La ciberseguridad y el cambiante rol de las juntas directivas:

De ofrecer supervisión a dar ejemplo

Jeffry Powell
Vicepresidente ejecutivo, Las Americas

Charlie Horrell
Director gerente para Europa, Medio Oriente y África

Al Percival
Director ejecutivo, Australia y Nueva Zelanda

Brian Locke
Director de seguridad

En una época en la que con frecuencia el hurto de la información de clientes conduce a reestructuraciones en las gerencias, las juntas directivas desempeñan un rol cada vez mayor a la hora de evaluar la idoneidad de la ciberseguridad en sus organizaciones.

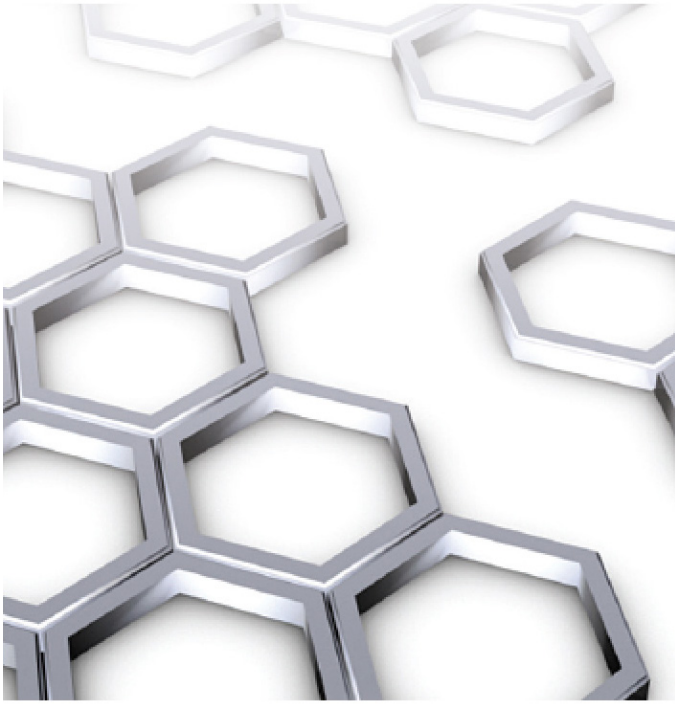
Pero muchas juntas directivas aún deben aplicar un examen igual de exhaustivo a su propia seguridad. Este artículo ofrece un marco para la evaluación por parte de los directores y la alta gerencia. La atención se centra en tres principales factores: dónde se almacenan los datos, la fortaleza de la protección que proporciona acceso y el control de las "claves" de acceso.

El compromiso de los líderes con la ciberseguridad no se impulsa solo desde adentro. Los entes reguladores también han empezado a elevar las expectativas. Por ejemplo, en los Estados Unidos la Comisión de Bolsa y Valores ha reafirmado la importancia de incluir procesos y eventos de ciberseguridad en la divulgación de factores de riesgo y eventos concretos.[1] Y aunque esta normativa puede no ser aplicable a empresas de capital privado y organizaciones sin fines de lucro, está sujeta a estrictos estándares por parte de sus propietarios, socios y donantes

A pesar de la responsabilidad de la junta directiva de supervisar la ciberseguridad, con frecuencia se pasa por alto un enlace clave en la cadena de la ciberseguridad: el rol de la junta directiva como custodio de la información de la empresa. Después de todo, como parte de su rutina, una junta directiva maneja, almacena y comparte internamente información confidencial, como es el caso de la información financiera, de ventas, planes estratégicos, políticas de compensación de altos ejecutivos y otra información privilegiada. El acceso no autorizado a esta información podría traer graves consecuencias.

El problema es que la posición de la junta directiva "por encima" de la organización significa que a menudo esta queda excluida de sus propios procesos. Como resultado, cuando el director de información examina las necesidades de ciberseguridad de la empresa, este podría, con razón,

Diligent



pensar que la seguridad de la junta directiva es un asunto que corresponde al secretario corporativo o al abogado general. Podría suponerse que la ciberseguridad a nivel de la junta directiva está fuera del dominio del director de información.

A ello se suma el hecho innegable de que todas las opciones de ciberseguridad implican un equilibrio entre la conveniencia y la efectividad. Debido al estatus de mayor categoría de los miembros y líderes de la junta directiva, existe una tendencia natural de estos a minimizar los inconvenientes de su parte. Como resultado, los miembros de la junta directiva con frecuencia eligen acceder a la información, almacenarla y compartirla en formas que pueden ser convenientes, pero que son considerablemente menos seguras que la manera en que procede la organización en su totalidad. Ello incluye el envío de paquetes de material de juntas directivas en documentos impresos, o el envío por correo electrónico de documentos PDF.

Otro caso en que se expresa el mencionado equilibrio es cuando se requieren contraseñas. En lugar de exigir la creación de contraseñas seguras que contengan palabras no reconocibles, formadas por una combinación de diferentes tipos de caracteres, pueden permitirse contraseñas simples, como el nombre de un niño. Mientras estas prácticas a menudo surgen de decisiones provisionales, más que ser producto de una política deliberada, son, sin embargo, resistentes al cambio debido a la inercia.

Dado el elevado nivel de riesgo en la actualidad, las juntas directivas y la alta gerencia deben hacer más que proporcionar supervisión de la ciberseguridad en una organización. Deben dar el ejemplo de las mejores prácticas de seguridad desde las más altas posiciones.

UN MARCO PARA EVALUAR LA SEGURIDAD DE LA JUNTA DIRECTIVA

Los líderes que desean tener una comprensión firme e intuitiva acerca de cómo juzgar las prácticas de ciberseguridad de su junta directiva pueden fácilmente terminar confundiéndose con el lenguaje especializado. Por fortuna, sin embargo, ello se puede corregir fácilmente a través de tres preguntas básicas:

1 ¿Cómo se almacena la información de la junta directiva?

2 ¿Qué tan fuertes son las defensas?

3 ¿Quién controla las claves?

Plantear estas preguntas puede contribuir a evaluar las soluciones actuales de la junta directiva respecto a la información que se comparte, las comunicaciones y la colaboración, así como de cualquier otro aspecto que esta considere.

¿Cómo se almacena la información de la junta directiva?

Una evaluación de la seguridad debería comenzar por examinar quién controla la información. No saber dónde está la información y carecer de la capacidad de controlar hacia dónde va, significa que la solución es extremadamente insegura.

Es por ello que enviar por correo electrónico documentos de junta directiva como archivos PDF no constituye una solución segura. Los archivos pueden ser reenviados accidentalmente por directores a personas que están fuera de la junta directiva, o guardados en cuentas personales de correo electrónico con mínimos niveles de seguridad.

Lo mismo es aplicable a los sistemas públicos para compartir archivos, en los que estos se almacenan “en la nube”. Lo que ello realmente significa es que sus archivos podrían estar en cualquier servidor en la red para compartir archivos; usted como cliente no tiene manera de saber con exactitud dónde están. Esta nebulosidad es la razón por la cual se le llama “nube” en primer lugar. Una razón para la popularidad entre los consumidores de los sistemas de almacenamiento basados en la nube, ha sido la suposición de que dichos sistemas son relativamente seguros. Pero casos importantes de ataques informáticos, tales como la revelación de contraseñas y de fotografías de celebridades por parte de proveedores de servicios de la nube,[2] demuestran cuán falsa es esta creencia.

Si bien los portales para juntas directivas alojados parecieran formar parte de la nube, y frecuentemente se les denomina de manera errónea “almacenamiento basado en la nube”, existen grandes diferencias. Para empezar, estos controlan de manera cuidadosa que sus datos se almacenen en el sistema de alojamiento. Además, estos almacenan la información de cada organización de manera independiente. Conocer la ubicación de los datos, así como las medidas de seguridad de protección, permite mayor control y seguridad sobre quién tiene acceso a la información.

¿Qué tan fuertes son las defensas?

Vigilar la ubicación donde residen los datos es tan importante como asegurar que solo los usuarios autorizados puedan tener acceso a estos datos. Esto es posible a través del cifrado; es decir, codificar los datos para convertirlos en una cadena de insignificantes 0 y 1. Solo quienes posean la clave digital correcta podrán descifrarlos.

Desde luego, los conjuntos de documentos impresos de las juntas directivas no tienen clave digital alguna, por lo que cualquier persona que logre obtenerlos podrá leerlos sin dificultad alguna. Además, si bien pudiera ser cierto que los PDF enviados por correo electrónico o almacenados en sistemas para compartir archivos pueden cifrarse y estar protegidos con contraseñas, la verdad es que toda la responsabilidad recae sobre quien distribuye y recibe el material para administrar los protocolos de contraseña. Adicionalmente, los documentos "protegidos" de esta manera siguen siendo vulnerables a los ataques perpetrados mediante "fuerza bruta" a través de productos de software fácilmente accesibles.

Los portales para juntas directivas de mayor calidad por lo general utilizan un cifrado de 256 bits; es decir, una clave de 256 ceros (0) y unos (1). Debido a que el número de combinaciones posibles es mayor que la cantidad de estrellas que tiene el universo, con seguridad se puede afirmar que incluso los criminales informáticos más avezados utilizando la tecnología más avanzada tardarían una eternidad para quebrantar el código.

¿Quién controla las claves?

Sin importar lo fuerte que sea el sistema de cifrado, cualquiera con la clave correcta podrá acceder a la información. Por ejemplo, cualquier persona que tenga la contraseña de un PDF protegido por contraseña es el propietario virtual del documento. Contraseñas robadas se traduce en documentos robados.

Sin embargo, con un portal para juntas directivas alojado, la contraseña no irá más lejos. Sí, es cierto que permite acceso al portal. Pero debido a que el control de las claves de cifrado que protegen los documentos de las juntas directivas reside dentro del sistema, la persona que inicie sesión solo podrá ver lo que tenga permitido. Un portal fuerte nunca pierde el control de los documentos.

Las implicaciones de seguridad son significativas. Si una contraseña es objeto de hurto, el administrador puede negar el acceso a dicha contraseña.

Considerando el acrecentado nivel de las amenazas en estos tiempos, las juntas directivas y los directores deben hacer más que supervisar la ciberseguridad de una organización. Deben dar el ejemplo de las mejores prácticas de seguridad desde las más altas posiciones.

Además, después de que ya no sean necesarios los documentos confidenciales, el administrador puede realizar "una depuración virtual", al aislar los documentos de cualquiera que intente acceder a dicha cuenta de usuario con la contraseña hurtada.

Más allá de la protección que brinda necesitar la contraseña correcta para obtener acceso, el administrador de una junta directiva puede limitar el acceso a documentos específicos de la junta directiva según criterios, tal como pertenecer a un comité, lo que permitiría, por ejemplo, que solo los miembros de los comités de auditoría o compensación puedan ver los documentos. El administrador también puede controlar desde cuál dispositivo específico un director puede acceder al sistema.

1 " CF Disclosure Guidance Topic No. 2: Cybersecurity," U.S. Securities and Exchange Commission Division

2 *Wall Street Journal*, "Apple Denies iCloud Breach: Tech Giant Says Celebrity Accounts Compromised by 'Very Targeted Attack,'"Septiembre 2 de 2014. **http://online.wsj.com/articles/apple-celebrityaccounts-compromised-by-very-targeted-attack-1409683803**

EL MENSAJE CORRECTO PROVIENE DE LA ALTA DIRECCIÓN

Si bien la ciberseguridad puede ocupar un lugar permanente en las agendas de las juntas directivas y la alta gerencia en un número cada vez mayor de organizaciones, ello no es suficiente. La seguridad también debe ser una parte permanente de la conducta de las juntas directivas.

Contar con la plataforma adecuada para administrar la información, las comunicaciones y la colaboración de las juntas directivas asegurará que en las salas de conferencia se sigan las prácticas de seguridad esenciales. También envía el mensaje correcto; es decir, la ciberseguridad es del interés de todos.

Diligent

Aprovechando el valor de la información. Con seguridad.

Diligent ayuda a las principales organizaciones del mundo a aprovechar, con seguridad, el poder de la información y la colaboración al ofrecer la tecnología necesaria para que sus juntas directivas y equipos de administración tomen mejores decisiones. Más de 3.100 clientes en más de 50 países confían en Diligent para obtener acceso inmediato a su información más urgente y confidencial, junto con las herramientas para revisar, discutir y colaborar con dicha información con los encargados clave de tomar las decisiones. La solución Diligent Boards (anteriormente Diligent Boardbooks) acelera y simplifica la manera en que se produce y entrega el material de la junta directiva a través de iPad, dispositivos Windows y navegadores. Al mismo tiempo, ofrece ventajas prácticas como reducir gastos de producción, respaldar las metas de sostenibilidad y ahorrar tiempo en los departamentos administrativo y de TI.

Visítenos en www.diligent.com y busque nuestro símbolo DIL en la Bolsa de Valores de Nueva Zelanda.