La seguridad informática de la junta directiva:

De preferencias arriesgadas a políticas sensatas

Debido al aumento y mayor nivel de sofisticación de los ataques a la seguridad informática, los directores corporativos deben dar prioridad a la seguridad de sus comunicaciones. Las juntas directivas deberían incorporar estrategias y normativas de seguridad informática en sus directrices para establecer con claridad qué es y qué no es aceptable comunicar y descargar, así como con quién hacerlo y, lo más importante, cómo hacerlo. Los directores deberían dar el ejemplo y mantener su adhesión a través de capacitaciones y auditorías.

El riesgo de la seguridad informática no es un concepto nuevo para las juntas directivas en 2017, ni tampoco lo son la amenaza de que un teléfono inteligente corporativo caiga en las manos equivocadas, ni las concepciones erróneas de que el correo electrónico y el almacenamiento de datos interno son seguros, y de que la protección mediante contraseña es igual a seguridad.[1]

Los titulares de prensa siguen enfatizando los riesgos en materia de leyes, reputación y competencia presentes en una filtración o fuga de datos. En octubre de 2016, la filtración de un correo electrónico y una presentación de la junta directiva de Salesforce compartieron con el mundo una lista de las potenciales adquisiciones objetivo de la empresa.[2] En marzo de 2017, las autoridades arrestaron a un lituano que obtuvo más de 100 millones de dólares al estafar a dos empresas de tecnología estadounidenses. Su método de ataque: enviar comunicaciones electrónicas que lucían como mensajes provenientes de un famoso fabricante chino.[3]

1 “La amenaza cibernética y la seguridad de la junta directiva: Tres ideas erróneas que menoscaban la seguridad de la sala de reuniones de la junta directiva”

2 http://www.businessinsider.com/leaked-salesforce-email-adobe-acquisition-list-2016-10

3 https://www.theguardian.com/technology/2017/mar/22/phishing-scam-us-tech-companies-tricked-100-million-lithuanian-man

Diligent

Legisladores y entes reguladores están respondiendo a estas amenazas cada vez más frecuentes. El Estado de Nueva York, por ejemplo, ahora requiere que todas las firmas de servicios financieros que hacen negocios dentro del estado (y todas las empresas que sostengan relaciones comerciales con estas) cuenten con planes de seguridad informática que abarquen todo, desde el rastro de auditoría hasta el acceso a los datos de los clientes, con la aprobación de la junta directiva.[4] Además, las recientes demandas que involucran a Target y Wyndham Worldwide revelan la incapacidad de implementar controles adecuados para la protección de datos como una potencial infracción de la responsabilidad fiduciaria de los directores.[5]

Como consecuencia, los directores han estado considerando implementar la seguridad en toda la empresa. No obstante, las propias comunicaciones de los directores no reflejan esta creciente concientización. De acuerdo con una encuesta realizada en 2017 por NYSE Governance Services, el 92 % de los más de 380 directores encuestados expresó una preferencia por el uso de cuentas de correo electrónico personales. Casi el 60 % admitió enviar regularmente comunicaciones de su junta directiva a través de cuentas de correo electrónico personales, como Google, Yahoo y Hotmail. Para resaltar las vulnerabilidades de seguridad aún más, el 22 % respondió que habitualmente almacena el material de su junta directiva en unidades de almacenamiento personales o externas.

A pesar del reciente auge de la concientización y educación, para las juntas directivas sigue siendo un reto estar al tanto de los problemas relacionados con la seguridad informática y los riesgos, en toda la empresa y en sus propias actividades. En una encuesta realizada en 2017 por Harvard Business School y Women Corporate Directors Foundation, solo el 24 % de los directores respondió que calificaría la seguridad informática en sus propias actividades como “por encima del promedio o excelente”.[6]

¿Cómo pueden las juntas directivas comenzar a reducir esta brecha? Una manera sería a través de sus normas y políticas de gobernanza.

INTEGRACIÓN DE LA SEGURIDAD DE LAS COMUNICACIONES EN LA GOBERNANZA DE LA JUNTA DIRECTIVA

Las políticas y normas de las juntas directivas cubren numerosos asuntos, tales como conductas financieras, aceptación de dádivas, confidencialidad y divulgaciones. Estas políticas con frecuencia incluyen reglas para las comunicaciones, que abarcan desde especificar lo que se puede comunicar entre los directores (p. ej. nada de solicitudes de ofertas ni sondeos de opinión) hasta cómo deberían producirse las comunicaciones con miembros de los medios y del público.

En el mundo actual de intensificación de riesgos y consecuencias, la seguridad informática debe formar parte de estas directrices. La normativa del estado de Nueva York recomienda que las políticas abarquen el acceso a los datos y la privacidad en torno a éstos, la gestión de identidades, el control de sistemas y redes, la continuidad del negocio, y más.[7]

¿Qué debería considerar para su propia política en su próxima reunión de comité, gobernanza o directores? Basándonos en nuestra experiencia con miles de juntas directivas corporativas en todo el mundo, en Diligent recomendamos:

RECEPCIÓN Y ENVÍO DE MENSAJES

Directores, asesor general, altos ejecutivos: ¿quiénes deberían enviar y recibir comunicaciones de la junta directiva y quiénes no? Estipule esto en detalle en sus directrices y establezca políticas para el envío y la recepción de archivos adjuntos, la retención y el archivo de mensajes y la eliminación remota de las comunicaciones en un dispositivo extraviado o hurtado. A continuación, refuerce la adhesión usando tecnologías como Diligent Messenger, que cierra el círculo, lo que impide que se produzcan envíos accidentales, p. ej.: al completar automáticamente la dirección de correo electrónico incorrecta en el campo de destinatario de un correo electrónico.

Debido al aumento de los correos electrónicos de suplantación de identidad en los ataques informáticos, las directrices también deben prohibir de manera explícita las respuestas de partes no autorizadas. Incluso las aplicaciones más seguras de mensajería para juntas directivas pueden no ser 100 % a prueba de las técnicas cada vez más sofisticadas de ataque informático.

El delincuente informático lituano que engañó a empresas de tecnología para que le enviaran 100 millones de dólares es solo un ejemplo. Otra estrategia de ataque reciente induce a la víctima a abrir un correo electrónico al piratear la “dirección de remitente” de un contacto de confianza. El destinatario llegará luego a una pantalla de inicio de sesión falsa (aunque convincente). En este punto, los atacantes capturan información sobre nombre y contraseña para acceder a la bandeja de entrada del destinatario.[8]

Por último, defina con exactitud lo que significa “comunicaciones oficiales de la junta directiva”. Algunos elementos, como las minutas, constituyen información más evidentemente confidencial, ¿pero dónde quedan las invitaciones a reuniones y agendas, o los correos electrónicos personales entre directores? Especifíquelo con claridad en su política de seguridad de las comunicaciones.

MANEJO DE ARCHIVOS ADJUNTOS

Cuando un empleado de Boeing reenvió una hoja de cálculo a su esposa para que lo ayudara con el formato, simultáneamente expuso los nombres, las fechas de nacimiento y los números de seguridad social de 36.000 empleados a un riesgo de seguridad.[9]

Además de establecer lo que se debe y no se debe hacer a la hora de enviar y recibir mensajes, su política para las comunicaciones debe incluir la transmisión de archivos electrónicos. Los archivos relacionados con las actividades de la junta directiva jamás se deben enviar a través de métodos no seguros sin cifrado, y solo se deben enviar a los usuarios autorizados. Especifique en detalle exactamente quiénes son estos usuarios autorizados.

Su política también debe especificar los tipos de archivos que pueden y no pueden descargar los directores. En el actual clima de suplantación de identidad, malware, así como de freeware y

4 http://fortune.com/2017/03/01/cyber-regulations-new-york

5 https://iapp.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors/

6 https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

7 https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf

8 http://fortune.com/2017/01/18/google-gmail-scam-phishing/

9 http://www.bizjournals.com/seattle/news/2017/02/28/boeing-discloses-36-000-employee-data-breach.html

shareware sospechosos, "lo que pareciera una descarga inocua para fines de trabajo puede fácilmente introducir un virus en su red y exponer datos confidenciales de negocios", escriben los expertos en seguridad informática de Sentek Global para la revista *Entrepreneur*.[10] Su equipo de seguridad informática interno o externo debe estar en capacidad de proporcionar orientación a tal respecto.

ARCHIVO Y RETENCIÓN DE COMUNICACIONES

Guardar minutas o un documento de fusiones y adquisiciones en una unidad de disco duro de una computadora portátil, o mantener un archivo sólido de correos electrónicos por varios años pueden ser "trucos prácticos" para ahorrarle tiempo a un director ocupado cuando está de viaje. Sin embargo, esta práctica supone una vulnerabilidad significativa para su junta directiva si los dispositivos llegaran a ser objeto de extravío o hurto o si agentes maliciosos llegaran a comprometer una bandeja de entrada de correo electrónico.

Estipule en la política de su junta directiva el tipo de material que tienen los directores permitido descargar, además de los teléfonos inteligentes, las tabletas, las computadoras y los software específicos que pueden utilizar. En tiempos en que los dispositivos personales y las bandejas de entrada se admiten como evidencia electrónica, y que un director puede recibir una citación personal si la empresa se somete a litigio, la normativa en relación con las comunicaciones de la junta directiva debe cubrir todos los aspectos relevantes. ¿Cómo deben asegurarse estos dispositivos? ¿Se les exigirá a los directores que eliminen archivos o correos electrónicos históricos después de cierto período de tiempo?

Esta parte de su política también debe proporcionar orientación en caso de que ocurran eventos adversos. En la situación de Boeing, la empresa realizó una investigación forense de ambos dispositivos a fin de garantizar la destrucción de todas las copias conocidas de la hoja de cálculo, seguida de una carta de notificación para todas las partes afectadas (con una oferta de dos años de supervisión de crédito gratuita) y capacitación adicional para sus empleados sobre el manejo de información personal.

¿A quién se deben notificar los incidentes? ¿A través de qué medios se deben borrar los datos de los dispositivos, y de qué manera se demostrará que dichas medidas fueron efectivas?

Su equipo de seguridad informática interno o externo debe estar en capacidad de ofrecer orientación sobre detalles técnicos específicos, como almacenamiento seguro, cifrado de datos, autenticación de identidad y control de acceso mediante administrador.

FOMENTO DE LA ADHESIÓN

El primer paso es la implementación de reglas correctas, y lo puede hacer en su próxima reunión de comité o de junta directiva. Lograr que estas reglas funcionen requiere de un proceso constante.

Para incrementar las probabilidades de éxito, cuente con una solución tecnológica que se ajuste a sus directrices. Diligent recomienda un sistema seguro y controlado de mensajería de circuito cerrado que se integre con un sistema existente de software para juntas directivas seguro. Busque establecer un cifrado de datos y una autenticación multifactorial (reforzando contraseñas con un método secundario de confirmación de identidad) en todos los dispositivos.

"La comodidad que pueden sacrificar los directores al no usar el correo electrónico personal la compensan con seguridad informática, mitigación de riesgos informáticos y menor responsabilidad personal", sostiene Dottie Schindlinger, evangelista de tecnología para la gobernanza de Diligent.

Para ayudar a los directores a evitar la tentación de recurrir a alternativas prácticas, asegúrese de que cualquier solución tecnológica que proporcione no plantee dificultades ni preocupaciones. Esta debería:

- Tener una configuración intuitiva, que solo se trate de descargar una aplicación en lugar de requerir diversos pasos desconocidos
- Ser fácil de usar
- Sincronizarse con los teléfonos inteligentes, las tabletas y las computadoras portátiles que utilizan los directores para llevar información en sus viajes

Independientemente de la solución que elija, su uso correcto y regular será clave para el éxito. Tómese el tiempo necesario para formar a los directores en el uso de la nueva tecnología a través de una capacitación práctica. (En la encuesta de NYSE a directores de empresas que cotizan en bolsa, solo el 9 % de los encuestados aseguró que debían recibir la misma capacitación de seguridad informática que los empleados). Refuerce la adopción a través de consultas periódicas, auditorías y verificación que involucren a los ejecutivos de seguridad de la información, cumplimiento y TI.

Con ataques de suplantación de identidad tipo Spear que se espera que sean cada vez más específicos y avanzados, la creciente amenaza del sabotaje de datos y los ataques a estados nación y al internet de las cosas que complican el panorama en general,[11] la seguridad informática sigue ascendiendo como una prioridad organizacional. Mientras tanto, las consecuencias que tiene en la reputación y la competencia el hecho de no mantenerse al día son cada vez más serias. Según Matteo Tonello de The Conference Board, las deficiencias en los procesos de gestión de riesgos y controles, así como en la seguridad de la información, "se consideran cada vez más como simples síntomas de una cultura de riesgo 'inadecuada' o 'deficiente'".[12]

La diligencia de la seguridad informática es imprescindible, y comienza en casa. Debido a las crecientes amenazas y riesgos en el entorno comercial de la actualidad y el creciente rol de las juntas directivas en la supervisión de la seguridad informática, los directores no pueden permitirse esperar para garantizar que sus propias comunicaciones acaten las mejores prácticas en materia de seguridad informática. Incluir el uso de un sistema de mensajería seguro en sus directrices y políticas para las comunicaciones es un excelente punto de partida.

10 https://www.entrepreneur.com/article/272847

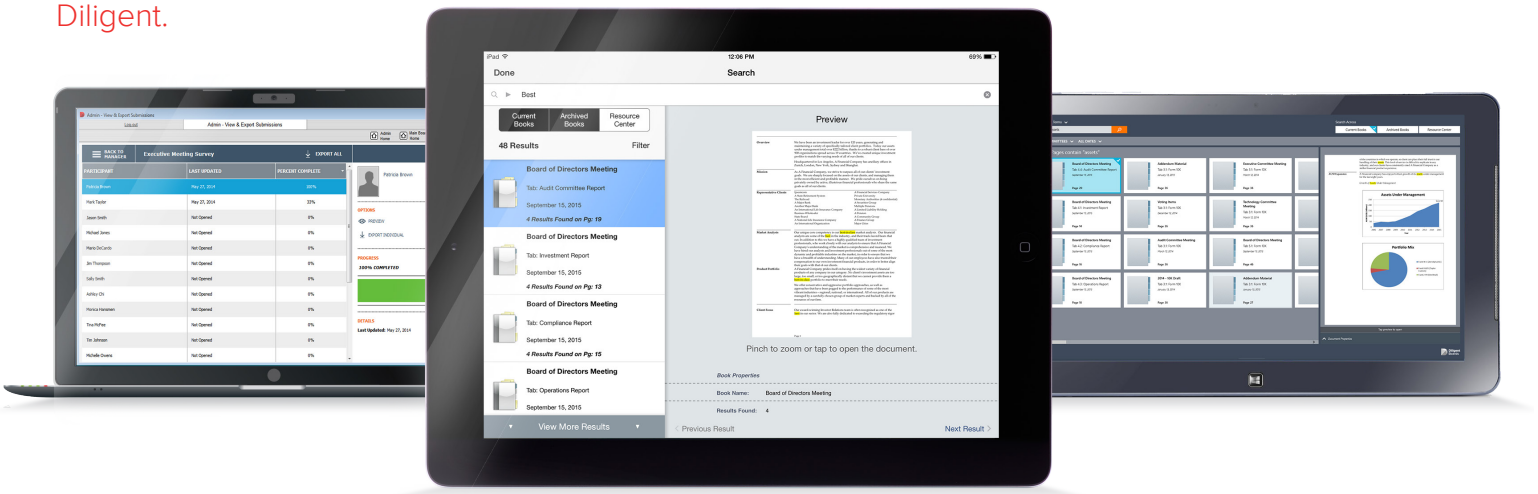
11 http://www.insurancejournal.com/news/international/2017/01/11/438549.htm

12 https://corpgov.law.harvard.edu/2017/02/15/risk-management-and-the-board-of-directors-4/

Diligent

Potenciar el valor de la información. Con seguridad.

Diligent ayuda a las principales organizaciones del mundo a potenciar, con seguridad, el poder de la información y la colaboración, dotando a sus juntas directivas y equipos de administración de los recursos de información necesarios para tomar mejores decisiones. Más de 4.700 clientes en más de 70 países confían en Diligent para contar con acceso inmediato a la información más sensible y confidencial junto con las herramientas para revisar, discutir y colaborar en la toma de decisiones clave. Diligent Boards acelera y simplifica la manera en que se produce y se entrega el material para juntas directivas a través de iPad, dispositivos con Windows y navegadores. Al mismo tiempo, Diligent Boards ofrece a líderes en todo el mundo ventajas prácticas como la reducción de los costos de producción, apoyo a las metas de sostenibilidad y ahorro de tiempo y recursos administrativos y de TI. Únase a los líderes. Obtenga Diligent.



Consíguelo en el App Store · Consíguelo de Microsoft · DISPONIBLE EN Google Play · AICPA SOC · ISO 27001 CERTIFIED BY BRIGHTLINE

Para mayor información o solicitar una demostración, comuníquese con nosotros a través de:

Tel.: + 1 973 939 9404
Correo electrónico: info@diligent.com
Visite: www.diligent.com