con la economía clandestina, ya que el lavado de activos como la criptomoneda representa una gran amenaza y puede tener un impacto significativo en la ciberseguridad de una organización.

Normas de privacidad y protección de datos[37]

A medida que desarrollan sus propias regulaciones, muchos legisladores en América Latina están considerando el enfoque de la Unión Europea a la ciberseguridad como un modelo a seguir. Si bien la mayoría de estas regulaciones están en sus inicios, el desarrollo y la implementación de regulaciones de ciberseguridad enfocadas en la privacidad se ha convertido en una prioridad para los gobiernos de América Latina. Los países de América Latina están comenzando a integrar el Reglamento General de Protección de Datos de la UE (GDPR, por sus siglas en inglés) y otras directivas de ciberseguridad de la UE en sus propios regímenes de protección de datos integrales. La región también está utilizando el Convenio de Budapest sobre la ciberdelincuencia como modelo (Argentina, Chile, Costa Rica, República Dominicana, Panamá y Paraguay fueron partes del Convenio de Budapest, y Colombia, México y Perú fueron observadores) y la aplicación las directivas de la UE de ciberseguridad ya están en vigor. Con la gran probabilidad de que la región adopte un modelo basado en la UE, las empresas seguramente deberán cumplir con los requisitos de ciberseguridad que requieren la implementación de medidas técnicas y organizativas “adecuadas” para garantizar un nivel de seguridad conforme al riesgo.

Requisitos de tecnología financiera

América Latina ha emergido a la vanguardia del desarrollo de nuevas tecnologías dentro del sector financiero. Los países de América Central y del Sur han conservado un sector financiero impulsado por la innovación, pero están surgiendo nuevos requisitos por cuenta de las políticas de ciberseguridad y los requisitos para el procesamiento y almacenamiento de datos. Muchas de estas regulaciones aún están en desarrollo, pero se espera que le brinden más certeza a la industria sobre las medidas de ciberseguridad que deben implementarse. Sin embargo, es probable que las instituciones financieras enfrenten cargas de obligaciones de ciberseguridad más pesadas debido al enfoque en la ciberseguridad de los dispositivos y servicios de tecnología financiera (fintech, en inglés).

Requisitos de "Notificación a la Autoridad"

Los países latinoamericanos tradicionalmente han requerido que se reporten las violaciones de datos a las partes afectadas, pero no a las autoridades regulatorias. Sin embargo, eso está empezando a cambiar a medida que las organizaciones latinoamericanas comienzan a cumplir con el GDPR y otras obligaciones reglamentarias europeas. Debido a la implementación de las normas de la UE, muchos países latinoamericanos están comenzando a crear autoridades nacionales de protección de datos y a adoptar normas de "notificación a la autoridad" similares a las incluidas en el GDPR, estableciendo requisitos no solo para notificar a los consumidores afectados sino también a las autoridades reguladoras pertinentes.

Papel del asesor legal

Los equipos internos legales y de cumplimiento, junto con asesores externos, desempeñan un papel fundamental en la lucha contra los ataques cibernéticos, especialmente a medida que los reguladores de la región se vuelven más fuertes y más activos en áreas como la ciberseguridad y gobernanza corporativa[38]. Los directores deben pedirle a la gerencia que solicite las opiniones de los asesores legales sobre:

- La implementación de un marco para mitigar los riesgos legales y regulatorios;
- El plan de respuesta a incidentes cibernéticos de la organización, incluida la interacción con los reguladores y la gestión de documentos;
- Posibles cuestiones de divulgación relacionadas con los factores de riesgo con miras a un futuro en general.

A medida que los estándares de divulgación, la orientación regulatoria, los requisitos formales y las circunstancias de la compañía continúan evolucionando, la gerencia y los directores deben esperar que el asesor legal los actualice periódicamente.

Litigio

Las juntas pueden enfrentar litigios, por ejemplo, si los clientes o empleados afectados por una violación de datos toman medidas contra la compañía, o si los accionistas alegan que la junta no tomó las medidas adecuadas para proteger los activos, o que administró mal la respuesta a una violación.

También se les puede exigir a las organizaciones que interpongan un litigio, por ejemplo, en forma de medidas cautelares que congelan dinero o información robada por delincuentes cibernéticos o en reclamos contra proveedores terceros responsables. En cada caso, se requerirá que la junta tome decisiones estratégicas basadas en una variedad de factores tales como costos, publicidad, perspectivas de éxito y deberes hacia los accionistas.

PRINCIPIO 3

Las juntas deben tener un acceso adecuado a la experiencia en ciberseguridad y se le debe proporcionar un tiempo regular y adecuado a las discusiones sobre la gestión de riesgos cibernéticos en las agendas de las reuniones de la junta.

En una encuesta reciente, solo el 14 por ciento de los directores cree que su junta tiene un nivel "alto" de conocimiento de los riesgos de ciberseguridad[39]. Un estudio de la OEA reveló que la mayoría de las Juntas Corporativas en América Latina tienen una comprensión "inicial" o "formativa" de la ciberseguridad, lo que significa que tienen una comprensión mínima o nula de la ciberseguridad y los deberes fiduciarios relacionados, o tienen cierta conciencia de los problemas cibernéticos, pero no de cómo los riesgos podrían afectar a sus organizaciones. Incluso entre las juntas corporativas en América Latina que tienen un conocimiento más avanzado sobre ciberseguridad, la gestión de los problemas cibernéticos ha tendido a ser más orientada al perímetro, y reactiva en lugar de proactiva. Como lo señaló el Foro Económico Mundial, "ser resistente requiere que quienes se encuentran en los niveles más altos de una empresa, organización o gobierno reconozcan la importancia de evitar y mitigar los riesgos de manera proactiva".

A menos que se hayan descubierto incidentes cibernéticos, las juntas no han sabido a dónde acudir para abordar la ciberseguridad en sus empresas. El estudio de la OEA enfatiza la importancia de utilizar las mejores prácticas de ciberseguridad dentro de su estructura de gobierno, y les pide a las juntas directivas que comprendan los riesgos a los que se enfrentan, los métodos de ataque primario y los protocolos de la compañía para enfrentar las amenazas cibernéticas.

Recibir informes una sola vez o solo periódicos también puede ser inadecuado. Un director observó: "[La ciberseguridad] es un blanco muy móvil. Las amenazas y vulnerabilidades están cambiando casi a diario, y los estándares sobre cómo administrar y supervisar el riesgo cibernético apenas están comenzando a tomar forma"[40]. En una sesión diferente de intercambio entre pares, otro director sugirió esta analogía útil: "La ciber-alfabetización puede considerarse similar a la alfabetización financiera. No todos los miembros de la junta son auditores, pero todos deberían poder leer una declaración financiera y comprender el lenguaje financiero de los negocios"[41]. (Véase el apéndice A para obtener más información sobre ciber-alfabetización)

Mejorar el acceso a la experticia en ciberseguridad

Las actas de la junta deben reflejar las ocasiones en que la ciberseguridad estuvo en la agenda de las reuniones de toda la junta y/o de los comités clave de la junta, así como también cuando los asuntos cibernéticos se entrelazaron en temas comerciales específicos ante la junta, como la capacitación de empleados o las alianzas estratégicas. Las discusiones en estas reuniones pueden incluir actualizaciones sobre riesgos específicos y estrategias de mitigación, así como informes sobre el programa general de ciberseguridad de la compañía y la integración de la tecnología con la estrategia, las políticas y las actividades comerciales de la organización.

Con el crecimiento de la amenaza cibernética, la responsabilidad (y las expectativas) de los miembros de la junta directiva ha aumentado. Los directores deben hacer más que simplemente comprender que existen amenazas y recibir informes de la gerencia. Deben emplear los mismos principios de indagación y desafío constructivo que son características estándar de las discusiones de la junta directiva sobre la estrategia y el desempeño de la empresa.

Como resultado, algunas compañías están evaluando la posibilidad de agregar experticia en ciberseguridad y/o seguridad de TI directamente a la junta a través de la contratación de nuevos directores. Si bien esto puede ser apropiado para algunas compañías u organizaciones, no existe un enfoque único que se aplique a todas las entidades.

Los comités de nominación y gobernanza deben sopesar muchos factores para cubrir las vacantes de la junta, incluida la necesidad de contar con experticia en la industria, conocimiento financiero, experiencia global, los deseos de la familia propietaria y los interesados mayoritarios, y otras habilidades deseadas, según las necesidades y circunstancias estratégicas de la empresa. En América Latina, a menudo, los propietarios de empresas familiares y los accionistas mayoritarios tienen una influencia clara en la toma de decisiones y la membresía de la junta corporativa y, por lo tanto, desempeñan un papel importante en la resolución de agregar experiencia cibernética a la junta. Ya sea que elijan agregar o no a un miembro de la junta con experiencia específica en el ámbito cibernético, las juntas pueden aprovechar otras formas de aportar perspectivas informadas sobre asuntos de ciberseguridad a la sala de juntas, incluyendo:

- Programar sesiones informativas profundas o exámenes con expertos externos independientes y objetivos que validen si el programa de ciberseguridad cumple con los objetivos previstos.
- Aprovechar a los asesores independientes existentes de la junta, como auditores externos y asesores externos, que cuentan con una perspectiva de múltiples clientes y de toda la industria sobre las tendencias de riesgo cibernético;
- Participar en programas relevantes de formación de directores, ya sea que se ofrezcan internamente o externamente.
- Brindar oportunidades para que los directores compartan sus aprendizajes de programas externos sobre ciberseguridad con otros miembros de la junta
- Crear oportunidades de formación sobre ciberseguridad para los miembros de la junta, las familias propietarias de la empresa y/o las partes interesadas mayoritarias que tienen gran influencia en las decisiones de la junta.

Lograr acceso a una experticia adecuada en ciberseguridad

La mayoría de los directores son especialistas en ciertos campos o áreas de especialización. Si bien pueden tener cierta experticia en la materia derivada de sus carreras anteriores, los directores deberían ofrecer una visión más amplia de la gestión y respuesta de riesgos en toda la empresa.

Una organización no necesariamente tiene que agregar un experto cibernético a su junta directiva. Esa es una decisión que es mejor que sea tomada por cada negocio. Sin embargo, las juntas deben tener claro dónde podría centrarse la responsabilidad cibernética: en un comité de la junta, un sector específico de la gerencia o toda la junta. Esto se refiere a la responsabilidad de la supervisión, no a la ejecución, de la ciberseguridad y los problemas de gestión de riesgos que la acompañan y transmitirles la importancia de la ciberseguridad a los accionistas mayoritarios y familias propietarias.

Además, los riesgos cibernéticos tienen algunas diferencias importantes con respecto a los riesgos tradicionales. Por ejemplo, las organizaciones no pueden protegerse completamente en un mundo interconectado y en rápida evolución. Los adversarios cibernéticos, incluidos estados nacionales, pueden tener muchos más recursos que incluso las corporaciones más grandes, y las dificultades prácticas asociadas con la captura y rastreo de delincuentes cibernéticos son a menudo mayores que aquellas asociadas con criminales más convencionales. Esto es algo que los miembros de la junta de supervisión cibernética deben entender.

Hay varias maneras que las juntas pueden tomar en cuenta para aumentar su acceso a la experticia en seguridad. Pueden crear un sistema de peso y contrapeso, procurando consejos de múltiples fuentes. Por ejemplo, algunas organizaciones sofisticadas han desarrollado estructuras de presentación de informes de tres fuentes independientes (no necesariamente externas), que podrían incluir la perspectiva de la persona responsable del riesgo cibernético, la perspectiva de la persona que evalúa el riesgo cibernético y la perspectiva del gerente operacional. Esto le permite a una organización desafiar las funciones y los enfoques, y ver el riesgo cibernético desde diversas perspectivas. El Principio 4, a continuación, ofrece un esquema de una estructura organizativa que, con el tiempo, puede mejorar la base de conocimiento general sobre ciberseguridad dentro de una empresa.

Mejora de los informes de gestión a la junta

La respuesta a la evaluación de la calidad de la información proporcionada a la junta por parte de la alta gerencia presentó como la más baja la información sobre la ciberseguridad. Casi una cuarta parte de los directores de empresas públicas de EE. UU. informaron que estaban insatisfechos o muy insatisfechos con la calidad de la información proporcionada por la gerencia sobre la ciberseguridad. Menos del 15 por ciento dijo sentirse muy satisfecho con la calidad de la información que recibieron, en comparación con una calificación de alta satisfacción de aproximadamente el 64 por ciento para la información sobre el desempeño financiero[42].

Los encuestados identificaron varias razones para su insatisfacción con los informes de ciberseguridad por parte de la gerencia, que incluyen:

- Dificultad para usar la información para comparar el desempeño, tanto internamente (entre las unidades de negocios dentro de la organización) como externamente (con sus pares en la industria);
- Insuficiente transparencia sobre el desempeño; y
- Dificultad en la interpretación de la información[43].

La ciberseguridad y el análisis del riesgo cibernético son disciplinas relativamente nuevas (ciertamente, menos maduras que el análisis financiero) y tomará tiempo para que maduren las prácticas de presentación de informes. No obstante, los miembros de la junta deben establecer expectativas claras con la gerencia sobre el formato, la frecuencia y el nivel de detalle que desean recibir de la información relacionada con la ciberseguridad y los indicadores clave de rendimiento. En especial, los informes deben redactarse en términos comerciales. Al revisar los informes de la gerencia, los directores también deben tener en cuenta que puede haber un sesgo inherente por parte de la gerencia para minimizar el verdadero estado del entorno de riesgo. Un estudio encontró que el 60 por ciento del personal de TI no informa sobre los riesgos de ciberseguridad sino hasta que se vuelven urgentes (y más difíciles de mitigar), y reconociendo que intentan excluir los resultados negativos[44]. Las juntas deben buscar crear una cultura de comunicación abierta, directa y transparente sobre la gestión y la información de riesgos cibernéticos.

Véase el Apéndice D para obtener más información sobre el tipo de métricas de informes de riesgo cibernético que las juntas pueden y deben esperar recibir de la gerencia.

Fuente: *2016-2017 NACD Public Company Governance Survey*

PRINCIPIO 4

Los directores de la junta deben establecer la expectativa de que la gerencia establecerá un marco de gestión de riesgo cibernético para toda la empresa con personal y presupuesto adecuados.

La tecnología integra a las organizaciones modernas, ya sea que los trabajadores estén al otro lado del corredor o al otro lado del mundo. Pero, como se señaló anteriormente, las estructuras de presentación de informes y los procesos de toma de decisiones en muchas empresas son legados de un pasado, donde cada departamento y unidad de negocios toman decisiones de manera relativamente independiente y sin tener en cuenta que la interdependencia digital es un hecho de los negocios modernos. Los directores deben buscar garantías de que la gerencia está adoptando un enfoque apropiado de ciberseguridad en toda la empresa. El Foro Económico Mundial (WEF, por sus siglas en inglés) señala que la función de gobernanza de las juntas es vital en relación con la ciberseguridad.

El Apéndice J contiene consideraciones para establecer una relación con el responsable central de seguridad informática (CISO, por sus siglas en inglés) y el equipo de seguridad.

Creación de un enfoque general para la gestión del riesgo cibernético

Una organización debe comenzar con una evaluación de su perfil único de riesgo y entorno de amenaza. Quizás el mayor riesgo para una organización moderna es operar bajo un mecanismo de evaluación de riesgos mal construido. La capacidad de una organización para implementar un marco de ciberseguridad efectivo comienza con una comprensión clara del entorno de riesgo, su particular apetito de riesgo y la disponibilidad de recursos necesarios para mitigar los riesgos cibernéticos potenciales. Realmente comienza con un sistema de gestión de riesgo empresarial (ERM, por sus siglas en inglés) relevante, debidamente desarrollado y en operación, en el que se recopilan, evalúan, priorizan, mitigan e informan adecuadamente los principales riesgos estratégicos de la empresa y otros riesgos.

Marco de controles técnicos para la gestión de riesgos

Es esencial que la gerencia pueda articularle claramente a la junta directiva la existencia e implementación de un marco técnico serio y coherente para administrar y asegurar los datos de las organizaciones. En Estados Unidos, el Marco de Ciberseguridad del NIST se usa para establecer un conjunto de estándares, metodologías, procedimientos y procesos que alinean las políticas, los negocios y los problemas tecnológicos para abordar los riesgos cibernéticos. El marco NIST busca proporcionar un lenguaje común para ser usado por la alta gerencia corporativa dentro de la organización en el desarrollo de un enfoque empresarial para la gestión del riesgo cibernético.

Varios gobiernos latinoamericanos han comenzado a avanzar con sus propios marcos de estándares de ciberseguridad. Por ejemplo, en los últimos años, el Gobierno de Perú ha solicitado asistencia técnica de la OEA para desarrollar su propio marco nacional de ciberseguridad. Perú también ha implementado la norma ISO 27001:2013, que también está siendo utilizada cada vez más en América Latina.

En una escala mayor, la Red Iberoamericana de Protección de Datos publicó los Estándares de Protección de Datos Personales para los Estados Iberoamericanos en junio de 2017. Estos estándares se basan en gran medida en las normas de seguridad del GDPR de la UE. Cabe señalar que también puede haber marcos de ciberseguridad específicos de la industria relevantes para las organizaciones. Por ejemplo, los regímenes reglamentarios de fintech, como los que está desarrollando la Comisión Nacional Bancaria y de Valores de México, pueden designar requisitos específicos para la seguridad de los datos y la privacidad de las entidades del sector financiero.

Muchas organizaciones adaptarán uno o más de estos marcos a su sector, cultura y planes de negocios únicos. Lo que es importante desde la perspectiva de la junta no es entender los detalles técnicos del marco, sino que la gerencia tiene un plan coherente para garantizar la ciberseguridad técnica y poder articularle esto claramente a la junta.

Si bien la existencia de un marco técnico coherente, impulsado por objetivos comerciales, es fundamental y, posiblemente, necesario para cumplir con varios requisitos de cumplimiento, las juntas deben ser conscientes de que el cumplimiento de los marcos técnicos no necesariamente equivale a que los datos de una organización estén adecuadamente protegidos. De hecho, las listas de verificación operativas de requisitos, que generalmente se basan en estos marcos, han sido ampliamente criticadas por no proporcionar una imagen real de la seguridad de una organización. Afortunadamente, el campo de la gestión del riesgo cibernético está evolucionando y ahora existen nuevos métodos de evaluación del riesgo cibernético que ofrecen una manera más contextualizada, empírica y económica para que una organización entienda su ciberseguridad relativa. Consulte el apéndice sobre métricas para conocer ejemplos de estos nuevos métodos de evaluación de riesgos.

Un marco de gestión para la ciberseguridad

Los directores también deben establecer la expectativa de que la gerencia tenga en cuenta si las estructuras corporativas tradicionales, que a menudo aíslan varios departamentos, son apropiadas para un sistema mucho más integrado y consistente con la era digital. Al menos con respecto a la ciberseguridad, las organizaciones líderes en todo el mundo están adoptando marcos de gestión que crean un equipo de gestión de riesgo cibernético para toda la empresa, no dominado por TI sino bajo la supervisión de un ejecutivo con una perspectiva amplia de la empresa, como un Director de Operaciones, Director Financiero o un Director de Riesgo. El equipo de gestión de riesgos cibernéticos también debe operar con un presupuesto separado y adecuado para evaluar y gestionar el riesgo cibernético. A continuación se describe un marco de este tipo desarrollado por ISA conjuntamente con el American National Standards Institute (ANSI).

Un enfoque integrado para la gobernanza del riesgo cibernético

1. Establezca la propiedad del riesgo cibernético sobre una base interdepartamental. Un alto gerente con autoridad interdepartamental, como el Director de Seguridad de la Información, el Director Financiero, el Director de Riesgos o el Director de Operaciones (no el Director de Información) debe dirigir el equipo.

2. Nombre a un equipo de gestión de riesgos cibernéticos entre la organización. Todos los departamentos interesados deben estar representados, incluidos los líderes de las unidades de negocios, legal, auditoría interna y cumplimiento, finanzas, recursos humanos, TI y gestión de riesgos. (Véase el aparte de “Funciones y responsabilidades de la gerencia clave” a continuación). Un objetivo clave de esta gestión entre la organización es garantizar que no haya un eslabón débil o excepción en materia de ciberseguridad dentro de la organización.

3. El equipo de riesgo cibernético deberá realizar una evaluación de riesgos orientada hacia el futuro en toda la empresa, utilizando un marco sistemático que tenga en cuenta la complejidad del riesgo cibernético, incluyendo, pero no limitado a, cumplimiento regulatorio. Esto incluiría evaluar el panorama actual de amenazas y el panorama de riesgo de la organización. Luego, se establecería claramente su apetito de riesgo. La identificación del riesgo potencial para la organización, así como su umbral de riesgo, le ayudará al equipo de riesgo cibernético a evaluar qué marco sistemático se alinea más adecuadamente con su misión y objetivos.

4. Tenga en cuenta que las leyes y regulaciones de ciberseguridad difieren significativamente entre jurisdicciones y sectores. Como se señaló en el Principio 2, la gerencia debe dedicar recursos para rastrear los estándares y requisitos que se aplican a la organización, especialmente a medida que algunos países amplían agresivamente el alcance de la participación del gobierno en el ámbito de la ciberseguridad.

5. Adopte un enfoque de colaboración para desarrollar informes para la junta. Se debe esperar que los ejecutivos realicen un seguimiento e informen las métricas que cuantifican el impacto comercial de las amenazas cibernéticas y la gestión de riesgos asociados. La evaluación de la efectividad de la gestión del riesgo cibernético y la resiliencia cibernética de la empresa deben realizarse como parte de auditorías internas trimestrales y otras revisiones de desempeño. Estos informes deben encontrar el equilibrio adecuado entre entregar demasiados detalles y lo que es estratégicamente importante para la Junta de Supervisión.

6. Desarrolle y adopte un plan de gestión de riesgos cibernéticos para toda la organización, incluida la estrategia de comunicaciones internas en todos los departamentos y unidades de negocio, y los planes de auditoría interna y aseguramiento. Si bien la ciberseguridad obviamente tiene un componente importante de TI (tecnología de la información), todas las partes interesadas deben participar en el desarrollo del plan corporativo y deben sentirse comprometidas con esta, incluidas las funciones legales, de auditoría, de riesgo y de cumplimiento. Se debe hacer una prueba del plan de forma rutinaria.

7. Desarrolle y adopte un presupuesto total de riesgo cibernético con recursos suficientes para satisfacer las necesidades y el apetito de riesgo de la organización. Las decisiones sobre recursos deben tener en cuenta la grave escasez de talentos con experiencia en ciberseguridad e identificar qué necesidades pueden satisfacerse internamente y qué se puede o debe subcontratar. Debido a que la ciberseguridad es más que la seguridad de TI (o tecnología de la información), no debe vincularse el presupuesto para la ciberseguridad exclusivamente a un departamento. Ejemplos incluyen asignaciones en áreas como capacitación de empleados, seguimiento de regulaciones legales, relaciones públicas, desarrollo de productos y administración de proveedores. El presupuesto también podría incluir una revisión de talento y un plan de sucesión para la gestión crítica, como son los Directores de Operaciones, de Tecnología, Seguridad Informática, etc. Se puede aumenta la preparación cibernética de la organización al evaluar la preparación de los sucesores y determinar si se necesita capacitación adicional para los empleados actuales para cumplir estos roles en el futuro o si el reclutamiento externo de talento es necesario. La revisión de talento le ayudará a la organización minimizar la interrupción causada por la rotación de empleados.

Fuente: *Internet Security Alliance*[1]

1 Adaptado de Internet Security Alliance y American National Standards Institute, The Financial Management of Cyber Risk: An Implementation Framework for CFOs (Washington, DC: ANSI, 2010). Véase también Internet Security Alliance, Sophisticated Management of Cyber Risk (Arlington, VA: ISA, 2013).

PRINCIPIO 5

La discusión de la junta directiva sobre el riesgo cibernético debe incluir la identificación de qué riesgos evitar, cuáles aceptar y cuáles mitigar o transferir a través de un seguro, así como planes específicos asociados con cada abordaje.

La ciberseguridad total es un objetivo poco realista. La ciberseguridad es un proceso continuo, no un estado final, y la seguridad no es igual que cumplimiento. Los equipos de administración deben determinar dónde creen, en un espectro de riesgo, que pueden optimizarse las operaciones y los controles de la empresa. En otras palabras, cuál es el apetito de riesgo cibernético de la organización (y que no sea cero, porque no es realista).

Definición del apetito de riesgo

El apetito de riesgo es la cantidad de riesgo que una organización está dispuesta a aceptar para lograr objetivos estratégicos o aquel que la organización no está dispuesta a aceptar en absoluto. Se le debe dar mucha importancia al apetito de riesgo en cualquier junta y es una consideración fundamental de un enfoque de gestión de riesgos en toda la empresa. Por lo tanto, debe definir el nivel de riesgo en el que se necesitan las acciones apropiadas para reducir el riesgo a un nivel aceptable. Cuando se define y comunica adecuadamente, este impulsa el comportamiento al establecer los límites para administrar el negocio y capitalizar las oportunidades.

Un debate sobre el apetito de riesgo debe abordar las siguientes preguntas:

- Valores corporativos - ¿Qué riesgos no aceptaremos?
- Estrategia: ¿Cuáles son los riesgos que debemos tomar?
- Partes interesadas: ¿Qué riesgos están dispuestos a asumir y a qué nivel?
- Capacidad: ¿Qué recursos se requieren para administrar esos riesgos?

"El apetito de riesgo es una cuestión de juicio basada en las circunstancias y objetivos específicos de cada compañía. No hay una solución única para todos".

Fuente: *PwC, Board oversight of risk: Defining risk appetite in plain English (New York, NY: PwC, 2014), p. 3.*

Al igual que con otras áreas de riesgo, la tolerancia al riesgo cibernético de una organización debe ser coherente con su estrategia y objetivos comerciales. Cuando una organización analiza su riesgo cibernético, debe hacerlo como parte de su evaluación general de riesgos, ubicando adecuadamente a los cibernéticos en el contexto de otros riesgos. La asignación de recursos de seguridad es una función de equilibrio entre los objetivos de negocio y los riesgos inherentes en los sistemas digitales (Véase "Definición del apetito de riesgo", página 19). Existen múltiples riesgos cibernéticos y múltiples métodos para abordarlos. La gerencia debe presentarle a la junta una imagen clara del panorama de riesgo y un plan para abordarlo. Para lograr esto, los directores y los equipos gerenciales deberán analizar las siguientes preguntas:

• **¿Qué datos, sistemas y operaciones comerciales estamos dispuestos a perder o ver comprometidos?** Las discusiones sobre la tolerancia al riesgo ayudarán a identificar el nivel de riesgo cibernético que la organización está dispuesta a aceptar como un asunto empresarial práctico. En este contexto, distinguir entre datos críticos o de alta sensibilidad (Véase Identificación de las 'Joyas de la Corona' de la compañía y categorías de datos muy confidenciales, página 9) y otros datos o sistemas que son igualmente importantes, pero menos esenciales o sensibles es un primer paso clave. Sin embargo, el compromiso de los datos no es el único componente del riesgo cibernético. Podrían existir implicaciones legales, incluidas sanciones reglamentarias por violaciones de datos, que superan con creces el valor real de los datos, y el riesgo de reputación de una mala publicidad puede corresponder más a factores externos que al valor real de los sistemas comprometidos.

• **¿Cómo deben asignarse las inversiones en mitigación del riesgo cibernético entre las defensas básicas y avanzadas?** Al considerar cómo abordar amenazas más sofisticadas, la gerencia debe centrarse más profundamente en las defensas sofisticadas diseñadas para proteger los datos y sistemas más críticos de la empresa. Si bien, en principio la mayoría de las organizaciones estarían de acuerdo con esto, en realidad, muchas organizaciones aplican medidas de seguridad a todos los datos y funciones por igual. Las juntas deben alentar a la gerencia a considerar las inversiones de ciberseguridad de la empresa en términos económicos de retorno de la inversión y a reevaluar el retorno de la inversión con regularidad. Recientemente han aparecido nuevas herramientas analíticas en el mercado que pueden ayudar a la gerencia a definir mejor el riesgo cibernético en términos económicos, y la gerencia debería considerar si estas herramientas son apropiadas para sus cálculos de riesgo cibernético. (Véase el Apéndice I sobre Economía de las métricas cibernéticas)

• **¿Qué opciones están disponibles para ayudarnos a mitigar ciertos riesgos cibernéticos?** Las organizaciones de todas las industrias y tamaños tienen acceso a soluciones integrales que pueden ayudar a reducir parte del riesgo cibernético. Incluyen una batería de medidas preventivas, como revisiones de marcos de ciberseguridad y prácticas de gobernanza, capacitación de empleados, seguridad de TI, servicios de respuesta de expertos y servicios de gestión de seguridad. Más allá de cobertura para pérdidas financieras, estas herramientas pueden ayudar a mitigar el riesgo de una organización de sufrir daños a la propiedad y lesiones personales como resultado de una violación cibernética. Algunas soluciones también incluyen acceso a herramientas proactivas, capacitación de empleados, seguridad de TI y servicios de respuesta de expertos, hasta agregar otra capa de protección y experticia. La inclusión de estos servicios de valor agregado demuestra aún más la importancia de sacar la ciberseguridad del departamento de TI y pasarla a generar discusiones de estrategia y riesgo en toda la empresa, tanto a nivel de la gerencia como de la junta. Sin embargo, la gerencia debe mantener a la junta informada sobre el cambiante panorama del riesgo cibernético y ser lo suficientemente ágil para poder adaptarse a los cambios rápidos de tecnologías y los escenarios de ciberataques, como el robo de datos, la corrupción de datos e incluso el uso de mecanismos de seguridad (por ejemplo, cifrado) como métodos de ataque (por ejemplo, ransomware).

• **¿Qué opciones están disponibles para ayudarnos a transferir ciertos riesgos cibernéticos?** Existe un seguro cibernético para proporcionar un reembolso financiero por pérdidas inesperadas relacionadas con incidentes de ciberseguridad. Esto puede incluir la divulgación accidental de datos, como perder una computadora portátil que no esté cifrada, o ataques externos malintencionados, como esquemas de suplantación de identidad (phishing), infecciones de programas malignos (malware) o ataques de denegación de servicio. Al elegir un socio de seguro cibernético, es importante que la organización elija un operador con la amplitud de innovación global que mejor se adapte a las necesidades de la organización. Las aseguradoras a menudo realizan revisiones en profundidad de los marcos de ciberseguridad de la empresa durante el proceso de suscripción y los precios de las pólizas pueden ser una señal sólida que ayuda a las compañías a comprender sus fortalezas y debilidades de la ciberseguridad. Muchas aseguradoras, en asociación con empresas de tecnología, bufetes de abogados,

empresas de relaciones públicas y otros, también ofrecen acceso a las medidas preventivas mencionadas anteriormente. Sin embargo, es importante tener en cuenta que no todos los países latinoamericanos tienen mercados de seguros maduros que permitan la transferencia del riesgo cibernético por medio del seguro, por lo que las organizaciones deberían considerar si el seguro de ciberseguridad es una opción viable para transferir el riesgo cibernético.

• **¿Cómo debemos evaluar el impacto de los incidentes de ciberseguridad?** Llevar a cabo una evaluación de impacto adecuada puede ser un reto dado el número de factores involucrados. En un mundo interconectado, puede haber riesgos cibernéticos para la organización que existen fuera de la capacidad de la organización para mitigarlos directamente de manera efectiva. Por ejemplo, la publicidad sobre violaciones de datos puede complicar sustancialmente el proceso de evaluación de riesgos. Las partes interesadas (incluidos los empleados, clientes, proveedores, inversionistas, la prensa, el público y las agencias gubernamentales) pueden ver poca diferencia entre una brecha comparativamente pequeña y una grande y peligrosa. Como resultado, los daños a la reputación y el impacto asociado (incluidas las reacciones de los medios de comunicación, los inversionistas y otras partes interesadas clave) pueden no corresponder directamente con el tamaño o la gravedad del evento. De hecho, en esta era de la súper transparencia, redes sociales y noticias inexactas, el impacto del riesgo de reputación que resulta de un incidente cibernético puede ser severo y desproporcionado, y le corresponde a la junta directiva y la alta gerencia pensar y estar preparados para el posible riesgo de reputación asociado con un incidente cibernético[45]. La junta debe buscar garantías de que la gerencia ha analizado detenidamente estas implicaciones cuando diseñó estrategias organizativas para la gestión de riesgos cibernéticos. Estos incluyen tanto la gestión operativa de TI como estrategias relacionadas con acuerdos legales con socios y proveedores que ayudan a garantizar la seguridad adecuada y un Plan de relaciones públicas o comunicación para abordar el riesgo de reputación cuando ocurra un evento.

APÉNDICE A

Evaluación de la cultura de ciberseguridad de la junta

Un informe de la Blue Ribbon Commission de la NACD sobre Evaluación de la Junta definió la cultura de la sala de juntas como "los valores compartidos que subyacen e impulsan las comunicaciones, las interacciones y la toma de decisiones de la junta. Es la esencia de cómo se hacen las cosas realmente"[46]. En palabras de un participante:

Las juntas necesitan cambiar sus mentalidades. Debemos pasar de preguntar: "¿Cuál es la probabilidad de que nos ataquen?" A decir: "Es probable que nos hayan atacado"; de ver la ciberseguridad como un costo a pasar a verla como una inversión que nos ayuda a mantenernos competitivos; de esperar que la gerencia prevenga o se defienda contra las amenazas cibernéticas a preguntar qué tan rápido puede detectarlas y responder a ellas[47]*. Además, las juntas deben considerar qué vulnerabilidades existen dentro de su organización que podrían ser explotadas por un atacante, identificando los activos de valor y qué beneficio se obtendría al atacar esos activos.*

Los directores que deseen incorporar un componente de ciberseguridad en las autoevaluaciones de su junta pueden usar las preguntas de la tabla a continuación como punto de partida. Una calificación de 1 es baja, una calificación de 5 es excelente.

**Use la escala numérica para indicar donde se ubica la cultura de la junta en general, en el espectro que se muestra a continuación. <----------> **			**Elemento de acción**
Nuestra junta, en general, considera que la ciberseguridad es un problema principalmente de TI/tecnología.	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Nuestra junta entiende la ciberseguridad como un problema de gestión de riesgos en toda la empresa.	
Nuestra junta se basa en el entorno legal para la ciberseguridad, en gran medida estable y generalmente aplicable a la mayoría de las empresas de la misma manera.	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Nuestra junta Directiva valora la necesidad de buscar asesoría legal, de forma regular, en relación con un entorno cibernético legal adaptado a nuestros planes y entornos empresariales en evolución.	
Nuestra junta no necesita actualizaciones periódicas sobre ciberseguridad por parte de expertos de la industria en el campo.	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Nuestra junta regularmente busca expertos cibernéticos en relación con nuestras necesidades cibernéticas emergentes y el panorama de amenazas.	
Nuestra junta no siente la necesidad de que la gerencia proporcione un plan específico para administrar el riesgo cibernético.	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Nuestra junta espera que la gerencia nos brinde un marco operativo y de gestión que refleje el impacto moderno de la tecnología digital, y cómo debemos administrar esa tecnología, de acuerdo con nuestras necesidades y riesgos comerciales.	
Nuestra junta no espera que la gerencia evalúe y administre los riesgos cibernéticos de manera particular.	1 2 3 4 5 ☐ ☐ ☐ ☐ ☐	Nuestra junta espera que la gerencia nos brinde un análisis claro de cuáles son nuestros riesgos cibernéticos, cuáles aceptamos, qué podemos mitigar y qué podemos transferir de manera coherente con nuestros objetivos comerciales.	

APÉNDICE B

Preguntas fundamentales que los directores deberían preguntarse acerca de la ciberseguridad

Incluso antes de una reunión de la junta, los directores pueden realizar una autoevaluación si han teniendo en cuenta varios aspectos de la ciberseguridad, más allá de los aspectos técnicos y operativos. En particular, las juntas deberían pensar en la ciberseguridad en términos de negocios y considerar si están preparando a su organización en un nivel estratégico. Entre las preguntas que los directores pueden querer hacer están las siguientes:

1. ¿El Director General alienta el diálogo abierto entre la junta directiva, las fuentes externas y la gerencia sobre las amenazas cibernéticas emergentes?

2. ¿Existen mecanismos para informar adecuadamente a los dueños de empresas familiares y accionistas mayoritarios que tienen poderes de decisión en la junta sobre la ciberseguridad de la organización?

3. ¿Quién gestiona nuestra ciberseguridad? ¿Tenemos el talento adecuado y líneas claras de comunicación/responsabilidad en materia de ciberseguridad? ¿Está el tema cibernético incluido en nuestro registro de riesgos?[48] ¿Qué consideramos nuestros activos comerciales más valiosos? ¿Cómo interactúa nuestro sistema de TI con esos activos?

4. ¿Estamos considerando los aspectos de ciberseguridad de nuestras principales decisiones comerciales, como fusiones y adquisiciones, asociaciones, lanzamientos de nuevos productos, etc., de manera oportuna?

5. ¿Creemos que existe una protección adecuada funcionando si alguien deseara atacar o dañar nuestras "joyas de la corona" u otros datos altamente confidenciales? ¿Qué se necesitaría para sentirse seguro de que esos activos/datos están protegidos?

6. ¿Estamos gastando sabiamente en herramientas de ciberseguridad y capacitación? ¿Sabemos si nuestro gasto es rentable? ¿Estamos realmente mejorando la seguridad o simplemente cumpliendo con requisitos de cumplimiento? ¿Qué mecanismos se están implementando para capacitar a los empleados en temas básicos de ciberseguridad en toda la empresa?

7. ¿Hemos considerado cómo administraríamos nuestras comunicaciones en el caso de un evento, incluida la comunicación con el público, nuestros accionistas, nuestros reguladores, nuestras agencias de calificación? ¿Tenemos estrategias segmentadas para cada una de estos públicos?

8. ¿Participa nuestra organización en alguna de las organizaciones de ciberseguridad y de intercambio de información del sector público o privado? ¿Deberíamos?

9. ¿La organización está supervisando adecuadamente la legislación y la regulación actuales y potenciales relacionadas con la ciberseguridad y el desarrollo de políticas y marcos nacionales de ciberseguridad?[49]

10. ¿La organización está aprovechando los recursos de los CSIRT nacionales para analizar el riesgo y prevenir ataques?

11. ¿Está la organización trabajando con pares para compartir información sobre amenazas de ciberseguridad?

12. ¿Tiene la empresa un seguro adecuado, incluidos directores y funcionarios, que cubra los eventos cibernéticos? ¿Qué se cubre exactamente?[50] ¿Existen beneficios, más allá de la transferencia de riesgos, para tomar un seguro cibernético?[51]

APÉNDICE C

Preguntas que le puede hacer la junta a la gerencia sobre la ciberseguridad relacionadas con el conocimiento de la situación

Los Principios 4 y 5 de este Manual se relacionan con la responsabilidad de la junta directiva de lograr que la gerencia proporcione información adecuada para gestionar el riesgo cibernético a nivel estratégico. Al implementar estos principios, los miembros de la junta pueden optar por hacer algunas de las siguientes preguntas de la gerencia. Las preguntas de ciberseguridad no solo deben plantearse en el contexto de una violación existente, sino en varios puntos del proceso de desarrollo empresarial. Para facilitar su uso, el Manual desglosa las preguntas en temas relevantes que tienen implicaciones de ciberseguridad.

1. ¿Cuáles son nuestros servicios críticos de negocios? ¿Cómo se relacionan con las entidades legales, las perspectivas de los reguladores, los departamentos de TI y los proveedores?

2. ¿Cómo estamos utilizando las operaciones de TI para avanzar en nuestros objetivos comerciales y cuáles son las debilidades de nuestro enfoque?

3. ¿Cuáles son los riesgos de ciberseguridad de la empresa y cómo los gestiona la empresa?[52]

a. ¿Tenemos un inventario de sistemas de TI y una lista de los sistemas de TI más críticos?
b. ¿Dónde está el mayor riesgo? ¿Dónde estamos en el reemplazo de programas obsoletos?
c. ¿Cuál es nuestro mapa de la junta para aprobarlos de modo que comprendamos la antigüedad de los sistemas y cuándo es el momento de reemplazar/actualizarlos?

4. ¿Se nos informó de los ataques cibernéticos que ya han ocurrido y lo graves que fueron?

5. ¿Qué es importante proteger y cuántas veces hemos visto comprometidos estos activos?

6. ¿Quiénes son nuestros probables adversarios? ¿Son hackers privados o estados-nación?

7. En opinión de la gerencia, ¿cuál es la vulnerabilidad más grave relacionada con la ciberseguridad (incluidos los sistemas, el personal o los procesos de TI (y tecnología))?

8. Si un adversario quisiera infligir el mayor daño a nuestra empresa, ¿cómo lo harían?

9. ¿Cuándo fue la última vez que realizamos una prueba de penetración o una evaluación externa independiente de nuestras defensas cibernéticas? ¿Cuáles fueron los hallazgos clave y cómo los estamos abordando? ¿Cuál es nuestro nivel de madurez?

10. ¿Respondemos ante reguladores o auditores externos? ¿Cuándo es probable que ocurra una auditoría? ¿Qué significaría una auditoría para el cumplimiento y la gestión de riesgos?

11. ¿Nuestro auditor externo indica que tenemos deficiencias relacionadas con la ciberseguridad en los controles internos de la compañía sobre la información financiera? Si es así, ¿Cuáles son y qué estamos haciendo para remediar estas deficiencias?

12. ¿Hemos considerado obtener una evaluación independiente, por parte de terceros, de nuestro programa de gestión de riesgos de ciberseguridad?

13. ¿Somos miembros de comunidades de intercambio de información? Si es así, ¿cuáles son las lecciones aprendidas de nuestros compañeros que han sufrido violaciones?

APÉNDICE D

Preguntas que le puede hacer la junta a la gerencia sobre estrategia y operaciones

1. ¿Cuáles son los marcos con los que nos alineamos? ¿Ha realizado un análisis de brechas?

2. ¿Tenemos estrategias apropiadamente diferenciadas para la ciberseguridad general y para proteger nuestros activos críticos misionales?

3 ¿Tenemos un equipo de gestión de riesgo cibernético para toda la empresa y con presupuesto independiente? ¿Es adecuado el presupuesto? ¿Cómo se integra con el proceso general de gestión de riesgos de la empresa? ¿Qué tipo de decisiones de estrategia tienen un impacto en el riesgo cibernético?

4. ¿Tenemos un marco sistemático, como el Marco de Ciberseguridad del NIST, las Normas de protección de datos funcionando, para abordar la ciberseguridad y garantizar una higiene adecuada de la ciberseguridad?

5. ¿Dónde están en desacuerdo la gerencia y nuestros equipos de TI/tecnología sobre la ciberseguridad?

6. ¿Los proveedores y contratistas subcontratados de la empresa cuentan con políticas y controles de ciberseguridad? ¿Se monitorean esos controles? ¿Se alinean esas políticas con las expectativas de nuestra empresa?

7. ¿Cuál es nuestra cobertura de seguro para temas cibernéticos? ¿Es adecuado? ¿Qué tipo de seguro tenemos? ¿Por qué tenemos ese tipo de seguro?

8. ¿Existe un programa continuo de capacitación y concientización en toda la compañía alrededor de la ciberseguridad?

9. ¿Cuál es nuestra estrategia para abordar las amenazas a la nube, traiga su propio dispositivo (BYOD) y la cadena de suministro?

10. ¿Cómo estamos abordando las vulnerabilidades de seguridad que se presentan dada una fuerza laboral cada vez más móvil?

11. ¿Estamos creciendo orgánicamente o comprando empresas? ¿Son empresas maduras o empresas nuevas? ¿Dónde estamos geográficamente?

12. ¿Cómo debe estructurarse la junta para supervisar la ciberseguridad a nivel de toda la empresa?

APÉNDICE E

Preguntas que le puede hacer la junta a la gerencia sobre la ciberseguridad relacionadas con amenazas internas

1. ¿Cómo ayudan nuestros controles operacionales, incluidas las restricciones de acceso, el cifrado, las copias de seguridad de datos, el monitoreo del tráfico de red, etc., a protegernos contra amenazas internas?

2. ¿Cómo hemos adaptado nuestras políticas de personal, como las verificaciones de antecedentes, orientación de los nuevos empleados, la capacitación relacionada con cambios de departamento/roles, salidas de los empleados, etc., para incorporar la ciberseguridad?

3. ¿Tenemos un plan de actividades para incidentes de información privilegiada que explique cómo y cuándo contactar a un abogado, a las autoridades policiales y/u otras autoridades, y explorar remedios legales?
4. ¿Tenemos capacidades de investigación forense?

5. ¿Cuáles son las prácticas líderes para combatir las amenazas internas y en qué se diferencian de las nuestras?

6. ¿Cómo funcionan conjuntamente las funciones clave (TI, RR.HH., Legal y Cumplimiento) con las unidades de negocios para establecer una cultura de concientización sobre el riesgo cibernético y la responsabilidad personal de la ciberseguridad? Las consideraciones incluyen lo siguiente:

a. Se debe requerir políticas escritas que cubran datos, sistemas y dispositivos móviles y deben cubrir a todos los empleados.

b. Establecimiento de un entorno seguro para informar sobre incidentes cibernéticos (incluido el auto-informe de problemas accidentales).
c. Capacitación regular sobre cómo implementar políticas de ciberseguridad de la empresa y reconocer amenazas.

7. ¿Qué intentamos prevenir cuando nos protegemos contra amenazas internas?

8. ¿Qué conflictos de interés pueden existir dentro de las organizaciones que podrían contribuir a tener una amenaza interna relacionada con la ciberseguridad?

APÉNDICE F

Preguntas que le puede hacer la junta a la gerencia sobre la ciberseguridad relacionadas con la cadena de suministro

1. ¿Qué hacemos actualmente y qué debemos hacer para incluir la ciberseguridad en nuestra actual gestión de riesgos de la cadena de suministro?

2. ¿Cuánto sabemos sobre nuestra cadena de suministro con respecto a los controles y la exposición al riesgo cibernético? ¿Qué procesos de diligencia debida utilizamos para evaluar la idoneidad de las prácticas de ciberseguridad de nuestros proveedores (tanto durante el proceso de incorporación como durante la vigencia de cada contrato)? ¿Qué departamentos/unidades de negocio están involucrados? ¿Existen acuerdos de contingencia apropiados en el caso de un problema importante con proveedores externos críticos?

3. ¿El negocio lleva a cabo un monitoreo estratégico apropiado de proveedores externos?

4. ¿Qué proveedores utilizamos para la nube? ¿Qué funciones empresariales críticas hemos subcontratado a terceros, tales como la seguridad en la nube?

5. ¿Cómo equilibramos las oportunidades financieras (menores costos, mayor eficiencia, etc.) creadas por una mayor flexibilidad de la cadena de suministro con riesgos cibernéticos potencialmente mayores?

6. ¿Cómo se incorporan los requisitos de ciberseguridad en los acuerdos con los proveedores? ¿Cómo se monitorean? ¿Estamos haciendo nuestra debida diligencia para hacer cumplir los contratos? Los contratos pueden ser escritos de manera que incluyan requisitos mínimos de ciberseguridad, como los siguientes:

a. Políticas de ciberseguridad escritas.
b. Políticas de personal, tales como verificación de antecedentes, capacitación, etc.
c. Controles de acceso.
d. Políticas de cifrado, copia de seguridad y recuperación.
e. Requisitos detallados en cuanto a los datos en poder del tercero.
    i. Requisitos de retención y eliminación de datos en poder del tercero.

ii. Borrar inventarios de tipos de datos en poder del tercero.
iii. Claridad sobre lo que se almacena, mueve, procesa, etc.

f. Acceso secundario a los datos.
g. Países donde se almacenarán los datos.
h. Notificación de violaciones de datos u otros incidentes cibernéticos.
i. Planes de comunicación para la notificación y respuesta a incidentes.
j. Planes de respuesta a incidentes.
k. Auditorías de prácticas de ciberseguridad y/o certificaciones periódicas de cumplimiento.

7. ¿Les permitimos a nuestros proveedores subcontratar la entrega de alguna parte del contrato? En caso afirmativo, ¿qué nivel de control/escrutinio ejercemos sobre los acuerdos de subcontratación? ¿Cómo supervisamos los cambios en los acuerdos de subcontratación durante la vigencia del contrato?

8. ¿Contamos con tecnología para hacer un perfil de proveedores y socios desde el punto de vista de la ciberseguridad para identificar posibles vulnerabilidades y gestionar activamente el riesgo de terceros?

9. ¿Estamos indemnizados por incidentes de seguridad en nuestra cadena de suministro? ¿Cuál es la solidez financiera de la indemnización?

10. ¿Qué tan difícil/costoso será establecer y mantener un sistema viable de pruebas de penetración y vulnerabilidad cibernética para nuestra cadena de suministro?

11. ¿Qué tan difícil/costoso será mejorar el monitoreo de los puntos de acceso en las redes de proveedores?

12. ¿Nuestros acuerdos de proveedores conllevan riesgos legales incrementales o generan requisitos de cumplimiento adicionales (por ejemplo, GDPR, FCA, etc.)?

APÉNDICE G

Preguntas que le puede hacer la junta a la gerencia sobre la planificación de un posible incidente, manejo de crisis y respuesta

1. ¿Cuál es nuestra capacidad para proteger, detectar y responder a incidentes? ¿Cómo se compara con otros en nuestro sector?

2. En el contexto de nuestro negocio, ¿qué constituye una violación importante a la ciberseguridad? ¿Cómo se compara esto con la definición (si existe) en las leyes y regulaciones relevantes aplicables a nuestro negocio?

3. ¿En qué momento se informa a la junta directiva de un incidente? ¿Cuáles son los criterios para informar?

4. ¿Qué se sabe sobre la intención y la capacidad del atacante? ¿Qué sabemos acerca de cómo el atacante podría usar los datos?

5. ¿Tenemos claro quiénes deben ser notificados y cuándo? ¿La ley requiere una notificación a los organismos reguladores o solo a las partes afectadas? Si es así, ¿Cuáles son las consideraciones de tiempo y estrategia para informar a los clientes sobre incidentes? ¿A los reguladores/entidades gubernamentales relevantes? ¿A los de cumplimiento de la ley? ¿A los vendedores/socios? ¿Internamente? ¿A los pares? ¿A los inversionistas? ¿Qué tiempos son obligatorios por ley y las regulaciones y qué es a discreción de la compañía?

6. ¿Cómo responderá la gerencia a un ciberataque?[54] ¿Tiene la empresa un plan validado de respuesta a incidentes?[55] ¿Estamos ejercitando adecuadamente nuestro plan de preparación y respuesta cibernética?

7. ¿Tenemos un plan de gestión de crisis en marcha? Para violaciones significativas, ¿qué tan bueno es nuestro plan de comunicación (tanto interno como externo) mientras se obtiene información sobre la naturaleza y el tipo de violación, los datos afectados y las derivaciones para la compañía y el plan de respuesta?[56]

8. ¿Qué estamos haciendo para evitar empeorar el problema para nuestra organización? ¿Cómo nos aseguramos de contar con el asesoramiento legal adecuado en los equipos de gestión de incidentes y crisis? ¿Están los equipos legales integrados en los planes de incidentes y crisis?

Después de un incidente de ciberseguridad

1. ¿Cómo supimos del incidente? ¿Nos notificó un tercero o se descubrió el incidente internamente?

2. ¿Cuál creemos que fue el motivo del incidente? ¿Cuál fue el impacto, y cómo lo medimos? ¿Alguna de nuestras operaciones ha sido comprometida?

3. ¿Está funcionando nuestro plan de respuesta a incidentes/crisis cibernética, y está funcionando según lo planeado?

4. ¿Qué está haciendo el equipo de respuesta para garantizar que el incidente está bajo control y que el atacante ya no tiene acceso a nuestra red interna?

5. ¿El equipo de respuesta está coordinando con los CSIRT nacionales para gestionar el incidente? ¿Qué mecanismos existen para colaborar y compartir información con colegas confiables en el sector privado y/o gobierno?

6. ¿Cuáles fueron las debilidades en nuestro sistema que permitieron que ocurriera el incidente y por qué no se identificaron o remediaron?

7. ¿El equipo de seguridad ha comprobado las vulnerabilidades asociadas en todos los sistemas/redes de la empresa, no solo en los sistemas o servicios afectados? ¿Han comparado lo que sucedió contra el marco de controles, e hicieron los cambios necesarios tanto en los controles de seguridad como en los controles de negocios?

8. ¿Qué pasos podemos tomar para asegurarnos de que este tipo de evento no vuelva a ocurrir? ¿Cómo nos aseguramos de que se aprendieron las lecciones y se les hará seguimiento a las acciones de remediación?

9. ¿Qué podemos hacer para mitigar las pérdidas causadas por el incidente?

10. ¿El incidente altera la tolerancia al riesgo del negocio? ¿Se ha discutido esto y se han capturado cambios?

Fuente: *NACD, et al., Cybersecurity: Boardroom Implications (Washington, DC: NACD, 2014) (an NACD white paper).*

APÉNDICE H

Consideraciones de ciberseguridad durante las fases de fusiones y adquisiciones

Las compañías involucradas en transacciones a menudo son objetivos principales para hackers y ciberdelincuentes, porque el valor de la información confidencial relacionada con el negocio es alta; y los plazos cortos, el entorno de alta presión y las cargas de trabajo significativas asociadas con las transacciones pueden hacer que los actores clave actúen de manera descuidada y potencialmente cometan errores. Las vulnerabilidades de ciberseguridad explotadas durante una transacción pueden presentar riesgos para el valor del acuerdo y el retorno de la inversión:

Riesgos a corto plazo

- Operaciones paralizadas como resultado de ransomware o malware.
- Los actores de amenazas pueden usar el período de transacción para ingresar y realizar un reconocimiento, un evento que a menudo no se detecta hasta mucho después de que se cierra el trato.
- Robo de información privilegiada, incluidas valoraciones, ofertas, etc.
- Reclamaciones de garantía, un cambio en los términos del acuerdo o una reducción en el valor del acuerdo.
- Investigaciones forenses relacionadas con una violación de datos.

Riesgos a largo plazo

- Exposición a riesgos derivados de demandas reglamentarias y otras.
- Investigación y sanciones reglamentarias.
- Pérdida de clientes, e impactos asociados en ventas y ganancias.
- Daño reputacional.
- Pérdida de participación de mercado ante competidores a los que no se les conoce una violación de datos.

Los directores deben solicitarle a la gerencia que realice una evaluación de riesgo cibernético para cada fase del ciclo de vida de la transacción para confirmar que los sistemas y procesos son seguros y para cuantificar los riesgos que pueden afectar a la compañía después del cierre de la negociación, incluidos los ingresos, las ganancias y el valor de mercado, participación en el mercado, y reputación de marca.

Estrategia y fase de identificación de objetivos

El riesgo de ataque comienza incluso antes de que se realice una oferta oficial o un anuncio de fusión. Los bufetes de abogados, asesores financieros, consultores y otras firmas asociadas son atractivos para los piratas informáticos porque mantienen secretos comerciales y otra información confidencial sobre clientes corporativos, incluidos los detalles sobre la exploración de negociación en la etapa inicial que podrían ser robados para notificar al tráfico con información privilegiada o para obtener una ventaja competitiva. Los ataques cibernéticos a firmas de abogados están aumentando a nivel mundial, lo que lleva a los abogados a etiquetar a los cibernéticos como una "amenaza existencial" para las empresas[57]. Por lo tanto, una empresa debe tener un entendimiento de los controles y la seguridad implementados por todos los terceros que lo asisten durante el proceso de fusiones y adquisiciones y una comprensión completa de cómo se compartirán los datos confidenciales entre las partes.

Los atacantes buscan indicios de que una compañía está considerando una fusión, adquisición o desinversión. Pueden ser alertados por chismes de la industria, una desaceleración en el ciclo de lanzamiento de una empresa, reducciones de personal o fuga de datos a través de los canales de las redes sociales. Hay cuatro formas principales en las que está en riesgo la información:

- Un pirata informático ingresa a la red a través de huecos en sus defensas, comenzando con las computadoras que trabajan con Internet en una empresa.
- Un hacker lanza un ataque de ingeniería social contra un empleado de la empresa.
- Los miembros de la empresa (empleados, contratistas, proveedores) liberan datos e información confidenciales, ya sea intencionalmente o como resultado de una negligencia. El riesgo de amenazas internas aumenta significativamente en las fusiones y adquisiciones.
- La información se expone a través de vulnerabilidades en proveedores externos o proveedores de servicios.

Durante esta fase, la gerencia debe comprender los riesgos cibernéticos asociados con la empresa objetivo y modelar el impacto de esos riesgos en la postura de cumplimiento, las previsiones financieras y las posibles valoraciones. La gerencia puede realizar el siguiente análisis incluso antes de que comience el compromiso directo con la empresa objetivo:

- Realización de búsquedas en "web profunda"58 (sitios web de difícil acceso preferidos por piratas informáticos) sobre el objetivo, sus sistemas, datos y propiedad intelectual. Esto ayuda a identificar si la compañía ya se encuentra en el radar de los piratas informáticos, si los sistemas o las credenciales ya están comprometidos, y si hay datos confidenciales para la venta o solicitados. La gerencia deberá considerar la legalidad de tales búsquedas con referencia a la información a la que se accede.
- Perfilación de la compañía objetivo desde el punto de vista de la ciberseguridad, mientras se implementa la tecnología relevante.
- Investigación de infecciones de malware en la empresa objetivo y brechas en sus defensas visibles desde el exterior. Esta información está disponible públicamente y puede usarse para comparar una compañía con otra, lo que le permite a la gerencia ahorrar tiempo y energía al no buscar compañías cuyo perfil de riesgo sea inaceptablemente alto.

- Modelización del impacto financiero de los riesgos cibernéticos identificados. Estos riesgos pueden no solo impactar el rendimiento de la compañía sobre el capital invertido, sino que también pueden resultar en la pérdida de ventajas competitivas, remediaciones costosas, multas y posiblemente años de litigios, dependiendo de lo que se robó. Una estimación inicial del impacto puede ser lo suficientemente material para alentar a los equipos de estrategia a alterar la trayectoria de una negociación. La estimación se puede refinar a medida que el proceso de transacción continúa y se mitigan los riesgos.

Diligencia debida y fases de ejecución del trato

Durante estas fases, la empresa debe realizar la debida diligencia de ciberseguridad confirmatoria. Los problemas importantes requerirían la negociación de una reducción en el precio de compra para cubrir los costos de la remediación necesaria. Dependiendo de los riesgos identificados, es posible que la junta desee postergar la aprobación de la transacción hasta que se complete la reparación o decida retirarse de la transacción si los riesgos que se identifican justifican dicha acción. La identificación de los riesgos de ciberseguridad durante la fase de diligencia se puede lograr realizando una diligencia de ciberseguridad que se adapte para descubrir estos riesgos:

- Identificar inversiones insuficientes en infraestructura de ciberseguridad, así como deficiencias en recursos de personal, políticas, etc.
- Identificar actitudes culturales laxas hacia el riesgo cibernético.
- Determinar los términos y condiciones relacionados con la ciberseguridad (o la falta de ellos) en los contratos con clientes y proveedores que tengan un impacto financiero potencial o que den lugar a un litigio por incumplimiento.
- Descubrir el incumplimiento de las leyes de privacidad de datos cibernéticos u otras regulaciones y requisitos aplicables.
- Identificar las violaciones de datos recientes u otros incidentes de ciberseguridad.

La debida diligencia efectiva en temas de ciberseguridad les demuestra a los inversionistas, reguladores y otras partes interesadas que la gerencia está buscando activamente proteger el valor y los impulsores estratégicos de la transacción, y que están apuntando a reducir el riesgo de un ataque cibernético antes de la integración. Luego, estos riesgos y ventajas se pueden tener en cuenta en el precio inicial pagado y en las inversiones para mejorar el rendimiento, que aumentarán el valor de la transacción. Esto permite presentar una propuesta de transacción sólida a los accionistas para su aprobación.

Fase de integración

La integración posterior a la negociación plantea una serie de desafíos relacionados con las personas, los procesos, los sistemas y la cultura. Los riesgos cibernéticos agregan otra dimensión de complejidad y riesgo a esta fase de la transacción. Los piratas informáticos aprovechan las inconsistencias que existen entre las plataformas y las operaciones tecnológicas de la empresa y la entidad recién fusionada o adquirida en esta fase.

Los equipos de integración deben tener la experiencia para explorar y profundizar en los detalles más pequeños para identificar y mitigar los riesgos cibernéticos, como los siguientes:

- Brechas de seguridad identificadas durante las fases anteriores.
- Priorización de las actividades de remediación basadas en el impacto potencial de las brechas identificadas.
- Priorización de actividades de integración.
- Formación de empleados en sistemas recién integrados.

Fase de creación de valor posterior a la transacción

Una vez que se completa una transacción, el monitoreo continuo de los riesgos cibernéticos por parte de la gerencia creará numerosas oportunidades para la mejora y el crecimiento de la cartera.

La gerencia debe continuar evaluando la madurez cibernética de la entidad fusionada o adquirida comparándola con los estándares de la industria y la competencia, tal como lo hacen con el negocio principal. La baja madurez podría afectar las proyecciones de crecimiento y la reputación de la marca debido a incidentes cibernéticos y posibles multas. Un incumplimiento o un problema de cumplimiento podría hacer que los reguladores investiguen, lo que podría ocasionar una pérdida financiera o un retraso en los planes de salida posteriores a la transacción. Los problemas cibernéticos también pueden llevar a acciones legales por parte de clientes y proveedores que causan pérdida de valor y menores rendimientos.

Una vista desde el lado de la venta

Por supuesto, muchos de los riesgos que afectan a la empresa adquirente y que se describen en este documento también se aplicarán al vendedor. En la fase de creación de la valoración posterior a la transacción, el vendedor está particularmente expuesto a las revelaciones de incumplimiento que pueden afectar el precio/momento de la transacción e incluso las operaciones en curso de la entidad vendedora si la transacción no se realiza. En consecuencia, una comprensión profunda de los vectores de riesgo existentes antes de la ejecución del acuerdo informará mejor a la naturaleza de las garantías otorgadas por la corporación vendedora y reducirá la exposición.

El flujo de información a los directores de las empresas vendedoras puede ser más limitado en su naturaleza y frecuencia a medida que pasa el tiempo después del anuncio del acuerdo y los directores deben establecer los umbrales y la naturaleza para cualquier comunicación de incumplimiento en el período posterior al anuncio.

Conclusión

La diligencia de ciberseguridad durante las fusiones y adquisiciones exige un enfoque doble. Las compañías deben llevar a cabo una diligencia debida rigurosa sobre los riesgos cibernéticos de la compañía objetivo y evaluar su impacto comercial relacionado a lo largo del ciclo de transacción para proteger el retorno de la inversión de la transacción y el valor posterior a la transacción de la entidad. Además, todas las partes involucradas en el proceso de acuerdo deben ser conscientes del mayor potencial de sufrir un ataque cibernético durante el proceso de transacción en sí y deben mantener diligentemente sus esfuerzos de ciberseguridad. La aplicación de este enfoque doble durante las fusiones y adquisiciones servirá para proteger, en última instancia, el valor de las partes interesadas.

APÉNDICE I

Métricas de ciberseguridad a nivel de junta

¿Qué métricas de ciberseguridad deben incluirse en una reunión informativa a nivel de junta? Esta pregunta es engañosamente simple. Al igual que virtualmente cualquier otra división y función dentro de la organización, la función de ciberseguridad recopila y analiza un gran volumen de datos y existe poco consenso sobre cuáles son los datos críticos que deben compartirse con el público de la junta. El desafío se suma al hecho de que la ciberseguridad es un dominio relativamente nuevo, con estándares y puntos de referencia que aún se están desarrollando o evolucionando.

En última instancia, los directores deberán trabajar con los miembros de la gerencia para definir la información de ciberseguridad, las métricas y otros datos que sean más relevantes para ellos, dado el entorno operativo de la organización, que incluye la industria o el sector, los requisitos regulatorios, la huella geográfica, etc. La mayoría de las veces, las juntas ven un alto volumen de métricas operativas que proporcionan muy poca información estratégica sobre el estado del programa de ciberseguridad de la organización. Las métricas que normalmente se presentan incluyen estadísticas como "número de ataques bloqueados", "número de vulnerabilidades no parcheadas" y otras medidas independientes orientadas al cumplimiento que brindan poco contexto estratégico sobre el desempeño de la organización y la posición de riesgo.

Como punto de partida, los directores pueden aplicar los mismos principios generales utilizados para otros tipos de métricas a nivel de la junta a los informes relacionados con la ciberseguridad (Véase la barra lateral, "Principios rectores para las métricas a nivel de la junta").

Además, las siguientes recomendaciones proporcionan un punto de partida para los tipos de métricas de ciberseguridad que los miembros de la junta deberían considerar solicitarle a la gerencia.

1. ¿Cuál es nuestro apetito de riesgo cibernético? Esta es una pregunta fundamental y una para la cual el Director de Seguridad de la Información (CISO) debe trabajar con la función de Director de Riesgos (CRO) para poderla contestar. Este tipo de colaboración puede producir puntos de datos cualitativos y cuantitativos para su presentación a la junta que brindan un contexto en torno al apetito de riesgo cibernético.

2. ¿Qué métricas tenemos que indican el riesgo para la empresa? Una organización ha implementado un "índice" de riesgo de ciberseguridad que incorpora varias métricas individuales que cubren la empresa, la cadena de suministro y el riesgo que enfrenta el consumidor.

3. ¿Cuánto de nuestro presupuesto de TI/tecnología se está gastando en actividades relacionadas con la ciberseguridad? ¿Cómo se compara esto con nuestros competidores/pares y/o con otros puntos de referencia externos? Estas métricas apoyarán las conversaciones sobre cómo determina la gerencia "cuánto gasto es suficiente" y si el aumento de las inversiones reducirá el riesgo residual de la organización. Las siguientes preguntas adicionales pueden ser:

- ¿Qué iniciativas no fueron financiadas en el presupuesto de este año? ¿Por qué?
- ¿Qué compensaciones se hicieron?
- ¿Tenemos los recursos adecuados, incluido el personal y los sistemas, y se están implementando de manera efectiva?

4. ¿Cómo medimos la efectividad del programa de ciberseguridad de nuestra organización y cómo se compara con los de otras compañías? Las métricas a nivel de junta deben resaltar los cambios, tendencias y patrones a lo largo del tiempo, mostrar el desempeño relativo e indicar el impacto. Las compañías de pruebas de penetración externas y los expertos externos pueden proporcionar una comparación de manzanas con manzanas dentro de los sectores de la industria.

5. ¿Cuántos incidentes de datos (por ejemplo, datos confidenciales expuestos) ha experimentado la organización en el último período de informe? Estas métricas informarán las conversaciones sobre tendencias, patrones y causas.

6. Las relaciones de la cadena de valor generalmente representan un riesgo mayor para las compañías dado el grado de interconexión del sistema y el intercambio de datos que ahora forma parte de las operaciones comerciales diarias. ¿Cómo evaluamos la posición de riesgo cibernético de nuestros proveedores, socios de emprendimientos conjuntos y clientes? ¿Cómo realizamos un seguimiento continuo de su postura de riesgo? ¿Cuántos proveedores externos se conectan a nuestra red o reciben datos confidenciales de nosotros? Esta es una métrica operacional límite, pero puede ayudar a respaldar las discusiones con la gerencia sobre el riesgo residual de terceros. Hay proveedores de servicios dentro del mercado de ciberseguridad que proporcionan un monitoreo pasivo y continuo de las posturas de ciberseguridad de las empresas. Un número creciente de empresas utilizan estos servicios para evaluar sus relaciones de terceros de alto riesgo, así como su propio estado de ciberseguridad.

7. ¿Qué métricas operacionales son rastreados y monitoreados rutinariamente por nuestro equipo de seguridad? Si bien las métricas operacionales son el dominio del equipo de TI/Seguridad, sería beneficioso para los directores comprender la amplitud y profundidad de las actividades de monitoreo de ciberseguridad de la compañía para los fines del conocimiento de la situación.

8. ¿Qué métricas utilizamos para evaluar el conocimiento de la ciberseguridad en toda la organización? Los datos sobre el cumplimiento de políticas, la implementación y la finalización de programas de capacitación y similares ayudarán a informar las conversaciones sobre los riesgos internos en diversos niveles de antigüedad y en diversas regiones y divisiones.

9. ¿Cómo hacemos un seguimiento de las personas o grupos que están exentos de las principales políticas de seguridad, monitoreo de actividades, etc.? Estas medidas indicarán las áreas donde la compañía está expuesta a riesgos adicionales, abriendo el camino para las discusiones sobre las compensaciones de riesgo/retorno en esta área.

Desarrollo de métricas económicas cibernéticas

El riesgo cibernético ahora se acepta como una conversación a nivel de la junta. Sin embargo, el desafío es cómo comunicarle, de manera efectiva y precisa, el impacto financiero de los incidentes cibernéticos a la junta. Antes de que las juntas puedan tomar decisiones informadas sobre cómo administrar el riesgo cibernético, primero deben tener la capacidad de traducir los datos de ciberseguridad en métricas financieras. Los directores de la junta deberán trabajar con la gerencia para delinear la información de ciberseguridad más relevante dado el entorno operativo de la organización, incluida la industria o el sector, los requisitos normativos, la huella geográfica, etc. Para comenzar, las siguientes recomendaciones de riesgo cibernético a nivel de junta proporcionan un punto de partida que las juntas deben considerar solicitarle a la gerencia:

- ¿Cuáles son nuestras métricas trimestrales de índice de pérdida esperada relacionadas con nuestra condición de riesgo cibernético en nuestras diferentes unidades de negocios y entornos operativos?

- ¿Cuál es el impacto financiero relacionado con nuestro peor escenario de riesgo cibernético?

- ¿Qué procesos hemos establecido relacionados con la toma de decisiones sobre la aceptación del riesgo cibernético, la solución del riesgo cibernético y la transferencia del riesgo cibernético? ¿Cómo medimos la manera en que estas decisiones reducen nuestra exposición financiera al riesgo cibernético?

- ¿Cómo estamos midiendo y priorizando nuestras actividades de control e implementación y los presupuestos de ciberseguridad frente a nuestra exposición financiera al riesgo cibernético? ¿Hemos conectado nuestra estrategia de implementación de control y los programas de ciberseguridad, incluidos los presupuestos, con nuestra estrategia de transferencia de riesgo cibernético?

- Según nuestros objetivos de desempeño financiero, ¿cómo puede el riesgo cibernético impactar nuestro desempeño financiero? ¿Cuál es nuestro valor anual de pérdida de riesgo cibernético esperado?

- ¿Cuál es nuestro plan de remediación de riesgo cibernético para alcanzar nuestro nivel de tolerancia de pérdida esperado? ¿Está nuestro plan produciendo un rendimiento financiero neto positivo?

- ¿Cómo alinea nuestro programa de ciberseguridad el análisis del índice de pérdida esperada basado en el riesgo cibernético y los objetivos de tolerancia de pérdida esperada? ¿Cómo estamos midiendo, rastreando y demostrando cómo nuestras inversiones en ciberseguridad están reduciendo nuestra exposición financiera a incidentes cibernéticos y entregando rendimiento de la inversión en ciberseguridad?

- ¿Cómo estamos midiendo y alineando nuestro análisis de índice de pérdida esperada basado en riesgo cibernético y la planificación de ciberseguridad con nuestro plan de transferencia de riesgo de seguro cibernético?

- ¿Cómo medimos la efectividad del programa de ciberseguridad de nuestra organización y cómo se compara con los de otras compañías?

Fuente: *Secure Systems Innovation Corporation (SSIC) and X-Analytics*

APÉNDICE J

Construcción de una relación con la gestión de la ciberseguridad y el equipo de seguridad

Hasta hace poco, la idea de un ejecutivo senior cuyos esfuerzos estaban dedicados a garantizar la ciberseguridad de la empresa era un concepto extraño para las empresas fuera del ámbito tecnológico. Los tiempos han cambiado. La alta gerencia dedicada, responsable de controlar el riesgo digital está aumentando en las medianas y grandes empresas en muchas industrias diferentes, una consecuencia de la realización de negocios en el mundo siempre conectado de hoy.

Según un estudio, el 54 por ciento de las empresas en todo el mundo emplean a un Director de Seguridad de la Información (CISO)[59]. Otra encuesta encontró que las organizaciones que contaban con un CISO tenían más probabilidades de tener equipos y planes dedicados a la respuesta a incidentes y tenían más confianza en la fuerza de las defensas de su compañía contra amenazas como el *malware*[60]. En América Latina, las organizaciones están comenzando a establecer un CISO dentro de sus organizaciones. Sin embargo, donde no hay un CISO, hay un equipo de seguridad que asume las responsabilidades de la ciberseguridad. La clave es que la junta desarrolla la relación con quienes lideran la ciberseguridad dentro de la organización. Es importante aclarar que el rol de un CISO y el equipo de seguridad no son los mismos tradicionalmente. Los CISO generalmente están asociados con la función de seguridad de la información como una segunda línea de defensa en la gestión y evaluación de los riesgos de la información, mientras que los equipos de ciberseguridad a menudo son la primera línea de defensa en la gestión de sistemas de TI directamente.

Construir las relaciones correctas entre el CISO o su equivalente y la junta es esencial. A medida que las funciones de seguridad de la información corporativa se vuelven más maduras, surge una nueva pregunta: ¿Cómo se comunica efectivamente la junta y la función de seguridad? El CISO o equivalente es responsable de administrar un riesgo operacional, reputacional y monetario significativo, por lo que es esencial una relación de confianza con la junta. Muchos miembros de la junta ahora buscan establecer una relación continua con el CISO e incluyen al ejecutivo de seguridad en una discusión sobre asuntos de ciberseguridad en reuniones de toda la junta y/o de comités clave. Durante estas reuniones informativas entre el CISO y la junta directiva, es importante que el equipo de gestión de riesgos cibernéticos esté plenamente representado ante la junta para mitigar los temores de castigos individuales por las vulnerabilidades de la ciberseguridad.

Las preguntas y pautas a continuación están diseñadas para ayudar a los directores a establecer o mejorar una relación con el CISO o equivalente. También pueden ayudar a los miembros de la junta a mejorar sus comunicaciones con el equipo de seguridad y ayudar a las juntas a obtener una mejor comprensión del enfoque general de la empresa en materia de ciberseguridad. Debido a que no todas las preguntas tendrán relevancia para todas las compañías, los directores deben seleccionar las que sean más adecuadas para los problemas y circunstancias a la mano.

1. Entienda el papel y el mandato del Equipo de Seguridad.

- ¿Cuál es el estatuto y el alcance de la autoridad del equipo de seguridad en términos de recursos, derechos de decisión, presupuesto, personal y acceso a la información? ¿Cómo se compara esto con las prácticas líderes en nuestra industria y en general?[61]

- ¿Cómo se determina el presupuesto de ciberseguridad de la organización? La comparación de esta cifra con las tendencias de gasto de la industria es probablemente la mejor manera de obtener un contexto sobre la suficiencia de la financiación. ¿Cuál es su tamaño (por ejemplo, el porcentaje del gasto total en TI/tecnología) y cómo se compara esta cifra con las prácticas líderes en nuestra industria y en general? ¿Qué papel juega el equipo de seguridad en la asignación del presupuesto de ciberseguridad y las decisiones de inversión? ¿Qué herramientas de seguridad u otras inversiones estaban por debajo de la línea de "corte" en el presupuesto?

- ¿Cuál es la relación de presentación de informes administrativos del equipo de seguridad (por ejemplo, los Directores de Información, Tecnología, Operación, Jefe de seguridad corporativa, otros)? ¿Se diferencia de la relación funcional de presentación de informes? ¿Qué protocolos se han implementado para garantizar que el equipo de seguridad tenga un canal independiente para escalar los problemas y proporcionar una divulgación rápida y completa de las deficiencias de la ciberseguridad?[62]

- ¿Qué papel desempeña el equipo de seguridad en la estructura de gestión de riesgos empresariales (ERM, por sus siglas en inglés) de la organización y en la implementación de los procesos de ERM?

- ¿Qué papel, si lo hay, desempeña el equipo de seguridad más allá de establecer y hacer cumplir las políticas de ciberseguridad y los sistemas de control relacionados?

  - Por ejemplo, ¿el equipo de seguridad proporciona información sobre el proceso de desarrollo de nuevos productos, servicios y sistemas o sobre el diseño de acuerdos de asociación y alianza, etc., de manera que la seguridad informática se "integra" en lugar de "agregarse" después del hecho?

- ¿El equipo de seguridad tiene las habilidades necesarias y la empresa puede atraer y retener el nivel necesario para ser eficaz?

- ¿Cómo se decide la división del riesgo? ¿Cómo se determina la postura de seguridad de la empresa, cómo se aprueba y con qué frecuencia se revisa?

- ¿Cuáles son los acuerdos existentes para poder ampliar el equipo de seguridad en caso de una crisis? ¿Tenemos las relaciones correctas con terceros adecuados?

2. Pase tiempo con el equipo de seguridad antes de que un incidente resulte beneficioso para otros.

- Una crisis es el momento equivocado para que los directores se familiaricen con el equipo de seguridad y el personal clave. Los miembros de la junta pueden hacer arreglos para visitar al equipo de seguridad y recibir orientaciones de primera mano del personal que se encuentra en la primera línea de la ciberseguridad. Podrían programar conjuntamente una reunión regular de la junta o una visita al sitio. Estas sesiones brindarán información valiosa y oportunidades de aprendizaje para los miembros de la junta. El equipo de seguridad también lo apreciará, ya que las visitas como esta pueden aumentar su visibilidad, elevar la moral y reforzar la necesidad de centrarse en esta área.

• Los directores también pueden solicitarle al ejecutivo de seguridad una evaluación de su situación de ciberseguridad personal, incluida la seguridad de sus dispositivos, redes domésticas, etc. Estas discusiones no solo son informativas para directores individuales, sino que también ayudarán a salvaguardar la información confidencial que reciben los miembros de la junta durante su servicio.

• Muchos equipos de seguridad producen informes internos de manera rutinaria para la gerencia y los altos líderes sobre tendencias e incidentes de ciberataques. Los directores pueden discutir con el equipo de seguridad, el secretario corporativo y los líderes de la junta si esta información puede ser relevante y útil para incluir en los materiales de la junta.

• Las juntas pueden sugerir una reunión trimestral o mensual con el personal clave de seguridad para acceder al estado actual de seguridad y exposición al riesgo. Las juntas deben entender que la seguridad está evolucionando y cambiando continuamente y, por lo tanto, las reuniones periódicas para evaluar el estado actual del perfil de riesgo de una organización proporcionan información sobre qué recursos son necesarios y dónde se debe prestar atención. Las juntas también deben solicitar que se realice una simulación o "ejercicio de mesa" de los planes de respuesta a incidentes al menos una vez al año.

3. Obtenga información sobre la red de relaciones del equipo de seguridad.

Dentro de la organización

• ¿Cómo colabora el equipo de seguridad de la información con otros departamentos y funciones corporativas en asuntos relacionados con la ciberseguridad? Por ejemplo, ¿El equipo de seguridad coordina con:

- Desarrollo de negocios con respecto a la diligencia debida en objetivos de adquisición y acuerdos de asociación;
- Auditoría interna sobre la evaluación y prueba de sistemas y políticas de control;
- Recursos humanos en capacitación de empleados y protocolos de acceso;
- Compra y cadena de suministro con respecto a los protocolos de ciberseguridad con proveedores, clientes y proveedores; y/o
- El área legal en cuanto al cumplimiento de las normas reglamentarias y de información relacionadas con la ciberseguridad y la privacidad de los datos?

El equipo de seguridad debe poder articular cómo la ciberseguridad no es solo un problema de tecnología; se trata de permitirle a la compañía implementar su estrategia de la manera más segura posible.

• ¿Qué apoyo recibe el equipo de seguridad del Director General, el Director de Informática y el equipo de alta gerencia?

• ¿Cómo desarrolla y mantiene el equipo de seguridad de la información el conocimiento de los objetivos estratégicos, el modelo de negocio y las actividades operativas de la organización?

- Por ejemplo, en las compañías que están buscando activamente una estrategia de "grandes datos" para mejorar el análisis de clientes y productos, ¿en qué medida el equipo de seguridad entiende la estrategia y contribuye a su ejecución segura?

- ¿Qué actividades de educación continuada realiza el equipo de seguridad de la información para mantenerse al día en cuestiones de ciberseguridad?

Fuera de la organización

- ¿El equipo de seguridad de la información participa en iniciativas de intercambio de información sobre ciberseguridad (por ejemplo, centradas en la industria, centradas en la comunidad de TI/tecnología o asociaciones público-privadas)? ¿Cómo se utiliza y comparte la información que se obtiene de la participación en tales iniciativas dentro de la organización?

- ¿El equipo de seguridad de la información tiene relaciones con partes interesadas del sector público, como agencias de aplicación de la ley y divisiones de ciberseguridad de las agencias reguladoras?

4. Evalúe el rendimiento.

- ¿Cómo se evalúa el desempeño del equipo de seguridad? ¿Cómo se evalúa el desempeño del equipo de seguridad de la información? ¿Quién realiza estas evaluaciones y qué métricas se utilizan?

- ¿Qué medidas e hitos de rendimiento de ciberseguridad se han establecido para la organización en su conjunto? ¿Utilizamos un enfoque basado en el riesgo que proporciona un mayor nivel de protección para los activos más valiosos y críticos de la organización?

- ¿Hasta qué punto se integran las actividades de evaluación y gestión de riesgos cibernéticos en los procesos de gestión de riesgos de toda la empresa? ¿Estamos utilizando la ciberseguridad adecuada para evaluar la higiene de la ciberseguridad desde una perspectiva de toda la organización?

5. Involucre a la infraestructura de seguridad en la discusión sobre el "estado de la organización".

- ¿Cuál fue el incidente de ciberseguridad más importante de la organización durante el último trimestre? ¿Cómo se descubrió? ¿Cuál fue nuestra respuesta? ¿Cómo se compara la velocidad de detección y recuperación con la de incidentes anteriores? ¿Qué lecciones aprendimos y cómo se incluyen en los esfuerzos de mejora continua de la organización?

- ¿Cuál fue nuestro "casi incidente" más significativo en ciberseguridad en el último trimestre? ¿Cómo se descubrió? ¿Cuál fue nuestra respuesta? ¿Qué lecciones aprendimos y cómo se incluyen en los esfuerzos de mejora continua de la organización?

- ¿Dónde hemos logrado el mayor progreso en ciberseguridad en los últimos seis meses y a qué factor (es) es (son) atribuible (s) a ese progreso? ¿Dónde quedan nuestras brechas más significativas y cuál es nuestro plan para cerrar esas brechas?

Principios rectores para presentar a la junta sobre ciberseguridad

Como la gerencia trabaja con las juntas directivas en materia de ciberseguridad, es fundamental que la ciberseguridad sea comunicada adecuadamente a la junta. Para utilizar de manera efectiva los siguientes apéndices, la gerencia debe tener en cuenta estas características al presentar información sobre ciberseguridad a la junta. Esta debe:

- Ser relevante para la audiencia (toda la junta; comité clave);
- Ser fácil de leer: use resúmenes, rótulos, gráficos y otros elementos visuales; evite la jerga técnica;
- Transmitir significado: comunique conocimientos, no solo información;
    - Resalte cambios, tendencias, patrones en el tiempo;
    - Muestre el desempeño relativo a los pares, promedios de la industria, otros indicadores externos relevantes, etc.
    - Indique el impacto en las operaciones comerciales, costos, participación de mercado, etc.;
- Se concisa: Evite la sobrecarga de información.

Por encima de todo, permita la discusión y el diálogo.

Acerca de los colaboradores

Internet Security Alliance

La Alianza por la Seguridad en Internet (Internet Security Alliance, ISA) es una asociación de comercio internacional, fundada en 2000, que se centra exclusivamente en la ciberseguridad. La junta de ISA está formada por el personal principal de ciberseguridad de empresas internacionales, que representa a prácticamente todos los sectores de la economía. La misión de ISA es integrar la economía con la tecnología avanzada y la política del gobierno para crear sistemas cibernéticos seguros y sostenibles. En 2014, ISA produjo el primer Manual de Supervisión de Riesgo Cibernético, que aborda específicamente el rol único que desempeñan las Juntas Corporativas en la gestión del riesgo cibernético. En su Encuesta Mundial sobre el Estado de la Seguridad de la Información, PricewaterhouseCoopers (PwC) informó que el manual fue ampliamente adoptado por las juntas corporativas y que su uso dio como resultado un mejor presupuesto de ciberseguridad, una mejor gestión del riesgo cibernético, una alineación más estrecha de la ciberseguridad con los objetivos comerciales generales y una ayuda para crear una cultura de seguridad en las organizaciones que la utilizan. Para obtener más información sobre ISA, visite www.isalliance.org.

Notas a pie de página

1. https://www.swiftinstitute.org/wp-content/uploads/2017/10/SIWP-2016-004-Cyber-Threat-Landscape-Carter-Final.pdf
2. https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean
3. https://www.sites.oas.org/cyber/Certs_Web/OAS-Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf
4. https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf?UWqJEbDm.dBKSLEIFTyYs1IxJaExh9Y7
5. Foro Economico Mundial, **"Advancing Cyber Resilience Principles and Tools for Boards"**
6. https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean
7. https://www.oas.org/es/sms/cicte/cipreport.pdf
8. Verizon RISK Team, et al., **2013 Data Breach Investigations Report,** March 2013.
9. https://www.cyberscoop.com/apt-c-36-blind-eagle-colombia/
10. Nicole Perlroth, **"Hackers Lurking in Vents and Soda Machines,"** *the New York Times*, Apr. 7, 2014.
11. Steve Morgan, **"Cyber Crime Costs Projected to Reach $2 Trillion by 2019,"** *Forbes*, Jan. 17, 2016.
12. Ibid.
13. http://aldianews.com/articles/culture/unknown-consequence-latin-americas-tech-boom/55104
14. http://www.seguridadinternacional.es/?q=es/content/cybersecurity-challenges-latin-america
15. https://www.trendmicro.com/en_ae/about/newsroom/press-releases/2015/trend-micro-partners-with-rmeducation-to-bring-worry-free-secur21221111111212.html
16. https://www.symantec.com/security-center/threat-report
17. https://www.threatmetrix.com/info/q1-2018-cybercrime-report/
18. Limor Kessem, **"2016 Cybercrime Reloaded: Our Predictions for the Year Ahead,"** Jan. 15, 2016.
19. FireEye Inc, **Mandiant M-Trends 2016**, p. 4.
20. Kessem, **"2016 Cybercrime Reloaded."**
21. Jeff Goldman, **"48 Percent of Companies Don't Inspect the Cloud for Malware,"** *eSecurity Planet (blog)*, Oct. 12, 2016.
22. Thor Olavsrud, **"Companies complacent about data breach preparedness,"** *CIO*, Oct. 28, 2016.
Eset, Latin American Security Report (2017)
23. http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf
24. Mark Smith, **"Huge rise in hack attacks as cyber-criminals target small business,"** *The Guardian*, Feb. 8, 2016.
25. Estudio del BID
26. AFCEA Cyber Committee, **The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment,** 27. October 2013. See also: Internet Security Alliance, **Sophisticated Management of Cyber Risk** (Arlington, VA: Internet 28. Security Alliance, 2013).
27. AFCEA Cyber Committee, **The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment,** October 2013.
28. https://www.oas.org/es/sms/cicte/cipreport.pdf
29. Internet Security Alliance and American National Standards Institute, The Financial Management of Cyber Risk: An Implementation Framework for CFOs, 2010.
30. NACD, et al., **Cybersecurity: Boardroom Implication** (Washington, DC: NACD, 2014) (an NACD white paper).
31. Ibid. See also: KPMG Audit Committee Institute, Global Boardroom Insights: The Cyber Security Challenge, Mar. 26, 2014.
32. NACD, **Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward** (Washington, DC: NACD, 2009).
33. Adaptado de Robyn Bew, **"Cyber-Risk Oversight: 3 Questions for Directors,"** Ethical Boardroom, Spring 2015.
34. Sección 174 de la Ley de Sociedades 2006
35. https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean
36. https://www.lexology.com/library/detail.aspx?g=c0701531-2665-4e4b-a87b-00434e25d55f
37. Regulación (EU) 2016/679 [NB: *Este párrafo ha sido escrito como si el GDPR estuviera vigente. La fecha de vigencia es mayo de 2018.*]

38. https://www.atkearney.com/documents/783760/869855/Governance+practices+of+Corporate+Boards+in+Latin+America.pdf/f5ae6de9-86e6-9999-8e9d-2fa4cc8e913d?version=1.0
39. NACD, **2016-2017 NACD Public Company Governance Survey** (Washington, DC: NACD, 2016), p. 26.
40. NACD Audit Committee Chair and Risk Oversight Advisory Councils, **Emerging Trends in Cyber-Risk Oversight**, July 17, 2015, p. 1.
41. NACD, et al., **Cybersecurity: Boardrooms Implications** (Washington, DC: NACD, 2014) (an NACD white paper), p. 3.
42. NACD, **2016-2017 NACD Public Company Governance Survey** (Washington, DC: NACD, 2016), p. 28.
43. Ibid.
44. Sean Martin, **"Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's Serious,"** *International Business Times*, April 16, 2014.
45. Andrea Bonime-Blanc. **"Cyber-Reputation: Risk Turbocharged"**. *Ethical Corporation Magazine*. March 2016.
46. Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness (Washington, DC: NACD, 2010), p. 7.
47. Las citas en cursiva son de participantes en la Global Cyber Summit, celebrada del 15 al 16 de abril de 2015, en Washington, DC. Las discusiones se llevaron a cabo bajo la Regla de Chatham House,
48. Lexology.com, Ed Batts, DLA Piper LLP, **"Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members,"** Jan. 23, 2014.
49. Ibid.
50. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, **"Board Oversight."**
51. Ibid.
52. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "**Board Oversight."**
53. Lexology.com, Ed Batts, DLA Piper LLP, **"Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members,"** Jan. 23, 2014.
54. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, **"Board Oversight."**
55. Ibid.
56. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, **"Board Oversight."**
57. https://www.law.com/international/2018/04/27/cyberattacks-geopolitical-shocks-and-global-competition-what-keeps-law-firm-leaders-up-at-night-396-2954/?slreturn=20180728162144
58. La Web Profunda es un término general que describe los sitios ocultos de Internet a los que los usuarios no pueden acceder sin usar un software especial como TOR (*The Onion Router, en inglés*). Si bien se puede acceder al contenido de estos sitios, los editores de estos sitios están ocultos. Los usuarios acceden a la web profunda con la expectativa de poder compartir información y/o archivos con poco riesgo de detección.
59. PwC, **Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016** (New York, NY: PwC, 2015), p. 26, and see Paul Solman, **"Chief information security officers come out from the basement,"** Financial Times, Apr. 29, 2014.
60. Kris Monroe, **"Why are CISOs in such high demand?"** Cyber Experts Blog, Feb. 8, 2016.
61. Véase, por ejemplo, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment (Armonk, NY: IBM Center for Applied Insights, 2014).
62. Un estudio de 2014 sobre problemas de seguridad de la información global encontró que las organizaciones con CISO que informan fuera de la oficina del Director de Informática tienen menos tiempo de inactividad y menos pérdidas financieras relacionadas con los incidentes de ciberseguridad en comparación con aquellos que informan directamente al Director de Informática. Véase Bob Bragdon, "**Maybe it really does matter who the CISO reports to,"** *The Business Side of Security (blog)*, June 20, 2014.

MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS

MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS